H3C S12500G-AF&S12500CR 系列交换机 日志信息参考

资料版本：6W102-20240202

产品版本：Release 8054P04 及以上版本

目 录

1 简介

本文包含日志的参数介绍、产生原因、处理建议等，为用户进行系统诊断和维护提供参考。

除了 S12500G-AF 和 S12500CR 特有的日志信息外，本文还包含 Release 8054Pxx～Release 8055Pxx 版本基于的 Comware V7 平台版本的日志信息，其中的部分日志信息本产品可能并不支持，请以设备的实际情况为准。

本文假设您已具备数据通信技术知识，并熟悉 H3C 网络产品。

1.1 日志格式说明

缺省情况下，日志信息根据输出方向不同，采用如下格式：

- 日志主机方向（RFC 3164 定义的格式）：

```
<PRI>TIMESTAMP Sysname %%vendorMODULE/severity/MNEMONIC: location; CONTENT
```

- 非日志主机方向：

```
Prefix TIMESTAMP Sysname MODULE/severity/MNEMONIC: CONTENT
```

表1-1 日志字段说明

字段	描述
<PRI>	优先级标识符，仅存在于输出方向为日志主机的日志信息。优先级的计算公式为：facility×8＋severity • facility表示日志主机的记录工具，由 **info-center loghost**命令设置，主要用于在日志主机端标志不同的日志来源，查找、过滤对应日志源的日志。 • severity表示日志信息的严重等级，具体含义请参见 表 1-2
Prefix	信息类型标识符，仅存在于输出方向为非日志主机方向的日志信息 • 百分号（%）：表示该日志信息为 Informational 级别及以上级别的日志 • 星号（*）：表示该日志信息为 Debug 级别的日志
TIMESTAMP	时间戳记录了日志信息产生的时间，方便用户查看和定位系统事件 • 日志主机方向：时间戳精确到秒，用户可以通过 **info-center timestamp loghost**命令自定义时间显示格式 • 非日志主机方向：时间戳精确到毫秒，用户可以通过 **info-center timestamp**命令自定义时间显示格式
Sysname	生成该日志信息的设备的名称或IP地址
%%vendor	厂家标志，%%10表示本日志信息由H3C设备生成 只有发往日志主机的日志中携带该字段
MODULE	生成该日志信息的功能模块的名称
severity	日志信息的等级，具体说明请参见表1-2
MNEMONIC	助记符，本字段为该日志信息的概述，是一个不超过32个字符的字符串
location	定位信息，用来标识该日志信息的产生者。本字段为可选字段，只有在日志信息发往日志主机时才会存在，可能包含以下参数： • -MDC=XX，表示生成该日志的 MDC 的编号

	• -DevIp=XXX.XXX.XXX.XXX，表示日志发送者的源 IP • -Slot=XX，表示生成该日志的 Slot 编号 • -Chassis=XX-Slot=XX，表示生成该日志的 Chassis 编号和 Slot 编号 格式如下： -attribute1=x-attribute2=y…-attributeN=z 定位信息和日志描述之间用分号和空格“; ”分隔 说明 日志手册中以输出到非日志主机方向的日志为例，不提供 location 字段。
CONTENT	该日志的具体内容，包含事件或错误发生的详细信息 对于本字段中的可变参数域，本文使用表1-3定义的方式表示 大部分日志的CONTENT字段为一个或多个句子，例如“VTY logged in from 192.168.1.21.”；部分日志专用于记录参数的取值，其CONTENT字段的形式为“关键信息1;关键信息2;……关键信息n.”，关键信息的格式可能为： • 关键字(关键字序号)=数值 • 关键字(关键字序号)=(文本序号)文字描述 其中，序号是设备出厂时约定的参数，用于供日志主机软件（例如安全管理系统）准确、高效地解析关键信息中的内容 • 关键字序号用来代表其前面的关键字 • 文本序号用来代表其后面的文字描述 例如：streamAlarmType(1032)=(42)Too fast speed of TCP session to destination IP，其中1032就是streamAlarmType的代号，42就是Too fast speed of TCP session to destination IP的代号

日志信息按严重性可划分为如 表 1-2所示的八个等级，各等级的严重性依照数值从 0～7 依次降低。

表1-2 日志重性等级说明

级别	严重程度	描述
0	Emergency	表示设备不可用的信息，如系统授权已到期
1	Alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	Critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	Error	表示错误信息，如接口链路状态变化，存储卡拔出等
4	Warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	Notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	Informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行ping命令的日志信息等
7	Debug	表示调试过程产生的信息

本文使用 表 1-3定义的方式表示日志描述字段中的可变参数域。

表1-3 可变参数域

参数标识	参数类型
INT16	有符号的16位整数
UINT16	无符号的16位整数
INT32	有符号的32位整数
UINT32	无符号的32位整数
INT64	有符号的64位整数
UINT64	无符号的64位整数
DOUBLE	有符号的双32位整数，格式为：[INT32].[INT32]
HEX	十六进制数
CHAR	字节类型
STRING	字符串类型
IPADDR	IP地址
MAC	MAC地址
DATE	日期
TIME	时间

1.2 如何获取日志信息

业务模块将生成的日志发送给信息中心模块，由信息中心模块统一管理。

缺省情况下，设备的信息中心功能处于开启状态，并允许向控制台（console）、监视终端（monitor）、日志缓冲区（logbuffer）、日志主机（loghost）和日志文件（logfile）方向输出日志信息。

通过 **info-center source**命令可以设置日志信息的输出规则，通过输出规则可以指定日志的输出方向以及对哪些特性模块或信息等级的日志信息进行输出。所有信息等级高于或等于设置等级的日志信息都会被输出到指定的输出方向。例如，输出规则中如果指定允许等级为 6（informational）的信息输出，则等级 0～6 的信息均会被输出到指定的输出方向。

关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

1.2.1 通过控制台获取日志

用户通过 Console 接口登录设备后，可以在控制台上实时看到设备输出的日志。

1.2.2 通过监视终端获取日志

监视终端是指以 AUX、VTY、TTY 类型用户线登录的用户终端。使用监视终端登录设备后，如需在当前终端上显示日志，还需要进行以下配置：

- 执行 **terminal monitor**命令打开终端显示功能

- 通过 **terminal logging level**命令设置在当前终端上显示日志的级别。实际能够在终端上显示的日志级别由 **info-center source**和 **terminal logging level**命令共同决定。

terminal monitor命令和 **terminal logging level**命令只对当前登录生效，用户重新登录设备后，需要重新配置。

1.2.3 通过日志缓冲区获取日志

通过 **display logbuffer**命令可以查看日志缓冲区中记录的日志。

1.2.4 通过日志文件获取日志

系统将日志保存到日志文件缓冲区后，用户可以通过以下方式将日志文件缓冲区中的日志保存到日志文件：

- 执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件。
- 系统周期性将日志文件缓冲区中的内容保存到日志文件。缺省情况下，周期为 24 小时。用户可以通过 **info-center logfile frequency**命令修改保存周期。

日志文件的缺省保存路径为 cfa0:/logfile/；如果 CF 卡已经分区，则缺省保存路径为 CF 卡第二个分区下的 logfile 目录（cfa1:/logfile/）。

通过 **more**命令可以查看日志文件的内容。

1.2.5 通过日志主机获取日志

用户配置 **info-center loghost**命令后，设备会向指定IP地址的日志主机发送日志，在日志主机上用户可以查看到设备的日志。如需指定多个日志主机，可多次执行 **info-center loghost**命令。

请注意：设备上配置的日志主机接收日志信息的端口号必须和日志主机侧的设置一致，否则，日志主机将无法接收日志信息。这个端口号的缺省值为 514。

1.3 软件模块列表

表 1-4列出了所有可能生成系统日志信息的软件模块。其中，“OPENSRC”代表所有开源软件模块的日志，本文使用“OPENSRC（开源软件名称）”表示不同开源软件模块输出的日志信息。

表1-4 软件模块列表

模块名	模块全称
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ANCP	Access Node Control Protocol
APMGR	Access Point Management
ARP	Address Resolution Protocol
ATK	ATK Detect and Defense
ATM	Asynchronous Transfer Mode

模块名	模块全称
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CFD	Connectivity Fault Detection
CFGMAN	Configuration Management
CGROUP	Collaboration Group
CONNLMT	Connect Limit
DEV	Device Management
DHCP	Dynamic Host Configuration Protocol
DHCPR	IPv4 DHCP Relay
DHCPS	IPv4 DHCP Server
DHCPS6	IPv6 DHCP Server
DHCPSP4	IPv4 DHCP snooping
DHCPSP6	IPv6 DHCP snooping
DIAG	Diagnosis
DLDP	Device Link Detection Protocol
DOT1X	802.1X
EDEV	Extender Device Management
eMDI	Enhanced Media Delivery Index
EPA	Endpoint Analysis
ERPS	Ethernet Ring Protection Switching
ETH	Ethernet
ETHMLAG	Ethernet Multichassis link aggregation
ETHOAM	Ethernet Operation, Administration and Maintenance
EVB	Ethernet Virtual Bridging
EVIISIS	Ethernet Virtual Interconnect Intermediate System-to-Intermediate System
FCOE	Fibre Channel Over Ethernet
FCLINK	Fibre Channel Link
FCZONE	Fibre Channel Zone
FGROUP	Flow Group
FIB	Forwarding Information Base
FILTER	Filter
FIPSNG	FIP Snooping
FS	File System

模块名	模块全称
FTP	File Transfer Protocol
gRPC	Google Remote Procedure Call
HA	High Availability
HQOS	Hierarchical QoS
HTTPD	Hypertext Transfer Protocol Daemon
HLTH	Health
IFMON	Interface Monitor
IFNET	Interface Net Management
IKE	Internet Key Exchange
IPCC	Intelligent Proactive Congestion Control
iNQA	Intelligent Network Quality Analyzer
iNOF	Intelligent Lossless NVMe Over Fabric
IMA	Integrity Measurements Architecture
IP6ADDR	IPv6 address
IP6FW	IPv6 Forwarding
IPADDR	IP address
IPFW	IP Forwarding
IPSEC	IP Security
IPSG	IP Source Guard
IPSGT	IP address-Security Group Tag
IRDP	ICMP Router Discovery Protocol
IRF	Intelligent Resilient Framework
ISIS	Intermediate System-to-Intermediate System
ISSU	In-Service Software Upgrade
KPI	Key Performance Indicator
L2PT	Layer 2 Protocol Tunneling
L2TPV2	Layer 2 Tunneling Protocol Version 2
L2VPN	Layer 2 VPN
LAGG	Link Aggregation
LDP	Label Distribution Protocol
LIPC	Leopard Inter-process Communication
LLDP	Link Layer Discovery Protocol
LOAD	Load Management
LOGIN	Login
LPDT	Loopback Detection

模块名	模块全称
LS	Local Server
LSPV	LSP Verification
MAC	Media Access Control
MACA	MAC Authentication
MACSEC	MAC Security
MBFD	MPLS BFD
MBUF	Memory buffer
MCS	Multicast snooping
MCS6	IPv6 Multicast snooping
MDC	Multitenant Device Context
MFIB	Multicast Forwarding Information Base
MGROUP	Mirroring group
MLAG	Multichassis link aggregation
MLD	Multicast Listener Discovery Protocol
MOD	Mirror On Drop
MPLS	Multiprotocol Label Switching
MRP	Media Redundancy Protocol
MTLK	Monitor Link
MTP	Maintain Probe
NAT	Network Address Translate
NA4	IPv4 NetAnalysis
NETCONF	Network Configuration Protocol
ND	Neighbor Discovery
NQA	Network Quality Analyzer
NSS	Session-based NetStream
NTP	Network Time Protocol
OAP	Open Application Platform
OPENSRC(FreeRADIUS)	Open Source
OBJP	Object Policy
OFP	OpenFlow Protocol
ONVIF	Open Network Video Interface Forum
OPTMOD	Optical Module
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PFILTER	Packet Filter

模块名	模块全称
PBB	Provider Backbone Bridge
PBR	Policy Based Route
PCE	Path Computation Element
PEX	Port Extender
PIM	Protocol Independent Multicast
PIM6	IPv6 Protocol Independent Multicast
PING	Packet Internet Groper
PKG	Package
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PKTCPT	Packet Capture
PoE	Power over Ethernet
PORTAL	Portal
PORTSEC	Port Security
PPP	Point to Point Protocol
PTP	Precision Time Protocol
PTS	Platform Trust Services
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RESMON	RESOURCE MONITER
RDDC	Redundancy
RIP	Routing Information Protocol
RIPNG	Routing Information Protocol Next Generation
RM	Routing Management
RPR	Resilient Packet Ring
RRPP	Rapid Ring Protect Protocol
RTM	Real-Time Management
SAVA	Source Address Validation Architecture
SAVI	Source Address Validation Improvement
SCMD	Service Control Manager
SCRLSP	Static CRLSP
SESSION	Session
SFLOW	Sampler Flow
SHELL	Shell

模块名	模块全称
SIMMGR	Simulation Manage
SLSP	Static LSP
SMARTMC	Smart Management Center
SMLK	Smart Link
SNMP	Simple Network Management Protocol
SOCKET	Socket
SSHC	Secure Shell Client
SSHS	Secure Shell Server
STAMGR	Station Management
STM	Stack Topology Management
STP	Spanning Tree Protocol
SYSEVENT	System Event
SYSLOG	System Log
TCSM	Trusted Computing Services Management
TACACS	Terminal Access Controller Access Control System
TELNETD	Telnet Daemon
TRACK	Track
TRILL	Transparent Interconnect of Lots of Links
TSTREAM	Telemetry Stream
USBDPY	USB Deployment
VCF	Vertical Converged Framework
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VSRP	Virtual Service Redundancy Protocol
VXLAN	Virtual eXtensible LAN
WEB	Web
WEBAUTH	Web Authentication
WIPS	Wireless Intrusion Prevention System

1.4 文档使用说明

本文将系统日志信息按照软件模块分类，每个模块以字母顺序排序。在每个模块中，系统日志信息按照助记符的名称，以字母顺序排序。在开源软件模块输出的日志信息中，助记符均为 SYSLOG，本文使用日志简要描述作为该类日志信息标题，不做特殊排序。

本文以表格的形式对日志信息进行介绍。有关表中各项的含义请参考 表 1-5。

表1-5 日志信息表内容说明

表项	说明	举例
日志内容	显示日志信息的具体内容	ACL [UINT32] [STRING] [COUNTER64] packet(s).
日志含义	日志信息的描述	匹配到IPv4 ACL规则的报文数的信息
参数解释	按照参数在日志中出现的顺序对参数进行解释 参数顺序用“$数字”表示，例如“$1”表示在该日志中出现的第一个参数	$1：ACL编号 $2：ACL规则的ID和内容 $3：与ACL规则匹配的数据包个数
日志等级	日志严重等级	6
举例	一个真实的日志信息举例。由于不同的系统设置，日志信息中的“<Int_16>TIMESTAMP HOSTNAME %%vendor”部分也会不同，本文表格中的日志信息举例不包含这部分内容	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
对系统的影响	产生该日志时，设备本身的软硬件系统、设备上的业务会受到哪些影响，即对设备自身的影响	对系统无影响
日志产生原因	解释日志信息和日志生成的原因	匹配一条ACL规则的数据包个数。该日志会在数据包个数发生变化时输出
处理建议	建议用户应采取哪些处理措施。级别为6的“Informational”日志信息是正常运行的通知信息，用户无需处理	系统正常运行时产生的信息，无需处理

2 AAA

本节介绍 AAA 模块输出的日志信息。

2.1 AAA_FAILURE

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA failed.
日志含义	用户AAA请求失败
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	5 (Notification)
举例	AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA failed.
对系统的影响	对系统无影响
日志产生原因	由于未收到服务器响应，用户名/密码错误，或其他原因（例如用户申请的服务类型不正确），用户的AAA请求被拒绝
处理建议	• 检查设备与服务器的连接 • 重新输入用户名和密码 • 检查服务器上的设置（例如服务类型）是否正确 • 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

2.2 AAA_LAUNCH

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA launched.
日志含义	用户发送AAA请求
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	6 (Informational)
举例	AAA/6/AAA_LAUNCH: -AAAType=AUTHEN-AAADomain=domain1-Service=login-UserName=cwf@system; AAA launched.
对系统的影响	对系统无影响
日志产生原因	用户通过AAA认证登录
处理建议	系统正常运行时产生的信息，无需处理

2.3 AAA_SUCCESS

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA succeeded.
日志含义	用户AAA请求成功
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	6 (Informational)
举例	AAA/6/AAA_SUCCESS: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA succeeded.
对系统的影响	对系统无影响
日志产生原因	设备接受用户的AAA请求
处理建议	系统正常运行时产生的信息，无需处理

3 ACL

本节介绍 ACL 模块输出的日志信息。

3.1 ACL_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The resources are insufficient.
日志含义	硬件资源不足，ACL规则加速失败
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4 (Warning)
举例	ACL/4/ACL_ACCELERATE_NO_RES: Failed to accelerate IPv6 ACL 2001. The resources are insufficient.
对系统的影响	如果ACL内包含有大量规则，且未进行加速，报文进行匹配的耗时变长，可能会影响协议类报文建立连接的时间或者报文转发的效率
日志产生原因	因硬件资源不足，系统加速ACL失败
处理建议	请删除一些ACL规则或者关闭其他ACL的加速功能，释放硬件资源

3.2 ACL_ACCELERATE_NONCONTIGUOUSMASK

日志内容	Failed to accelerate IPv4 ACL [UINT32]. ACL acceleration supports only contiguous wildcard masks.
日志含义	IPv4 ACL规则加速失败
参数解释	$1：ACL编号
日志等级	4 (Warning)
举例	ACL/4/ACL_ACCELERATE_NONCONTIGUOUSMASK: Failed to accelerate IPv4 ACL 2001. ACL acceleration supports only contiguous wildcard masks.
对系统的影响	如果IPv4 ACL内包含有大量规则，且未进行加速，报文进行匹配的耗时变长，可能会影响协议类报文建立连接的时间或者报文转发的效率
日志产生原因	因IPv4 ACL中的规则指定了非连续的通配符掩码，导致ACL加速失败
处理建议	请修改或删除指定了非连续的通配符掩码的IPv4 ACL规则

3.3 ACL_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The operation is not supported.
日志含义	ACL规则加速失败，操作不支持
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4 (Warning)
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 ACL 2001. The operation is not supported.
对系统的影响	如果ACL内包含有大量规则，且未进行加速，报文进行匹配的耗时变长，可能会影响协议类报文建立连接的时间或者报文转发的效率
日志产生原因	因系统不支持ACL加速而导致ACL加速失败
处理建议	系统正常运行时产生的信息，无需处理

3.4 ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP

日志内容	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
日志含义	IPv6 ACL规则加速失败
参数解释	$1：ACL编号
日志等级	4 (Warning)
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP: Failed to accelerate IPv6 ACL 3001. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
对系统的影响	如果IPv6 ACL内包含有大量规则，且未进行加速，报文进行匹配的耗时变长，可能会影响协议类报文建立连接的时间或者报文转发的效率
日志产生原因	因IPv6 ACL中的规则指定了hop-by-hop参数，导致ACL加速失败
处理建议	请删除指定了hop-by-hop参数的IPv6 ACL规则

3.5 ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG

日志内容	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support specifying multiple TCP flags in one rule.
日志含义	IPv6 ACL规则加速失败
参数解释	$1：ACL编号
日志等级	4 (Warning)
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG: Failed to accelerate IPv6 ACL 3001. ACL acceleration does not support specifying multiple TCP flags in one rule.
对系统的影响	如果IPv6 ACL内包含有大量规则，且未进行加速，报文进行匹配的耗时变长，可能会影响协议类报文建立连接的时间或者报文转发的效率
日志产生原因	因IPv6 ACL中的规则指定了多个TCP 标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）参数，导致ACL加速失败
处理建议	请删除IPv6 ACL规则中指定的多个TCP 标志位参数，最多仅保留一个标志位，或者删除该IPv6 ACL规则

3.6 ACL_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] ACL [UINT32].
日志含义	ACL规则加速失败
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4 (Warning)
举例	ACL/4/ACL_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 ACL 2001.
对系统的影响	如果ACL内包含有大量规则，且未进行加速，报文进行匹配的耗时变长，可能会影响协议类报文建立连接的时间或者报文转发的效率
日志产生原因	因系统异常或者其他未知原因导致ACL加速配置失败
处理建议	1. 请先执行 **undo accelerate**命令，再重新执行 **accelerate**命令配置ACL规则的加速匹配功能 2. 如果重新配置 ACL 规则的加速匹配功能仍然失败，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

3.7 ACL_IPV6_STATIS_INFO

日志内容	IPv6 ACL [UINT32] [STRING] [UINT64] packet(s).
日志含义	匹配到IPv6 ACL规则的报文数的信息
参数解释	$1：ACL编号 $2：IPv6 ACL规则的ID及内容 $3：匹配上规则的报文个数
日志等级	6 (Informational)
举例	ACL/6/ACL_IPV6_STATIS_INFO: IPv6 ACL 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
对系统的影响	对系统无影响
日志产生原因	匹配上IPv6 ACL规则的报文数量发生变化
处理建议	系统正常运行时产生的信息，无需处理

3.8 ACL_NO_MEM

日志内容	Failed to configure [STRING] ACL [UINT32] due to lack of memory
日志含义	内存不足，ACL规则下发失败
参数解释	$1：ACL类型 $2：ACL编号
日志等级	3 (Error)
举例	ACL/3/ACL_NO_MEM: Failed to configure IPv4 ACL 2001 due to lack of memory.
对系统的影响	该ACL无法下发，不能正常生效
日志产生原因	内存不足导致配置ACL失败
处理建议	使用**display memory-threshold**命令检查内存使用情况： • 如果内存使用率过高，可以增加设备内存 • 如果内存使用率异常，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

3.9 ACL_REFRESH_EMTEMPLATE_FAIL

日志内容	Failed to refresh an exact-match template [UINT]. Reason：[STRING]
日志含义	删除、创建或修改EM模板失败
参数解释	$1：EM模板ID $2：失败原因。取值包括： • Not enough hardware resources to complete the operation：硬件资源不足 • The parameter is incorrect.：EM 模板参数设置不正确 • Can't modify the exact-match template. The exact-match template has been matched.：当前 EM 模板已匹配 OpenFlow 表项无法修改
日志等级	3 (Error)
举例	ACL/3/ACL_REFRESH_EMTEMPLATE_FAIL: Failed to refresh an exact-match template 1. Reason：Not enough hardware resources to complete the operation.
对系统的影响	对系统无影响
日志产生原因	删除、创建或修改EM模板失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

3.10 ACL_STATIS_INFO

日志内容	ACL [UINT32] [STRING] [UINT64] packet(s).
日志含义	匹配到IPv4 ACL规则的报文数的信息
参数解释	$1：ACL编号 $2：IPv4 ACL规则的ID及内容 $3：匹配上规则的报文个数
日志等级	6 (Informational)
举例	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
对系统的影响	对系统无影响
日志产生原因	匹配上IPv4 ACL规则的报文数量发生变化
处理建议	系统正常运行时产生的信息，无需处理

4 ANCP

本节介绍 ANCP（Access Node Control Protocol）模块输出的日志信息。

4.1 ANCP_INVALID_PACKET

日志内容	-NeighborName=[STRING]-State=[STRING]-MessageType=[STRING]; The [STRING] value [STRING] is wrong, and the value [STRING] is expected.
日志含义	设备收到无效的ANCP报文
参数解释	$1：ANCP邻居名 $2：邻居状态 $3：报文类型 $4：错误字段 $5：错误字段值 $6：期望值
日志等级	6 (Informational)
举例	ANCP/6/ANCP_INVALID_PACKET: -NeighborName=Dslam-State=SYNSENT-MessageType=SYNACK; The Sender Instance value 0 is wrong, and the value 1 is expected.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	系统收到一个错误的ANCP邻接报文，报文中指定字段与预期值不一致
处理建议	1. 请检查并确保 ANCP 配置正确 2. 执行以上操作后，若问题仍未解决，请收集如下信息，并联系技术支持人员 ○ 上述步骤的执行结果 ○ 设备的配置文件、日志信息、告警信息

5 APMGR

本节介绍 AP 管理模块输出的日志信息。

5.1 APMGR_AC_MEM_ALERT

日志内容	The memory utilization has reached the threshold.
日志含义	AC内存到达门限值导致AP上线失败
参数解释	无
日志等级	4 (Warning)
举例	APMGR/4/APMGR_AC_MEM_ALERT: The memory utilization has reached the threshold.
对系统的影响	AP无法上线
日志产生原因	创建手工AP成功时触发，但由于达到内存门限值，AP不能上线
处理建议	此时不应该继续创建AP，且不允许有新AP上线

5.2 APMGR_ADD_AP_FAIL

日志内容	AP [STRING] failed to come online using serial ID [STRING]: MAC address [STRING] is being used by AP [STRING].
日志含义	AP的MAC地址重复导致AP上线失败
参数解释	$1：AP的名称 $2：AP的序列号 $3：AP的MAC地址 $4：AP的名称
日志等级	4 (Warning)
举例	APMGR/4/ APMGR_ADD_AP_FAIL: AP ap1 failed to come online using serial ID 01247ef96: MAC address 0023-7961-5201 is being used by AP ap2.
对系统的影响	AP无法上线
日志产生原因	AP上线过程中，由于MAC地址已存在，添加MAC地址失败，AP不能上线
处理建议	将此AP的MAC地址或serial ID对应的手工AP删除一个，AP方能正常上线

5.3 APMGR_AP_OFFLINE

日志内容	AP [STRING] went offline. State changed to Idle.
日志含义	AP下线
参数解释	$1：AP的名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_AP_OFFLINE: AP ap1 went offline. State changed to Idle.
对系统的影响	无
日志产生原因	产生此日志的可能原因包括： • AP 主动下线 • AP 异常下线
处理建议	• 若 AP 主动下线，则不用排查问题 • 若 AP 异常下线，需要根据调试信息定位并解决问题 • 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

5.4 APMGR_AP_ONLINE

日志内容	AP [STRING] went online. State changed to Run.
日志含义	AP上线
参数解释	$1：AP的名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_AP_ONLINE: AP ap1 went online. State changed to Run.
对系统的影响	无
日志产生原因	AP上线，状态变为运行状态
处理建议	无需处理

5.5 APMGR_CWC_IMG_DOWNLOAD_COMPLETE

日志内容	System software image file [STRING] downloading through the CAPWAP tunnel to AC [STRING] completed.
日志含义	AP从AC下载系统镜像成功
参数解释	$1：镜像文件名 $2：AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel to AC 192.168.10.1 completed.
对系统的影响	无
日志产生原因	AP从AC下载系统镜像成功时，打印该日志
处理建议	无需处理

5.6 APMGR_CWC_IMG_DOWNLOAD_START

日志内容	Started to download the system software image file [STRING] through the CAPWAP tunnel to AC [STRING].
日志含义	AP开始进行版本文件下载
参数解释	$1：下载的镜像文件名 $2：AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_IMG_DOWNLOAD_START: Started to download the system software image file 5800.ipe through the CAPWAP tunnel to AC 192.168.10.1.
对系统的影响	无
日志产生原因	AP通过CAPWAP隧道从AC下载版本文件时，打印该日志
处理建议	保持AP和AC之间正常的网络连接使AP能够正常升级

5.7 APMGR_CWC_IMG_NO_ENOUGH_SPACE

日志内容	Insufficient flash memory space for downloading system software image file [STRING].
日志含义	AP上的Flash剩余空间不足导致AP进行版本升级不成功
参数解释	$1：下载的镜像文件名
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_IMG_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading system software image file 5800.ipe.
对系统的影响	无
日志产生原因	由于AP上的Flash剩余空间不足
处理建议	建议删除AP上无用的文件以进行版本升级

5.8 APMGR_CWC_LOCAL_AC_DOWN

日志内容	CAPWAP tunnel to Central AC [STRING] went down. Reason: [STRING].
日志含义	Central AC与Local AC之间隧道断开
参数解释	$1：Central AC的IP地址 $2：隧道断开的原因 • Added local AC IP address：添加新的 Local AC IP 地址 • Deleted local AC IP address：Local AC IP 地址被删除 • Local AC interface used for CAPWAP tunnel went down：CAPWAP 隧道使用的 Local AC 接口 DOWN • Local AC config changed：Local AC 配置改变 • N/A：不涉及
日志等级	4 (Warning)
举例	APMGR/4/APMGR_CWC_LOCAL_AC_DOWN: CAPWAP tunnel to Central AC 2.2.2.1 went down. Reason: Added local AC IP address.
对系统的影响	无
日志产生原因	参见打印的隧道断开原因
处理建议	**1.** 检查 Central AC 与 Local AC 的连接是否正常 **2.** 检查 Central AC 上的配置 **3.** 检查 Local AC 上的配置 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

5.9 APMGR_CWC_LOCAL_AC_UP

日志内容	CAPWAP tunnel to Central AC [STRING] went up.
日志含义	Central AC与Local AC建立CAPWAP隧道
参数解释	$1：Central AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_LOCAL_AC_UP: CAPWAP tunnel to Central AC 2.2.2.1 went up.
对系统的影响	无
日志产生原因	Central AC与Local AC成功建立CAPWAP隧道时，打印该日志
处理建议	无需处理

5.10 APMGR_CWC_REBOOT

日志内容	AP in state [STRING] is rebooting. Reason: [STRING]
日志含义	AP重启
参数解释	$1：AP的当前状态 $2：重启原因 • AP was reset：AP 重启 • Image was downloaded successfully：版本文件下载成功 • Stayed in idle state for a long time：长时间处于 idle 状态
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_REBOOT: AP in state Run is rebooting. Reason: AP was reset.
对系统的影响	无
日志产生原因	AP重启及重启原因
处理建议	无需处理

5.11 APMGR_CWC_RUN_DOWNLOAD_COMPLETE

日志内容	File [STRING] successfully downloaded through the CAPWAP tunnel to AC [STRING].
日志含义	AP从AC下载文件成功
参数解释	$1：下载文件的文件名 $2：AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel to AC 192.168.10.1.
对系统的影响	无
日志产生原因	AP从AC下载文件成功
处理建议	无需处理

5.12 APMGR_CWC_RUN_DOWNLOAD_START

日志内容	Started to download the file [STRING] through the CAPWAP tunnel to AC [STRING].
日志含义	AP开始从AC下载文件
参数解释	$1：下载文件的文件名 $2：AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_RUN_DOWNLOAD_START: Started to download the file ac.cfg through the CAPWAP tunnel to AC 192.168.10.1.
对系统的影响	无
日志产生原因	AP开始进行版本文件下载
处理建议	保持AP和AC之间都处于RUN状态，AC才能够正常下载文件到AP

5.13 APMGR_CWC_RUN_NO_ENOUGH_SPACE

日志内容	Insufficient flash memory space for downloading file [STRING].
日志含义	AP上的Flash剩余空间不足导致AP进行文件下载不成功
参数解释	$1：下载文件的文件名
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_RUN_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading file ac.cfg.
对系统的影响	无
日志产生原因	AP上的Flash剩余空间不足
处理建议	建议删除AP上无用的文件以进行文件下载

5.14 APMGR_CWC_TUNNEL_DOWN

日志内容	CAPWAP tunnel to AC [STRING] went down. Reason: [STRING].
日志含义	AP与AC间CAPWAP隧道断开
参数解释	$1：AC的IP地址 $2：隧道断开原因 • Added AP IP address：添加新的 AP IP 地址 • Deleted AP IP address：AP IP 地址被删除 • AP interface used for CAPWAP tunnel went down：CAPWAP 隧道使用的 AP 接口 DOWN • AP config changed：AP 配置改变 • AP was reset：AP 重启 • Number of echo retransmission attempts exceeded the limit：超过 echo 报文重传次数 • Full retransmission queue：重传队列满 • Data channel timer expired：数据隧道定时器超时 • Backup AC IP address changed：备 AC IP 地址改变 • Backup tunnel changed to master tunnel：备隧道切换成主隧道 • Failed to change backup tunnel to master tunnel：备切主失败 • Backup method changed：备份模式改变 • N/A：不涉及
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_TUNNEL_DOWN: CAPWAP tunnel to AC 192.168.10.1 went down. Reason: AP was reset.
对系统的影响	无
日志产生原因	AP与AC之间CAPWAP隧道断开以及断开原因
处理建议	1. 检查设备 AP 与设备 AC 的连接是否正常 2. 检查 AP 上的配置 3. 检查 AC 上的配置 4. 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

5.15 APMGR_CWC_TUNNEL_UP

日志内容	[STRING] CAPWAP tunnel to AC [STRING] went up.
日志含义	AP与AC间CAPWAP隧道建立
参数解释	$1：与AC连接的隧道的主备类型 • Master：主隧道 • Backup：备隧道 $2：AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWC_TUNNEL_UP: Master CAPWAP tunnel to AC 192.168.10.1 went up.
对系统的影响	无
日志产生原因	AP成功连接到AC，即AP已进入Run状态
处理建议	无需处理

5.16 APMGR_CWS_IMG_DOWNLOAD_COMPLETE

日志内容	System software image file [STRING] downloading through the CAPWAP tunnel for AP [STRING] completed.
日志含义	AP从AC下载系统镜像成功
参数解释	$1：AP已经下载完成的版本文件名 $2：AP名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_ CWS_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel for AP ap2 completed.
对系统的影响	无
日志产生原因	AP从AC下载系统镜像成功时，打印该日志
处理建议	无需处理

5.17 APMGR_CWS_IMG_DOWNLOAD_START

日志内容	AP [STRING] started to download the system software image file [STRING].
日志含义	AP开始进行版本文件下载
参数解释	$1：AC端配置的AP名称 $2：AP正在下载升级的版本文件名
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWS_IMG_DOWNLOAD_START: AP ap1 started to download the system software image file 5800.ipe.
对系统的影响	无
日志产生原因	AP通过CAPWAP隧道从AC下载版本文件时，打印该日志
处理建议	无需处理

5.18 APMGR_CWS_LOCAL_AC_DOWN

日志内容	CAPWAP tunnel to local AC [STRING] went down. Reason: [STRING].
日志含义	Central AC与Local AC之间隧道断开
参数解释	$1：Local AC的IP地址 $2：隧道断开的原因： • Neighbor dead timer expired：邻居截止定时器超时 • Local AC was deleted：Local AC 被删除 • Serial number changed：序列号改变 • Processed join request in Run state：在 Run 状态下处理 join request 报文 • Failed to retransmit message：处理重传消息失败 • N/A：不涉及
日志等级	4 (Warning)
举例	APMGR/4/APMGR_CWS_LOCAL_AC_DOWN: CAPWAP tunnel to local AC 1.1.1.1 went down. Reason: Serial number changed.
对系统的影响	无
日志产生原因	Central AC与Local AC之间隧道断开及断开原因
处理建议	1. 检查 Central AC 与 Local AC 的连接是否正常 2. 检查 Central AC 上的配置 3. 检查 Local AC 上的配置 4. 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

5.19 APMGR_CWS_LOCAL_AC_UP

日志内容	CAPWAP tunnel to local AC [STRING] went up.
日志含义	Central AC与Local AC建立CAPWAP隧道
参数解释	$1：Local AC的IP地址
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWS_LOCAL_AC_UP: CAPWAP tunnel to local AC 1.1.1.1 went up.
对系统的影响	无
日志产生原因	Central AC与Local AC成功建立CAPWAP隧道时，打印该日志
处理建议	无需处理

5.20 APMGR_CWS_RUN_DOWNLOAD_COMPLETE

日志内容	File [STRING] successfully downloaded through the CAPWAP tunnel for AP [STRING].
日志含义	AP从AC下载文件成功
参数解释	$1：AP已经下载完成的文件的文件名 $2：AC端配置的AP名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWS_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel for AP ap2.
对系统的影响	无
日志产生原因	AP从AC下载文件成功时，打印该日志
处理建议	无需处理

5.21 APMGR_CWS_RUN_DOWNLOAD_START

日志内容	AP [STRING] started to download the file [STRING].
日志含义	AP开始从AC下载文件
参数解释	$1：AC端配置的AP名称 $2：AP正在下载的文件的文件名
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWS_RUN_DOWNLOAD_START: AP ap1 started to download the file ac.cfg.
对系统的影响	无
日志产生原因	AP开始进行文件下载
处理建议	无需处理

5.22 APMGR_CWS_TUNNEL_DOWN

日志内容	CAPWAP tunnel to AP [STRING] went down. Reason: [STRING].
日志含义	AC与AP间CAPWAP隧道断开
参数解释	$1：AC端配置的AP名称 $2：隧道断开原因 • Neighbor dead timer expired：邻居截止定时器超时 • AP was reset：AP 重启 • AP was deleted：AP 被删除 • Serial number changed：序列号改变 • Processed join request in Run state：在 Run 状态下处理 join request 报文 • Failed to retransmit message：处理重传消息失败 • Received WTP tunnel down event from AP：接收到来自 AP 的 WTP DOWN 隧道事件 • Backup AC closed the backup tunnel：备 AC DOWN 自身的隧道 • Tunnel switched：由于隧道切换 • N/A：不涉及
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWS_TUNNEL_DOWN: CAPWAP tunnel to AP ap1 went down. Reason: AP was reset.
对系统的影响	AP不可用
日志产生原因	AP下线及下线原因
处理建议	**1.** 检查设备 AP 与设备 AC 的连接是否正常 **2.** 检查 AP 上的配置 **3.** 检查 AC 上的配置 **4.** 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

5.23 APMGR_CWS_TUNNEL_UP

日志内容	[STRING] CAPWAP tunnel to AP [STRING] went up.
日志含义	AC与AP间CAPWAP隧道建立
参数解释	$1：与AP连接的隧道的主备类型 • Master：主隧道 • Backup：备隧道 $2：AP名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_CWS_TUNNEL_UP: Backup CAPWAP tunnel to AP ap1 went up.
对系统的影响	无
日志产生原因	AC端配置的AP成功上线，即此AP进入Run状态
处理建议	无需处理

5.24 APMGR_LOCAL_AC_OFFLINE

日志内容	Local AC [STRING] went offline. State changed to Idle.
日志含义	Local AC下线
参数解释	$1：Local AC的名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_LOCAL_AC_OFFLINE: Local AC ac1 went offline. State changed to Idle.
对系统的影响	Local AC不可用
日志产生原因	产生此日志的可能原因包括： • Local AC 主动下线 • Local AC 异常下线
处理建议	• 若 Local AC 主动下线，则不用排查问题 • 若 Local AC 异常下线，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

5.25 APMGR_LOCAL_AC_ONLINE

日志内容	Local AC [STRING] went online. State changed to Run.
日志含义	Local AC上线
参数解释	$1：Local AC的名称
日志等级	6 (Informational)
举例	APMGR/6/APMGR_LOCAL_AC_ONLINE: Local AC ac1 went online. State changed to Run.
对系统的影响	无
日志产生原因	Local AC上线，状态变为运行状态
处理建议	无需处理

6 ARP

本节介绍 ARP 模块输出的日志信息。

6.1 ARP_ACTIVE_ACK_NO_REPLY

日志内容	No ARP reply from IP [STRING] was received on interface [STRING].
日志含义	接口未收到ARP应答
参数解释	$1：IP地址 $2：接口名称
日志等级	6 (Informational)
举例	ARP/6/ARP_ACTIVE_ACK_NO_REPLY: No ARP reply from IP 192.168.10.1 was received on interface Ethernet0/1/0.
对系统的影响	无
日志产生原因	产生此日志的可能原因包括： • ARP 主动确认功能检测到攻击 • 接口向所收到 ARP 报文的发送端 IP 发送 ARP 请求，未收到 ARP 应答
处理建议	1. 检查设备上学习到的 ARP 表项中的 IP 和 MAC 是否对应（如果网络部署中存在网关和服务器，优先检查网关和服务器的 IP 和 MAC 是否对应） 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.2 ARP_ACTIVE_ACK_NOREQUESTED_REPLY

日志内容	Interface [STRING] received from IP [STRING] an ARP reply that was not requested by the device.
日志含义	接口收到的ARP应答不是设备发送的ARP请求报文的应答报文
参数解释	$1：接口名称 $2：IP地址
日志等级	6 (Informational)
举例	ARP/6/ARP_ACTIVE_ACK_NOREQUESTED_REPLY: Interface GigabitEthernet1/0/1 received from IP 192.168.10.1 an ARP reply that was not requested by the device.
对系统的影响	可能导致部分正常的ARP应答报文被丢弃，影响正常业务
日志产生原因	产生此日志的可能原因包括： • ARP 主动确认功能检测到攻击 • 接口在未向 ARP 报文发送端 IP 地址发送 ARP 请求的情况下，收到 ARP 应答
处理建议	**1.** 通过抓包的方式检查网络中是否存在 ARP 报文攻击，查找攻击源 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.3 ARP_BINDRULETOHW_FAILED

日志内容	Failed to download binding rule to hardware on the interface [STRING], SrcIP [IPADDR], SrcMAC [MAC], VLAN [UINT16], Gateway MAC [MAC].
日志含义	下发绑定规则失败
参数解释	$1：接口名称 $2：源IP地址 $3：源MAC地址 $4：VLAN编号 $5：网关MAC地址
日志等级	5 (Notification)
举例	ARP/5/ARP_BINDRULETOHW_FAILED: Failed to download binding rule to hardware on the interface Ethernet1/0/1, SrcIP 1.1.1.132, SrcMAC 0015-E944-A947, VLAN 1, Gateway MAC 00A1-B812-1108.
对系统的影响	无
日志产生原因	由于硬件资源不足、内存不足或其他硬件错误导致绑定规则下发失败
处理建议	**1.** 执行 **display qos-acl resource**命令，检查硬件ACL资源是否充足 **2.** 如果充足，则请执行步骤 2 **3.** 如果不充足，则请取消部分 ACL 配置或接受当前结果 **4.** 执行 **display memory**命令，检查内存资源是否充足 **5.** 如果充足，则请执行步骤 3 **6.** 如果不充足，则请取消部分配置或接受当前结果 **7.** 硬件发生错误，请取消最后一次相关配置，并重新尝试 **8.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.4 ARP_BROADCAST_PASS

日志内容	形式一： Failed to issue the command to hardware on interface [string] in slot [INT32]. 形式二： Failed to issue the command to hardware on interface [string] in chassis [INT32] slot [INT32]. 形式三： Failed to issue IP address [STRING] of interface [STRING] to hardware in slot [INT32]. 形式四： Failed to issue IP address [STRING] of interface [STRING] to hardware in chassis [INT32] slot [INT32].
日志含义	**arp broadcast pass-through enable**命令或者VLAN接口IP地址下发硬件失败
参数解释	形式一： $1：接口名称 $2：slot编号 形式二： $1：接口名称 $2：chassis编号 $3：slot编号 形式三： $1：IP地址 $2：接口名称 $3：slot编号 形式四： $1：IP地址 $2：接口名称 $3：chassis编号 $4：slot编号
日志等级	4 (Warning)
举例	形式一： ARP/4/ARP_BROADCAST_PASS: Failed to issue the command to hardware on interface Vlan-interface 1 in slot 1. 形式二： ARP/4/ARP_BROADCAST_PASS: Failed to issue the command to hardware on interface Vlan-interface 1 in chassis 1 slot 1. 形式三： ARP/4/ARP_BROADCAST_PASS: Failed to issue IP address 1.1.1.2 of interface Vlan-interface1 to hardware in slot 1. 形式四： ARP/4/ARP_BROADCAST_PASS: Failed to issue IP address 1.1.1.2 of interface Vlan-interface1 to hardware in chassis 1 slot 1.
对系统的影响	**arp broadcast pass-through enable**命令或者VLAN接口IP地址下发硬件失败，可能导致CPU资源被大量ARP广播报文占用，造成设备CPU损耗

日志产生原因	产生此日志的可能原因包括： • 指定 slot 上硬件资源不足 • 硬件不支持配置 **arp broadcast pass-through enable**功能
处理建议	1. 确认硬件是否支持 **arp broadcast pass-through enable**功能 o 如果不支持，则无需处理 o 如果支持，则请执行步骤 2 2. 执行 **display hardware internal qacl show**命令，检查硬件ACL资源是否充足 o 如果充足，则请执行步骤 3 o 如果不充足，则请删除一些 ACL 规则或者关闭其他 ACL 的加速功能，释放硬件资源 3. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.5 ARP_DETECTION_DROP_L2IF

日志内容	ARP attack detection dropped a packet because of [STRING]. (Interface [STRING]; Source IP [STRING]).
日志含义	二层接口下ARP Detection检测丢包
参数解释	$1：ARP Detection丢包的类型 • sourceMacInvalidDrop：ARP 报文源 MAC 地址检查不合法丢弃 • destMacInvalidDrop：ARP 报文目的 MAC 地址检查不合法丢弃 • ipInvalidDrop：ARP 报文源和目的 IP 地址检查不合法丢弃 • ipcimNobindingDrop：ARP 报文结合用户合法性检查不通过丢弃 $2：ARP Detection丢包的接口 $3：ARP Detection丢包的源IP地址
日志等级	4 (Warning)
举例	ARP/4/ARP_DETECTION_DROP_L2IF: ARP attack detection dropped a packet because of ipInvalidDrop. (Interface GigabitEthernet2/0/1; Source IP 224.0.0.0).
对系统的影响	存在ARP报文因为ARP Detection功能检测被丢弃，不影响正常业务
日志产生原因	ARP Detection功能开启之后，二层接口下ARP Detection功能检测到不合法ARP报文并将其丢弃
处理建议	1. 根据丢包原因修改发包源 MAC 地址、目的 MAC 地址、目的 IP 或符合用户合法性检查规则等 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.6 ARP_DETECTION_DROP_VLAN

日志内容	ARP attack detection dropped a packet because of [STRING]. (Interface [STRING]; VLAN [STRING]; Source IP [STRING]).
日志含义	VLAN内ARP Detection检测丢包
参数解释	$1：ARP Detection丢包的类型 • sourceMacInvalidDrop：ARP 报文源 MAC 地址检查不合法丢弃 • destMacInvalidDrop：ARP 报文目的 MAC 地址检查不合法丢弃 • ipInvalidDrop：ARP 报文源和目的 IP 地址检查不合法丢弃 • ipcimNobindingDrop：ARP 报文结合用户合法性检查不通过丢弃 $2：ARP Detection丢包的接口 $3：ARP Detection丢包的VLAN ID $4：ARP Detection丢包的源IP地址
日志等级	4 (Warning)
举例	ARP/4/ARP_DETECTION_DROP_VLAN: ARP attack detection dropped a packet because of ipInvalidDrop. (Interface GigabitEthernet2/0/1; VLAN 1; Source IP 224.0.0.0).
对系统的影响	存在ARP报文因为ARP Detection功能检测被丢弃，不影响正常业务
日志产生原因	ARP Detection功能开启之后，VLAN内ARP Detection功能检测到不合法ARP报文并将其丢弃
处理建议	**1.** 根据丢包原因修改发包源 MAC 地址、目的 MAC 地址、目的 IP 或符合用户合法性检查规则等 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.7 ARP_DETECTION_DROP_VSI

日志内容	ARP attack detection dropped a packet because of [STRING]. (Interface [STRING]; Service-instance [STRING]; Source IP [STRING]).
日志含义	VSI内ARP Detection检测丢包
参数解释	$1：ARP Detection丢包的类型 • sourceMacInvalidDrop：ARP 报文源 MAC 地址检查不合法丢弃 • destMacInvalidDrop：ARP 报文目的 MAC 地址检查不合法丢弃 • ipInvalidDrop：ARP 报文源和目的 IP 地址检查不合法丢弃 • ipcimNobindingDrop：ARP 报文结合用户合法性检查不通过丢弃 $2：ARP Detection丢包的接口 $3：ARP Detection丢包的Service ID $4：ARP Detection丢包的源IP地址
日志等级	4 (Warning)
举例	ARP/4/ARP_DETECTION_DROP_VSI: ARP attack detection dropped a packet because of ipInvalidDrop. (Interface GigabitEthernet2/0/1; Service-instance 1; Source IP 224.0.0.0).
对系统的影响	存在ARP报文因为ARP Detection功能检测被丢弃，不影响正常业务
日志产生原因	ARP Detection功能开启之后，VSI内ARP Detection功能检测到不合法ARP报文并将其丢弃
处理建议	**1.** 根据丢包原因修改发包源 MAC 地址、目的 MAC 地址、目的 IP 或符合用户合法性检查规则等 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.8 ARP_DETECTION_LOG

日志内容	Detected an ARP attack on interface [STRING]: IP [STRING], MAC [STRING], VLAN [STRING]. [UINT32] packet(s) dropped.
日志含义	ARP Detection检测到ARP攻击
参数解释	$1：接口名称 $2：IP地址 $3：MAC地址 $4：VLAN ID $5：丢弃的报文数
日志等级	5 (Notification)
举例	ARP/5/ARP_DETECTION_LOG: Detected an ARP attack on interface GigabitEthernet1/0/1: IP 1.1.1.1, MAC 1-1-1, VLAN 100. 2 packet(s) dropped.
对系统的影响	不影响正常业务
日志产生原因	ARP Detection功能开启之后，接口上存在因ARP Detection功能检查引起的丢包
处理建议	**1.** 检查发送该 ARP 报文的主机的合法性，如果该主机非法，则需要断开该主机网络 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.9 ARP_DUPLICATE_IPADDR_DETECT

日志内容	Detected an IP address conflict. The device with MAC address [STRING] connected to interface [STRING] in VSI [STRING] and the device with MAC address [STRING] connected to interface [STRING] in VSI [STRING] were using the same IP address [IPADDR].
日志含义	检测到IP地址冲突
参数解释	$1：MAC地址 $2：接口名称（包括Tunnel口、三层接口和以太网服务实例等） $3：VSI名称 $4：冲突对端的源MAC地址 $5：冲突对端的源接口名称（包括Tunnel口、三层接口和以太网服务实例等） $6：冲突对端的VSI名称 $7：冲突的IP地址
日志等级	4 (Warning)
举例	ARP/4/ARP_DUPLICATE_IPADDR_DETECT: Detected an IP address conflict. The device with MAC address 00-00-01 connected to interface Ethernet0/0/1 service-instance 1000 in VSI vpna and the device with MAC address 00-00-02 connected to interface tunnel 10 in VSI vpna were using the same IP address 192.168.1.1.
对系统的影响	网络中可能存在IP地址配置冲突，可能会造成网络的路由振荡、用户业务或者流量中断等故障
日志产生原因	接口收到ARP报文中发送端的IP地址与本设备学习到的ARP表项中的IP地址冲突
处理建议	**1.** 检查网络中是否存在配置了相同 IP 地址的设备，调整冲突设备的 IP 地址 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.10 ARP_DYNAMIC

日志内容	The maximum number of dynamic ARP entries for the device reached.
日志含义	设备上学习到的动态ARP表项数量达到最大值
参数解释	无
日志等级	6 (Informational)
举例	ARP/6/ARP_DYNAMIC: The maximum number of dynamic ARP entries for the device reached.
对系统的影响	可能出现由于资源不足而无法学习到新的动态ARP表项，导致业务不通
日志产生原因	设备上学习到的动态ARP表项总数到达最大值时打印该提示日志
处理建议	**1.** 执行 **display arp**命令，查看动态ARP表项 **2.** 执行 **arp max-learning-number**命令将设备允许学习动态ARP表项的最大数目的数值调大 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.11 ARP_DYNAMIC_IF

日志内容	The maximum number of dynamic ARP entries for interface [STRING] reached.
日志含义	接口上学习到的动态ARP表项数量达到最大值
参数解释	$1：接口名
日志等级	6 (Informational)
举例	ARP/6/ARP_DYNAMIC_IF: The maximum number of dynamic ARP entries for interface GigabitEthernet1/0/1 reached.
对系统的影响	可能出现由于资源不足而无法学习到新的动态ARP表项，导致业务不通
日志产生原因	接口上学习到的动态ARP表项总数到达最大值时打印该提示日志
处理建议	1. 执行 **display arp**命令，查看指定接口上的动态ARP表项 2. 根据网络规划和业务部署，检查接口上学习到的动态 ARP 表项是否是用户必需的 o 如果动态 ARP 表项是用户必需的，请执行步骤 3 o 如果动态ARP表项不是用户必需的，在确保业务不受影响的前提下，执行 **undo arp** 命令删除指定的ARP表项 3. 执行 **arp max-learning-num**命令将指定接口允许学习动态ARP表项的最大数目的数值调大 4. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.12 ARP_DYNAMIC_SLOT

日志内容	形式一： The maximum number of dynamic ARP entries for slot [INT32] reached. 形式二： The maximum number of dynamic ARP entries for chassis [INT32] slot [INT32] reached.
日志含义	单板上学习到的动态ARP表项数量达到最大值
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	6 (Informational)
举例	ARP/6/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for slot 2 reached. ARP/6/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for chassis 1 slot 2 reached.
对系统的影响	可能出现由于资源不足而无法学习到新的动态ARP表项，导致业务不通
日志产生原因	形式一： 指定slot上学到的动态ARP表项数量达到最大值 形式二： 指定chassis内slot上学到的动态ARP表项数量达到最大值
处理建议	1. 执行 **display arp**命令，查看指定单板上的动态ARP表项 2. 根据网络规划和业务部署，检查学习到的动态 ARP 表项是否是用户必需的 o 如果动态 ARP 表项是用户必需的，请执行步骤 3 o 如果动态ARP表项不是用户必需的，在确保业务不受影响的前提下，执行 **undo arp** 命令删除指定的ARP表项 3. 执行 arp max-learning-number命令，将设备指定单板学习动态ARP表项的最大数目的数值调大 4. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.13 ARP_ENTRY_CHECK_ALARM

日志内容	The incoming ARP packet attempted to modify an existing ARP entry. (Interface [STRING]; Source MAC [STRING]; Source IP [STRING]; VLAN [STRING]; Second VLAN [STRING]; PortIfName [STRING]).
日志含义	设备收到了试图修改已有ARP表项的ARP报文
参数解释	$1：ARP表项被更新为静态ARP表项后的接口 $2：ARP表项被更新为静态ARP表项后的源MAC地址 $3：ARP表项被更新为静态ARP表项后的源IP地址 $4：ARP表项被更新为静态ARP表项后的外层VLAN $5：ARP表项被更新为静态ARP表项后的内层 VLAN $6：ARP表项被更新为静态ARP表项后的端口
日志等级	4 (Warning)
举例	ARP/4/ARP_ENTRY_CHECK_ALARM: The incoming ARP packet attempted to modify an existing ARP entry. (Interface GigabitEthernet2/0/2; Source MAC 0001-0001-0001; Source IP 3.3.3.4; VLAN 65535; Second VLAN 65535; PortIfName).
对系统的影响	网络中可能存在非法用户仿冒其它用户进行ARP欺骗攻击，从而影响业务正常运行
日志产生原因	设备收到的ARP报文中的信息与当前存在的表项内容不一致
处理建议	**1.** 检查当前 ARP 表项，分析 ARP 表项的变化是否合理 ○ 如果 ARP 表项变化是用户的合理迁移导致的，则需要更新对应的配置 ○ 如果 ARP 表项变化不合理，建议通过 MAC 地址确认该 ARP 报文的发送端，确认是否存在 ARP 攻击并采取防攻击措施 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.14 ARP_ENTRY_CONFLICT

日志内容	The software entry for [STRING] on [STRING] and the hardware entry did not have the same [STRING].
日志含义	ARP软件表项与硬件表项不一致
参数解释	$1：IP地址 $2：VPN实例名。如果该ARP属于公网，显示为the public network $3：不一致的表项参数类型 • MAC address：MAC 地址 • output interface：ARP 表项的出接口 • output port ：ARP 表项的出端口 • outermost layer VLAN ID：第一层 VLAN 标签 • second outermost layer VLAN ID：第二层 VLAN 标签 • VSI index：VSI 索引 • link ID：VSI 出链路标识符
日志等级	6 (Informational)
举例	ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.1 on the VPN a and the hardware entry did not have the same MAC address, output port, VSI index, and link ID. ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.2 on the public network and the hardware entry did not have the same MAC address, output port, VSI index, and link ID.
对系统的影响	可能造成业务流量不通或者转发到错误的端口等异常
日志产生原因	由于资源不足或者软件运行错误等异常情况造成硬件转发表项信息与内存中记录的信息存在差异
处理建议	无需处理，ARP会主动重刷硬件表项

6.15 ARP_ENTRY_ENOUGHRESOURCE

日志内容	Issued the software entry to the driver for IPv4 address [STRING] on VPN instance [STRING]. Issued the software entry to the driver for IPv4 address [STRING] on the public network.
日志含义	下发ARP软件表项到驱动刷新硬件表项
参数解释	$1：IPv4地址 $2：VPN实例名。如果该ARP属于公网，该字段不显示
日志等级	6 (Informational)
举例	ARP/6/ARP_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv4 address 10.1.1.1 on VPN instance vpn_1. ARP/6/ARP_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv4 address 10.1.1.2 on the public network.
对系统的影响	无
日志产生原因	通过**arp consistency-check enable**命令开启ARP表项一致性检查功能后，如果根据ARP软件表项刷新驱动硬件表项成功，则输出本日志
处理建议	无需处理

6.16 ARP_ENTRY_INCONSISTENT

日志内容	Inconsistent software and hardware ARP entries for IPv4 address [STRING] on VPN instance [STRING]. Inconsistent parameters: [STRING]. Inconsistent software and hardware ARP entries for IPv4 address [STRING] on the public network. Inconsistent parameters: [STRING].
日志含义	ARP软件表项与硬件表项不一致
参数解释	$1：IPv4地址 $2：VPN实例名。如果该ARP属于公网，该字段不显示 $3：不一致的表项参数类型 o MAC address：MAC 地址 o output interface：ARP 表项的出接口 o output port ：ARP 表项的出端口 o outermost layer VLAN ID：第一层 VLAN 标签 o second outermost layer VLAN ID：第二层 VLAN 标签 o VSI index：VSI 索引 o link ID：VSI 出链路标识符
日志等级	6 (Informational)
举例	ARP/6/ARP_ENTRY_INCONSISTENT: Inconsistent software and hardware ARP entries for IPv4 address 10.1.1.1 on VPN instance vpn_1. Inconsistent parameters: MAC address, output port, VSI index, and link ID. ARP/6/ARP_ENTRY_INCONSISTENT: Inconsistent software and hardware ARP entries for IPv4 address 10.1.1.2 on the public network. Inconsistent parameters: MAC address, output port, VSI index, and link ID.
对系统的影响	可能造成业务流量不通等异常
日志产生原因	通过**arp consistency-check enable**命令开启ARP表项一致性检查功能后，如果设备检测到ARP软件表项与硬件表项不一致（比如ARP表项的出接口），则输出本日志
处理建议	无需处理，ARP模块会主动根据ARP软件表项刷新驱动硬件表项

6.17 ARP_ENTRY_NORESOURCE

日志内容	Not enough hardware resources to issue the software entry to the driver for IPv4 address [STRING] on VPN instance [STRING]. Not enough hardware resources to issue the software entry to the driver for IPv4 address [STRING] on the public network.
日志含义	硬件资源不足时ARP软件表项下发驱动
参数解释	$1：IPv4地址 $2：VPN实例名。如果该ARP属于公网，该字段不显示
日志等级	6 (Informational)
举例	ARP/6/ARP_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv4 address 10.1.1.1 on VPN instance vpn_1. ARP/6/ARP_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv4 address 10.1.1.2 on the public network.
对系统的影响	无
日志产生原因	通过**arp consistency-check enable**命令开启ARP表项一致性检查功能后，当ARP软件表项下发驱动时，如果驱动没有足够的ARP硬件表项资源，则输出此日志
处理建议	无需处理，ARP模块会主动根据ARP软件表项刷新驱动硬件表项

6.18 ARP_EVENTQUE_ALERT

日志内容	The current size of the EVENT queue has reached [UINT32]. Please check the network environment.
日志含义	当前ARP事件队列长度超过4096
参数解释	$1: ARP事件队列长度
日志等级	4 (Warning)
举例	ARP/4/ARP_EVENTQUE_ALERT: The current size of the EVENT queue has reached 4096. Please check the network environment.
对系统的影响	ARP事件队列长度达到队列容量上限时会丢弃ARP事件消息，影响正常业务
日志产生原因	当ARP事件队列中ARP事件消息的个数超过4096时，系统将每隔60秒输出一次日志信息进行提示
处理建议	**1.** 检查接口上收到的 ARP 报文是否正常，如果收到异常的 ARP 报文，则通过抓包的方式检查网络中是否存在 ARP 报文攻击，查找攻击源 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.19 ARP_HARDWARE_REFRESH_NORESOURCE

日志内容	Failed to refresh the host route in FIB according to the ARP entry because the device resources are insufficient. IP address=[STRING]; VPN instance name=[STRING]; VPN instance index=[UINT16]; Interface=[STRING].
日志含义	设备资源不足导致转发表中的主机路由根据ARP表项刷新失败
参数解释	$1：ARP表项的IP地址 $2：ARP表项的VPN实例名称。如果是公网内的日志信息，则显示为Public $3：ARP表项的VPN实例索引。如果是公网内的日志信息，则显示为0 $4：ARP表项所对应的出接口名称
日志等级	4 (Warning)
举例	ARP/4/ARP_HARDWARE_REFRESH_NORESOURCE: Failed to refresh the host route in FIB according to the ARP entry because the device resources are insufficient. IP address=1.1.1.1; VPN instance name=vpn1; VPN instance index=1; Interface=GigabitEthernet1/0/1.
对系统的影响	影响正常的报文转发，导致业务不通
日志产生原因	使用**arp hardware log enable**命令开启ARP表项下发硬件日志功能后，由于硬件资源不足导致转发表中的主机路由无法成功刷新
处理建议	**1.** 请检查设备资源使用情况，删除不必要的配置 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.20 ARP_HARDWARE_SEND_NORESOURCE

日志内容	Failed to send the ARP entry to the driver because the device resources are insufficient. IP address=[STRING]; VPN instance name=[STRING]; VPN instance index=[UINT16]; Interface=[STRING].
日志含义	设备资源不足导致ARP表项下发到硬件失败
参数解释	$1：ARP表项的IP地址 $2：ARP表项的VPN实例名称。如果是公网内的日志信息，则显示为Public $3：ARP表项的VPN实例索引。如果是公网内的日志信息，则显示为0 $4：ARP表项所对应的出接口名称
日志等级	4 (Warning)
举例	ARP/4/ARP_HARDWARE_SEND_NORESOURCE: Failed to send the ARP entry to the driver because the device resources are insufficient. IP address=1.1.1.1; VPN instance name=vpn1; VPN instance index=1; Interface=GigabitEthernet1/0/1.
对系统的影响	影响正常的报文转发，导致业务不通
日志产生原因	使用**arp hardware log enable**命令开启ARP表项下发硬件日志功能后，由于硬件资源不足导致ARP表项无法成功下发到硬件
处理建议	**1.** 请检查设备资源使用情况，删除不必要的配置 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.21 ARP_HOST_IP_CONFLICT

日志内容	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IP address as the host connected to interface [STRING].
日志含义	接口收到主机ARP报文中的源IP地址与其他接口连接的主机的IP地址冲突
参数解释	$1：IP地址 $2：接口名称 $3：接口名称
日志等级	4 (Warning)
举例	ARP/4/ARP_HOST_IP_CONFLICT: The host 1.1.1.1 connected to interface GigabitEthernet1/0/1 cannot communicate correctly, because it uses the same IP address as the host connected to interface GigabitEthernet1/0/2.
对系统的影响	可能会造成用户业务或者流量中断
日志产生原因	产生此日志的可能原因包括： • 本设备下连接的不同主机配置了相同的 IP 地址 • 网络中可能存在 ARP 攻击
处理建议	**1.** 根据日志信息，检查对应接口下连接的主机配置，调整冲突主机的 IP 地址 **2.** 检查发送该 ARP 报文的主机的合法性，如果该主机非法，则需要断开该主机网络 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.22 ARP_LIPCQUE_ALERT

日志内容	The number of ARP entries in the ARP_LIPC queue has reached [UINT32]. Please check the network environment.
日志含义	在队列中等待主控板向其他板同步的ARP表项的个数达到队列容量的50%或80%
参数解释	$1：在队列中等待主控板向其他板同步的ARP表项的个数
日志等级	4 (Warning)
举例	ARP/4/ARP_LIPCQUE_ALERT: The number of ARP entries in the ARP_LIPC queue has reached 65. Please check the network environment.
对系统的影响	在队列中等待主控板向其他板同步的ARP表项个数达到队列容量的上限时会丢弃ARP表项，可能导致部分正常的ARP报文被丢弃，造成流量转发不通
日志产生原因	在队列中等待主控板向其他板同步的ARP表项的个数达到队列容量的50%或80%时会触发告警，系统将每隔60秒输出一次日志信息进行提示，可能原因包括： • 网络中可能存在环路 • 网络中可能存在 ARP 攻击
处理建议	**1.** 配置 STP，检查网络中是否存在环路 **2.** 通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.23 ARP_LOCALPROXY_ENABLE_FAILED

日志内容	Failed to enable local proxy ARP on interface [STRING].
日志含义	使能本地代理ARP功能失败
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ARP/4/ARP_LOCALPROXY_ENABLE_FAILED: Failed to enable local proxy ARP on interface VSI-interface 1.
对系统的影响	可能会造成用户业务或者流量中断
日志产生原因	产生此日志的可能原因包括： • 接口上使能本地代理 ARP 功能失败 • 主控板使能本地代理 ARP 功能成功、非主控板使能本地代理 ARP 功能失败时，在相应非主控板打印该提示日志
处理建议	1. 检查设备相应单板是否支持配置本地代理 ARP 功能 2. 检查设备的硬件资源是否充足，删除不必要的配置 3. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.24 ARP_MAC_MISMATCH_ALARM

日志内容	IP address [STRING]: The MAC address [STRING] of the configured static ARP is inconsistent with the actual MAC address [STRING].
日志含义	静态ARP表项的MAC地址与实际ARP报文的源MAC地址不一致
参数解释	$1：静态ARP表项的IP地址 $2：静态ARP表项的MAC地址 $3：实际ARP报文的源MAC地址
日志等级	4 (Warning)
举例	ARP/4/ARP_MAC_MISMATCH_ALARM: IP address 192.168.56.1: The MAC address 0001-0001-0001 of the configured static ARP is inconsistent with the actual MAC address 0a00-2700-000f.
对系统的影响	短静态ARP表项会无法解析成功，可能影响业务正常运行
日志产生原因	使用**`snmp-agent trap enable arp mac-mismatch`**命令开启ARP MAC地址不一致的告警功能后，设备上配置的静态ARP表项的MAC地址和用户实际的MAC地址不一致

处理建议	1. 检查该 ARP 报文中的源 MAC 地址是否是用户正确的 MAC 地址
	  ○ 如果是用户正确的 MAC 地址，则修改静态 ARP 表项的 MAC 地址与实际 ARP 报文的源 MAC 地址一致
	  ○ 如果不是用户正确的 MAC 地址，则认为收到的该 ARP 报文是非法报文，无需处理
	2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.25 ARP_MAC_MISMATCH_CLEAR

日志内容	IP address [STRING]: The MAC address [STRING] of the configured static ARP is consistent with the actual MAC address.
日志含义	静态ARP表项的MAC地址与实际ARP报文的源MAC地址一致
参数解释	$1：静态ARP表项的IP地址 $2：静态ARP表项的MAC地址
日志等级	5 (Notification)
举例	ARP/5/ARP_MAC_MISMATCH_CLEAR: IP address 192.168.56.1: The MAC address 0a00-2700-000f of the configured static ARP is consistent with the actual MAC address.
对系统的影响	短静态ARP成功解析，业务正常运行
日志产生原因	ARP MAC地址不一致告警恢复，静态ARP表项的MAC地址与实际ARP报文的源MAC地址从不一致转变为一致
处理建议	无需处理

6.26 ARP_PKTQUE_ALERT

日志内容	The current size of the ARP_PKT queue has reached [UINT32]. Please check the network environment.
日志含义	当前ARP报文队列长度超过4096
参数解释	$1: ARP报文队列长度
日志等级	6 (Informational)
举例	ARP/6/ARP_PKTQUE_ALERT: The current size of the ARP_PKT queue has reached 4096. Please check the network environment.
对系统的影响	当上送CPU的ARP报文队列长度达到队列容量上限时会丢弃ARP报文，造成流量转发不通
日志产生原因	当上送CPU的ARP报文队列长度超过4096时，系统将每隔60秒输出一次日志信息进行提示
处理建议	**1.** 检查接口上收到的 ARP 报文是否正常，如果收到异常的 ARP 报文，则通过抓包的方式检查网络中是否存在 ARP 报文攻击，查找攻击源 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.27 ARP_RATE_EXCEEDED

日志内容	The ARP packet rate ([UINT32] pps) exceeded the rate limit ([UINT32] pps) on interface [STRING] in the last [UINT32] seconds.
日志含义	ARP报文速率超过了接口限速速率
参数解释	$1：ARP报文速率 $2：ARP报文限速速率 $3：接口名称 $4：间隔时间
日志等级	4 (Warning)
举例	ARP/4/ARP_RATE_EXCEEDED: The ARP packet rate (100 pps) exceeded the rate limit (80 pps) on interface Ethernet0/1/0 in the last 10 seconds.
对系统的影响	接口上的ARP报文速率超过ARP限速速率时会被丢弃，可能影响正常的ARP学习与应答，造成流量转发不通
日志产生原因	接口上的ARP报文速率超过了接口的ARP限速速率
处理建议	**1.** 检查接口上收到的 ARP 报文是否正常 ○ 如果收到的ARP报文均合理，则执行 **arp rate-limit**命令将指定接口上ARP报文限速速率的数值调大 ○ 如果检查到收到异常的 ARP 报文，请执行步骤 2 **2.** 通过抓包的方式检查网络中是否存在 ARP 报文攻击，查找攻击源 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.28 ARP_RATELIMIT_NOTSUPPORT

日志内容	形式一： ARP packet rate limit is not support on slot [INT32]. 形式二： ARP packet rate limit is not support on chassis [INT32] slot [INT32].
日志含义	不支持ARP报文限速功能
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	6 (Informational)
举例	ARP/6/ARP_RATELIMIT_NOTSUPPORT: ARP packet rate limit is not support on slot 2.
对系统的影响	无
日志产生原因	形式一： 指定slot不支持ARP报文限速功能 形式二： 指定chassis内slot不支持ARP报文限速功能
处理建议	无需处理

6.29 ARP_SENDER_IP_INVALID

日志内容	Sender IP [STRING] was not on the same network as the receiving interface [STRING].
日志含义	ARP报文发送端IP地址和接口不在同一网段
参数解释	$1：IP地址 $2：接口名称
日志等级	6 (Informational)
举例	ARP/6/ARP_SENDER_IP_INVALID: Sender IP 192.168.10.2 was not on the same network as the receiving interface GigabitEthernet1/0/1.
对系统的影响	网络中可能存在ARP攻击，影响设备正常运行
日志产生原因	产生此日志的可能原因包括： • ARP 报文发送端 IP 地址配置错误，与对应接口不在同一网段 • 发送该 ARP 报文的主机不合法，网络中可能存在 ARP 攻击
处理建议	1. 检查该 ARP 报文发送端 IP 地址对应主机的合法性 o 如果该主机非法，则需要断开该主机网络 o 如果该主机合法，则在确保业务不受影响的前提下，调整主机和对应接口的 IP 地址在相同网段 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.30 ARP_SENDER_MAC_INVALID

日志内容	Sender MAC [STRING] was not identical to Ethernet source MAC [STRING] on interface [STRING].
日志含义	ARP报文中的发送端MAC地址和接口收到ARP报文的以太网数据帧首部中的源MAC地址不一致
参数解释	$1：MAC地址 $2：MAC地址 $3：接口名称
日志等级	6 (Informational)
举例	ARP/6/ARP_SENDER_MAC_INVALID: Sender MAC 0000-5E14-0E00 was not identical to Ethernet source MAC 0000-5C14-0E00 on interface GigabitEthernet1/0/1.
对系统的影响	网络中可能存在ARP攻击，影响设备正常运行
日志产生原因	发送该ARP报文的主机不合法，网络中可能存在ARP攻击
处理建议	1. 检查该 ARP 报文发送端 MAC 地址对应主机的合法性，如果该主机非法，则需要断开该主机网络 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.31 ARP_SENDER_SMACCONFLICT

日志内容	Packet was discarded because its sender MAC address was the MAC address of the receiving interface. Interface: [STRING], sender IP: [STRING], target IP: [STRING].
日志含义	ARP报文因发送端MAC地址和接口MAC地址冲突而丢弃
参数解释	$1：接口名称 $2：发送端IP地址 $3：目标IP地址
日志等级	6 (Informational)
举例	ARP/6/ARP_SENDER_SMACCONFLICT: Packet was discarded because its sender MAC address was the MAC address of the receiving interface. Interface: GigabitEthernet1/0/1 sender IP: 1.1.2.2 target IP: 1.1.2.1,
对系统的影响	可能造成用户业务中断
日志产生原因	ARP报文中的发送端MAC地址和接收报文的接口MAC地址冲突，可能原因包括： • 网络中可能存在终端的 MAC 地址与该接口的 MAC 地址相同 • 网络中可能存在环路
处理建议	1. 配置 STP，检查网络中是否存在环路 2. 检查网络中是否存在 MAC 地址相同的设备 o 如果能确定 MAC 地址冲突的设备，在确保业务不受影响的前提下，调整冲突设备的 MAC 地址 o 如果不能确定 MAC 地址冲突的设备，在确保业务不受影响的前提下，调整对应接口的 MAC 地址 3. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.32 ARP_SENDER_SMACCONFLICT_VSI

日志内容	Packet was discarded because its sender MAC address was the MAC address of the receiving interface. Interface: [STRING], sender IP: [STRING], target IP: [STRING],VSI index: [UINT32], link ID: [UINT32].
日志含义	ARP报文因发送端MAC地址和VSI接口MAC地址冲突而丢弃
参数解释	$1：接口名称 $2：发送端IP地址 $3：目标IP地址 $4：VSI索引 $5：link ID
日志等级	6 (Informational)
举例	ARP/6/ ARP_SENDER_SMACCONFLICT_VSI: Packet was discarded because its sender MAC address was the MAC address of the receiving interface. Interface: VSI3 sender IP: 1.1.2.2 target IP: 1.1.2.1, VSI Index: 2, Link ID: 0
对系统的影响	可能造成用户业务中断
日志产生原因	ARP报文中的发送端MAC地址和接收报文的VSI接口的MAC地址冲突，可能原因包括： • 网络中可能存在终端的 MAC 地址与该接口的 MAC 地址相同 • 网络中可能存在环路
处理建议	**1.** 配置 STP，检查网络中是否存在环路 **2.** 检查网络中是否存在 MAC 地址相同的设备 o 如果能确定 MAC 地址冲突的设备，在确保业务不受影响的前提下，调整冲突设备的 MAC 地址 o 如果不能确定 MAC 地址冲突的设备，在确保业务不受影响的前提下，调整对应接口的 MAC 地址 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.33 ARP_SOURCE_SUPPRESSION

日志内容	The number of unresolvable IP packets received on interface [STRING] from IP address [STRING] exceeded the ARP source suppression threshold [UINT32].
日志含义	接口收到从某IP地址发送的不能解析的IP报文数量超过了ARP源抑制的阈值
参数解释	$1：收到目的IP地址不能解析的IP报文接口名称 $2：目的IP地址不能解析的IP报文的源IP地址 $3：ARP源抑制的报文数阈值
日志等级	4 (Warning)
举例	ARP/4/ARP_SOURCE_SUPPRESSION: The number of unresolvable IP packets received on interface GE1/0/1 from IP address 10.1.1.20 exceeded the ARP source suppression threshold 10.
对系统的影响	不影响正常业务
日志产生原因	ARP源抑制功能开启后，网络中每5秒内从某IP地址向设备某接口发送目的IP地址不能解析的IP报文超过了设置的阈值，产生此日志的可能原因包括： • 网络中存在 IP 报文攻击 • 网络链路存在故障
处理建议	1. 通过 IP 或者 ARP 相关报文调试手段确认被抑制报文的目的 IP 地址，检查该目的 IP 地址是否有效，以此判断是网络故障还是遭到攻击 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.34 ARP_SOURCE_IP

日志内容	An attack from IP [STRING] was detected on interface [STRING].
日志含义	检测到源IP地址固定的ARP攻击
参数解释	$1：收到的ARP攻击报文中的源IP地址 $2：收到源IP地址固定的ARP报文的接口名称
日志等级	6 (Information)
举例	ARP/6/ARP_SOURCE_IP: An attack from IP 1.1.1.1 was detected on interface GE1/0/1.
对系统的影响	设备处理大量源IP地址固定的ARP报文会造成CPU繁忙，影响正常的业务处理
日志产生原因	在固定的时间（5秒）内，某个接口收到的同一源IP地址的ARP报文个数超过检测阈值

处理建议	1. 执行 **display arp source-ip**命令，查看检测到的源IP地址固定的ARP攻击检测表项，根据网络规划和业务部署，确认表项中该地址是否为用户信任的IP地址
	  ○ 如果是，则执行 **arp source-ip exclude-ip**命令配置该地址为ARP攻击检测的保护IP地址
	  ○ 如果不是，则通过抓包的方式检查网络中是否存在 ARP 报文攻击，查找攻击源
	2. 若问题仍未解决，请收集配置文件和日志信息，并联系技术支持

6.35 ARP_SRC_MAC_FOUND_ATTACK

日志内容	An attack from MAC [STRING] was detected on interface [STRING].
日志含义	接口检测到源MAC地址固定的ARP攻击
参数解释	$1：MAC地址 $2：接口名称
日志等级	6 (Informational)
举例	ARP/6/ARP_SRC_MAC_FOUND_ATTACK: An attack from MAC 0000-5E14-0E00 was detected on interface GigabitEthernet1/0/1.
对系统的影响	部分正常的ARP报文可能被丢弃，影响正常业务
日志产生原因	源MAC地址固定的ARP攻击检测功能检测到攻击。5秒内，收到同一源MAC地址（源MAC地址固定）的ARP报文超过一定的阈值
处理建议	1. 检查该源 MAC 地址对应主机的合法性 o 如果该主机合法，则执行 **arp source-mac exclude-mac**命令将该MAC地址配置为保护MAC地址 o 如果该主机非法，则需要断开该主机网络或者执行 **arp source-mac filter** 命令将源MAC地址固定的ARP攻击检测功能的检查模式配置为过滤模式 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.36 ARP_SUP_ENABLE_FAILED

日志内容	Failed to enable ARP flood suppression on VSI [STRING].
日志含义	在VSI内开启ARP泛洪抑制功能失败
参数解释	$1：VSI名称
日志等级	4 (Warning)
举例	ARP/4/ARP_SUP_ENABLE_FAILED: Failed to enable ARP flood suppression on VSI vpna.
对系统的影响	可能导致ARP表项溢出，无法缓存正常用户的ARP表项，从而影响正常的报文转发
日志产生原因	产生此日志的可能原因包括： • 设备不支持在 VSI 内开启 ARP 泛洪抑制功能 • 设备硬件资源不足
处理建议	1. 检查设备是否支持在 VSI 内配置 ARP 泛洪抑制功能 2. 检查设备的硬件资源是否充足，删除不必要的配置 3. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.37 ARP_SUPPR_ALARM_CLEAR

日志内容	The number of ARP suppression entries dropped below the threshold. Threshold=[UINT32]; Number of Suppression ARP entries=[UINT32].

日志含义	ARP泛洪抑制表项数量降到了阈值以下
参数解释	$1：ARP泛洪抑制表的告警阈值 $2：设备ARP泛洪抑制表的数量
日志等级	5 (Notification)
举例	ARP/5/ARP_SUPPR_ALARM_CLEAR: The number of ARP suppression entries dropped below the threshold. Threshold=100; Number of Suppression ARP entries=59.
对系统的影响	无
日志产生原因	设备ARP泛洪抑制表的数目恢复到安全阈值之下。ARP泛洪抑制的安全阈值=产品定制的抑制表项规格×60%
处理建议	无需处理

6.38 ARP_SUPPR_THRESHOLD_EXCEED

日志内容	The number of ARP suppression entries exceeded the threshold. Threshold=[UINT32]; Number of ARP Suppression entries=[UINT32].
日志含义	Arp泛洪抑制表项数量超过了阈值
参数解释	$1：ARP泛洪抑制表的告警阈值 $2：设备当前ARP泛洪抑制表的数量
日志等级	4 (Warning)
举例	ARP/4/ARP_SUPPR_THRESHOLD_EXCEED: The number of ARP suppression entries exceeded the threshold. Threshold=100; Number of ARP Suppression entries=81.
对系统的影响	可能出现由于资源不足而无法学习到新的ARP泛洪抑制表项，导致正常业务中断
日志产生原因	设备ARP泛洪抑制表大于告警阈值。ARP泛洪抑制的告警阈值=产品定制的抑制表项规格×80%
处理建议	1. 执行 **display arp suppression xconnect-group**命令，查看ARP泛洪抑制表项 2. 根据网络规划和业务部署，检查设备上的 ARP 泛洪抑制表项是否是用户必需的 o 如果 ARP 泛洪抑制表项是用户必需的，请执行步骤 3 o 如果ARP泛洪抑制表项不是用户必需的，执行 **reset arp suppression xconnect-group**命令清除ARP泛洪抑制表项 3. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.39 ARP_TARGET_IP_INVALID

日志内容	Target IP [STRING] was not the IP of the receiving interface [STRING].
日志含义	接口IP地址与收到ARP报文中的目标IP地址不一致
参数解释	$1：IP地址 $2：接口名称
日志等级	6 (Informational)
举例	ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.10.2 was not the IP of the receiving interface GigabitEthernet1/0/1.
对系统的影响	网络中可能存在ARP攻击，影响设备正常运行
日志产生原因	发送该ARP报文的主机不合法，网络中可能存在ARP攻击
处理建议	1. 检查收到的 ARP 报文是否为 ARP 广播报文 o 如果是，则为正常现象，无需处理 o 如果不是，则请执行步骤 2 2. 检查发送该 ARP 报文的主机的合法性，如果该主机非法，则需要断开该主机网络 3. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.40 ARP_THRESHOLD_REACHED

日志内容	The alarm threshold for dynamic ARP entry learning was reached on interface [STRING].
日志含义	接口上学习到的动态ARP表项数量达到告警阈值
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ARP/4/ARP_THRESHOLD_REACHED: The alarm threshold for dynamic ARP entry learning was reached on interface GigabitEthernet1/0/1
对系统的影响	可能会出现由于资源不足而无法学习到新的ARP表项，导致业务不通
日志产生原因	当前接口上学习的动态ARP表项的数量达到了告警阈值
处理建议	1. 执行 **display arp**命令，查看指定接口上的动态ARP表项 2. 根据网络规划和业务部署，检查接口上学习到的动态 ARP 表项是否是用户必需的 o 如果动态 ARP 表项是用户必需的，请执行步骤 3 o 如果动态ARP表项不是用户必需的，在确保业务不受影响的前提下，执行 **undo arp**命令删除指定的ARP表项 3. 通过抓包的方式检查网络中是否存在 ARP 报文攻击，查找攻击源 4. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.41 ARP_USER_DUPLICATE_IPADDR_DETECT

日志内容	Detected a user IP address conflict. New user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] and old user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] were using the same IP address [IPADDR].
日志含义	检测到终端用户间IP地址冲突
参数解释	$1：新用户的MAC地址 $2：新用户所在的外层VLAN $3：新用户所在的内层VLAN $4：连接新用户的接口名称 $5：旧用户的MAC地址 $6：旧用户所在的外层VLAN $7：旧用户所在的内层VLAN $8：连接旧用户的接口名称 $9：终端用户的IP地址
日志等级	6 (Informational)
举例	ARP/6/ARP_USER_DUPLICATE_IPADDR_DETECT: Detected a user IP address conflict. New user (MAC 0010-2100-01e1, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 and old user (MAC 0120-1e00-0102, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 were using the same IP address 192.168.1.1.
对系统的影响	网络中可能存在冲突的IP地址，可能会造成用户业务或者流量中断等故障
日志产生原因	新用户的IP地址和某个旧用户的IP地址相同
处理建议	排查所有终端用户的IP地址，调整冲突用户的IP地址，解决IP地址冲突问题

6.42 ARP_USER_MOVE_DETECT

日志内容	Detected a user (IP address [IPADDR], MAC address [STRING]) moved to another interface. Before user move: interface [STRING], SVLAN [STRING], CVLAN [STRING]. After user move: interface [STRING], SVLAN [STRING], CVLAN [STRING].
日志含义	检测到用户进行了端口迁移
参数解释	$1：迁移用户的IP地址 $2：迁移用户的MAC地址 $3：迁移前接口名称 $4：迁移前用户所在的外层VLAN $5：迁移前用户所在的内层VLAN $6：迁移后接口名称 $7：迁移后用户所在的外层VLAN $8：迁移后用户所在的内层VLAN
日志等级	6 (Informational)
举例	ARP/6/ARP_USER_MOVE_DETECT: Detected a user (IP address 192.168.1.1, MAC address 0010-2100-01e1) moved to another interface. Before user move: interface GigabitEthernet1/0/1, SVLAN 100, CVLAN 10. After user move: interface GigabitEthernet1/0/2, SVLAN 100, CVLAN 10.
对系统的影响	可能造成用户业务中断。当发生大量用户迁移操作时，可能会降低设备性能
日志产生原因	开启ARP记录终端用户端口迁移功能后，终端用户发生接口迁移动作
处理建议	1. 使用 **display arp user-move record**命令查看终端用户迁移信息，检查迁移是否合理 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.43 DUPIFIP

日志内容	Duplicate address [STRING] on interface [STRING], sourced from [STRING].
日志含义	ARP报文发送端IP地址与接口IP地址重复
参数解释	$1：IP地址 $2：接口名称 $3：MAC地址
日志等级	6 (Informational)
举例	ARP/6/DUPIFIP: Duplicate address 1.1.1.1 on interface GigabitEthernet1/0/1, sourced from 0015-E944-A947.
对系统的影响	可能造成用户业务中断
日志产生原因	网络中存在其他设备配置的IP地址与本接口IP地址相同
处理建议	1. 检查网络中是否存在其他设备配置了与本接口相同的 IP 地址，调整冲突设备的 IP 地址 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.44 DUPIP

日志内容	IP address [STRING] conflicted with global or imported IP address, sourced from [STRING].
日志含义	ARP报文发送端IP地址与全局或导入的IP地址冲突
参数解释	$1：IP地址 $2：MAC地址
日志等级	6 (Informational)
举例	ARP/6/DUPIP: IP address 30.1.1.1 conflicted with global or imported IP address, sourced from 0000-0000-0001.
对系统的影响	可能造成用户业务中断
日志产生原因	网络中存在其他设备配置的IP地址与本设备全局或导入的IP地址相同
处理建议	**1.** 检查网络中是否存在其他设备配置了与本设备相同的 IP 地址，调整冲突设备的 IP 地址 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

6.45 DUPVRRPIP

日志内容	IP address [STRING] conflicted with VRRP virtual IP address on interface [STRING], sourced from [STRING].
日志含义	ARP报文发送端IP地址与VRRP虚拟IP地址冲突
参数解释	$1：IP地址 $2：接口名称 $3：MAC地址
日志等级	6 (Informational)
举例	ARP/6/DUPVRRPIP: IP address 1.1.1.1 conflicted with VRRP virtual IP address on interface GigabitEthernet1/0/1, sourced from 0015-E944-A947.
对系统的影响	可能造成用户业务中断
日志产生原因	网络中存在其他设备配置的IP地址与本设备VRRP虚拟IP地址相同
处理建议	**1.** 检查网络中是否存在其他设备配置的 IP 地址与本设备 VRRP 虚拟 IP 地址相同，调整冲突设备的 IP 地址 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

7 ATK

本节介绍 ATK 模块输出的日志信息。

7.1 ATK_ICMP_ADDRMASK_REQ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=17;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码请求报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.2 ATK_ICMP_ADDRMASK_REQ_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP地址掩码请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=17;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码请求报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码请求报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP地址掩码请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=17;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码请求报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码请求报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.4 ATK_ICMP_ADDRMASK_REQ_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP地址掩码请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=17;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码请求报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.5 ATK_ICMP_ADDRMASK_RPL

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP地址掩码应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=18;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码应答报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.6 ATK_ICMP_ADDRMASK_RPL_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP地址掩码应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=18;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码应答报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码应答报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP地址掩码应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=18;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码应答报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码应答报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.8 ATK_ICMP_ADDRMASK_RPL_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP地址掩码应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=18;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP地址掩码应答报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.9 ATK_ICMP_ECHO_REQ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=8;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.10 ATK_ICMP_ECHO_REQ_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=8;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文首包触发日志；日志聚合开关关闭，每个ICMP请求回显报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.11 ATK_ICMP_ECHO_REQ_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=8;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文首包触发日志；日志聚合开关关闭，每个ICMP请求回显报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.12 ATK_ICMP_ECHO_REQ_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=8;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.13 ATK_ICMP_ECHO_RPL

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=0;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP回显应答报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.14 ATK_ICMP_ECHO_RPL_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=0;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP回显应答报文首包触发日志；日志聚合开关关闭，每个ICMP回显应答报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.15 ATK_ICMP_ECHO_RPL_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=0;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP回显应答报文首包触发日志；日志聚合开关关闭，每个ICMP回显应答报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.16 ATK_ICMP_ECHO_RPL_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_ECHO_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=0;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP回显应答报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.17 ATK_ICMP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到ICMP报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的ICMP报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ICMP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.18 ATK_ICMP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到ICMP报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的ICMP报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ICMP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.19 ATK_ICMP_INFO_REQ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP信息请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=15;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息请求的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.20 ATK_ICMP_INFO_REQ_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP信息请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=15;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息请求的报文首包触发日志；日志聚合开关关闭，每个ICMP信息请求的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.21 ATK_ICMP_INFO_REQ_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP信息请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=15;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息请求的报文首包触发日志；日志聚合开关关闭，每个ICMP信息请求的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.22 ATK_ICMP_INFO_REQ_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP信息请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=15;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息请求的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.23 ATK_ICMP_INFO_RPL

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP信息应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=16;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息应答的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.24 ATK_ICMP_INFO_RPL_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP信息应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=16;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息应答的报文首包触发日志；日志聚合开关关闭，每个ICMP信息应答的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.25 ATK_ICMP_INFO_RPL_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP信息应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=16;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息应答的报文首包触发日志；日志聚合开关关闭，每个ICMP信息应答的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.26 ATK_ICMP_INFO_RPL_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP信息应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_INFO_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=16;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP信息应答的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.27 ATK_ICMP_LARGE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP超大报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_LARGE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超大报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.28 ATK_ICMP_LARGE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP超大报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_LARGE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超大报文首包触发日志；日志聚合开关关闭，每个ICMP超大报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.29 ATK_ICMP_LARGE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP超大报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_LARGE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超大报文首包触发日志；日志聚合开关关闭，每个ICMP超大报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.30 ATK_ICMP_LARGE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP超大报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_LARGE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超大报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.31 ATK_ICMP_PARAPROBLEM

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP参数错误的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_PARAPROBLEM:SubModule(1127)=SINGLE;IcmpType(1062)=12;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP参数错误的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.32 ATK_ICMP_PARAPROBLEM_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP参数错误的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=12;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP参数错误的报文首包触发日志；日志聚合开关关闭，每个ICMP参数错误的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.33 ATK_ICMP_PARAPROBLEM_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP参数错误的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=12;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP参数错误的报文首包触发日志；日志聚合开关关闭，每个ICMP参数错误的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.34 ATK_ICMP_PARAPROBLEM_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP参数错误的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_PARAPROBLEM_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=12;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP参数错误的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.35 ATK_ICMP_PINGOFDEATH

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP标志位异常的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_PINGOFDEATH:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，标志位设置为最后一片并且(IPoffset*8)+(IPdatalenth)>65535的ICMP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.36 ATK_ICMP_PINGOFDEATH_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP标志位异常的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，标志位设置为最后一片并且(IPoffset*8)+(IPdatalenth)>65535的ICMP报文首包触发日志；日志聚合开关关闭，每个标志位设置为最后一片并且(IPoffset*8)+(IPdatalenth)>65535的ICMP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.37 ATK_ICMP_PINGOFDEATH_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP标志位异常的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，标志位设置为最后一片并且(IPoffset*8)+(IPdatalenth)>65535的ICMP报文首包触发日志；日志聚合开关关闭，每个标志位设置为最后一片并且(IPoffset*8)+(IPdatalenth)>65535的ICMP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.38 ATK_ICMP_PINGOFDEATH_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP标志位异常的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_PINGOFDEATH_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，标志位设置为最后一片并且(IPoffset*8)+(IPdatalenth)>65535的ICMP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.39 ATK_ICMP_REDIRECT

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP重定向报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_REDIRECT:SubModule(1127)=SINGLE;IcmpType(1062)=5;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP重定向报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.40 ATK_ICMP_REDIRECT_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP重定向报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_REDIRECT_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=5;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP重定向报文首包触发日志；日志聚合开关关闭，每个ICMP重定向报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.41 ATK_ICMP_REDIRECT_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP重定向报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_REDIRECT_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=5;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP重定向报文首包触发日志；日志聚合开关关闭，每个ICMP重定向报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.42 ATK_ICMP_REDIRECT_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP重定向报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_REDIRECT_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=5;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP重定向报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.43 ATK_ICMP_SMURF

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP请求回显报文目的地址异常的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_SMURF:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.44 ATK_ICMP_SMURF_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP请求回显报文目的地址异常的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_SMURF_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文首包触发日志 日志聚合开关关闭，符合上述条件的ICMP请求回显报文，每个报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.45 ATK_ICMP_SMURF_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP请求回显报文目的地址异常的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_SMURF_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文首包触发日志 日志聚合开关关闭，符合上述条件的ICMP请求回显报文，每个报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.46 ATK_ICMP_SMURF_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP请求回显报文目的地址异常的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_ICMP_SMURF_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.47 ATK_ICMP_SOURCEQUENCH

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP源端被关闭的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_SOURCEQUENCH:SubModule(1127)=SINGLE;IcmpType(1062)=4;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP源端被关闭的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.48 ATK_ICMP_SOURCEQUENCH_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP源端被关闭的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=4;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP源端被关闭的报文首包触发日志；日志聚合开关关闭，每个ICMP源端被关闭的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP源端被关闭的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=4;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP源端被关闭的报文首包触发日志；日志聚合开关关闭，每个ICMP源端被关闭的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.50 ATK_ICMP_SOURCEQUENCH_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP源端被关闭的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=4;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP源端被关闭的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.51 ATK_ICMP_TIMEEXCEED

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP超时的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TIMEEXCEED:SubModule(1127)=SINGLE;IcmpType(1062)=11;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超时的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.52 ATK_ICMP_TIMEEXCEED_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP超时的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=11;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超时的报文首包触发日志；日志聚合开关关闭，每个ICMP超时的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.53 ATK_ICMP_TIMEEXCEED_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP超时的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=11;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超时的报文首包触发日志；日志聚合开关关闭，每个ICMP超时的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.54 ATK_ICMP_TIMEEXCEED_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP超时的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TIMEEXCEED_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=11;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP超时的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.55 ATK_ICMP_TRACEROUTE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP类型为11且代码为0的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMP_TRACEROUTE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为11且代码为0的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.56 ATK_ICMP_TRACEROUTE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP类型为11且代码为0的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMP_TRACEROUTE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为11且代码为0的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为11且代码为0的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.57 ATK_ICMP_TRACEROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP类型为11且代码为0的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMP_TRACEROUTE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为11且代码为0的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为11且代码为0的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.58 ATK_ICMP_TRACEROUTE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP类型为11且代码为0的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMP_TRACEROUTE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为11且代码为0的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.59 ATK_ICMP_TSTAMP_REQ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP时间戳请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=13;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳请求的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.60 ATK_ICMP_TSTAMP_REQ_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP时间戳请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=13;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳请求的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳请求的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP时间戳请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=13;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳请求的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳请求的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.62 ATK_ICMP_TSTAMP_REQ_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP时间戳请求报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=13;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳请求的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.63 ATK_ICMP_TSTAMP_RPL

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP时间戳应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=14;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳应答的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.64 ATK_ICMP_TSTAMP_RPL_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP时间戳应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=14;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳应答的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳应答的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP时间戳应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=14;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳应答的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳应答的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.66 ATK_ICMP_TSTAMP_RPL_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP时间戳应答报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=14;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP时间戳应答的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.67 ATK_ICMP_TYPE

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TYPE:SubModule(1127)=SINGLE;IcmpType(1062)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP用户自定义类型的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.68 ATK_ICMP_TYPE_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TYPE_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMP用户自定义类型的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.69 ATK_ICMP_TYPE_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TYPE_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMP用户自定义类型的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.70 ATK_ICMP_TYPE_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_TYPE_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP用户自定义类型的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.71 ATK_ICMP_UNREACHABLE

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_UNREACHABLE:SubModule(1127)=SINGLE;IcmpType(1062)=3;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP目的不可达的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.72 ATK_ICMP_UNREACHABLE_RAW

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=3;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMP目的不可达的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.73 ATK_ICMP_UNREACHABLE_RAW_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMP目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=3;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMP目的不可达的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.74 ATK_ICMP_UNREACHABLE_SZ

日志内容	SubModule(1127)=[STRING];IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMP_UNREACHABLE_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=3;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP目的不可达的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.75 ATK_ICMPV6_DEST_UNREACH

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6目的不可达的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.76 ATK_ICMPV6_DEST_UNREACH_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMPV6目的不可达的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMPV6目的不可达的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.78 ATK_ICMPV6_DEST_UNREACH_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6目的不可达的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6目的不可达的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.79 ATK_ICMPV6_ECHO_REQ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_REQ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6请求回显的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.80 ATK_ICMPV6_ECHO_REQ_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6请求回显的报文首包触发日志；日志聚合开关关闭，每个ICMPV6请求回显的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6请求回显的报文首包触发日志；日志聚合开关关闭，每个ICMPV6请求回显的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.82 ATK_ICMPV6_ECHO_REQ_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6请求回显报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6请求回显的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.83 ATK_ICMPV6_ECHO_RPL

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_RPL:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6回显应答的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.84 ATK_ICMPV6_ECHO_RPL_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6回显应答的报文首包触发日志；日志聚合开关关闭，每个ICMPV6回显应答的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6回显应答的报文首包触发日志；日志聚合开关关闭，每个ICMPV6回显应答的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.86 ATK_ICMPV6_ECHO_RPL_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6回显应答报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6回显应答的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.87 ATK_ICMPV6_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到ICMPV6报文攻击
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_ICMPV6_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1007)=2002::2;DstPort(1008)=22;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的ICMPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ICMPv6 flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.88 ATK_ICMPV6_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到ICMPV6报文攻击
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_ICMPV6_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1007)=2002::2;DstPort(1008)=22;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的ICMPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ICMPv6 flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.89 ATK_ICMPV6_GROUPQUERY

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6组播侦听者查询的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPQUERY:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者查询的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.90 ATK_ICMPV6_GROUPQUERY_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6组播侦听者查询的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者查询的报文首包触发日志；日志聚合开关关闭，每个ICMPV6组播侦听者查询的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6组播侦听者查询的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者查询的报文首包触发日志；日志聚合开关关闭，每个ICMPV6组播侦听者查询的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.92 ATK_ICMPV6_GROUPQUERY_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6组播侦听者查询的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者查询的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.93 ATK_ICMPV6_GROUPREDUCTION

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6组播侦听者Done的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者Done的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.94 ATK_ICMPV6_GROUPREDUCTION_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6组播侦听者Done的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者Done的报文首包触发日志；日志聚合开关关闭，每个ICMPV6组播侦听者Done的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6组播侦听者Done的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者Done的报文首包触发日志；日志聚合开关关闭，每个ICMPV6组播侦听者Done的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.96 ATK_ICMPV6_GROUPREDUCTION_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6组播侦听者Done的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者Done的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.97 7ATK_ICMPV6_GROUPREPORT

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6组播侦听者报告的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREPORT:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者报告的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.98 ATK_ICMPV6_GROUPREPORT_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6组播侦听者报告的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者报告的报文首包触发日志；日志聚合开关关闭，每个ICMPV6组播侦听者报告的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6组播侦听者报告的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者报告的报文首包触发日志；日志聚合开关关闭，每个ICMPV6组播侦听者报告的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.100 ATK_ICMPV6_GROUPREPORT_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6组播侦听者报告的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6组播侦听者报告的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.101 ATK_ICMPV6_LARGE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6超长报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_LARGE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超长报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.102 ATK_ICMPV6_LARGE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6超长报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_LARGE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超长报文首包触发日志；日志聚合开关关闭，每个ICMPV6超长报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.103 ATK_ICMPV6_LARGE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6超长报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_LARGE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超长报文首包触发日志；日志聚合开关关闭，每个ICMPV6超长报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.104 ATK_ICMPV6_LARGE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6超长报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_LARGE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超长报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.105 ATK_ICMPV6_PACKETTOOBIG

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6数据超长报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6数据超长的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.106 ATK_ICMPV6_PACKETTOOBIG_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6数据超长报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6数据超长的报文首包触发日志；日志聚合开关关闭，每个ICMPV6数据超长的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6数据超长报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6数据超长的报文首包触发日志；日志聚合开关关闭，每个ICMPV6数据超长的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.108 ATK_ICMPV6_PACKETTOOBIG_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6数据超长报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6数据超长的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.109 ATK_ICMPV6_PARAPROBLEM

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6参数问题的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6参数问题的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.110 ATK_ICMPV6_PARAPROBLEM_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6参数问题的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6参数问题的报文首包触发日志；日志聚合开关关闭，每个ICMPV6参数问题的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6参数问题的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6参数问题的报文首包触发日志；日志聚合开关关闭，每个ICMPV6参数问题的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.112 ATK_ICMPV6_PARAPROBLEM_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6参数问题的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6参数问题的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.113 ATK_ICMPV6_TIMEEXCEED

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6超时的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超时的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.114 ATK_ICMPV6_TIMEEXCEED_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6超时的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超时的报文首包触发日志；日志聚合开关关闭，每个ICMPV6超时的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6超时的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超时的报文首包触发日志；日志聚合开关关闭，每个ICMPV6超时的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.116 ATK_ICMPV6_TIMEEXCEED_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6超时的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6超时的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.117 ATK_ICMPV6_TRACEROUTE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP类型为3的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMPV6_TRACEROUTE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为3的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.118 ATK_ICMPV6_TRACEROUTE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING].
日志含义	设备检测到ICMP类型为3的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMPV6_TRACEROUTE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为3的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为3的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING].
日志含义	设备检测到ICMP类型为3的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMPV6_TRACEROUTE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为3的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为3的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.120 ATK_ICMPV6_TRACEROUTE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMP类型为3的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_ICMPV6_TRACEROUTE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMP类型为3的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.121 ATK_ICMPV6_TYPE

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TYPE:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6用户自定义类型的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.122 ATK_ICMPV6_TYPE_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TYPE_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMPV6用户自定义类型的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.123 ATK_ICMPV6_TYPE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到ICMPV6用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TYPE_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMPV6用户自定义类型的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.124 ATK_ICMPV6_TYPE_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到ICMPV6用户自定义类型的报文攻击
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_ICMPV6_TYPE_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，ICMPV6用户自定义类型的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.125 ATK_IP_OPTION

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到用户自定义IP选项的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IP_OPTION:SubModule(1127)=SINGLE;IPOptValue(1061)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，用户自定义IP选项的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.126 ATK_IP_OPTION_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到用户自定义IP选项的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IP_OPTION_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，用户自定义IP选项的报文首包触发日志；日志聚合开关关闭，每个用户自定义IP选项的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.127 ATK_IP_OPTION_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到用户自定义IP选项的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IP_OPTION_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，用户自定义IP选项的报文首包触发日志；日志聚合开关关闭，每个用户自定义IP选项的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.128 ATK_IP_OPTION_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到用户自定义IP选项的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IP_OPTION_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，用户自定义IP选项的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.129 ATK_IP4_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为ACK的IPV4报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_ACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为ACK的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ACK flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.130 ATK_IP4_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为ACK的IPV4报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_ACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为ACK的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ACK flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.131 ATK_IP4_DIS_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足分布式port scan的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_DIS_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	报文满足分布式portscan时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.132 ATK_IP4_DIS_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足分布式port scan的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_DIS_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	报文满足分布式portscan时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.133 ATK_IP4_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到DNS Query的报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_DNS_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送DNSQuery的报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 DNS flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.134 ATK_IP4_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到DNS Query的报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_DNS_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送DNSQuery的报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 DNS flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.135 ATK_IP4_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为SYN+ACK的报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_FIN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 FIN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.136 ATK_IP4_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为SYN+ACK的报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_FIN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 FIN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.137 ATK_IP4_FRAGMENT

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.138 ATK_IP4_FRAGMENT_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.139 ATK_IP4_FRAGMENT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.140 ATK_IP4_FRAGMENT_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.141 ATK_IP4_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到HTTP的Get报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_HTTP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的HTTP的Get报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 HTTP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.142 ATK_IP4_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到HTTP的Get报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_HTTP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的HTTP的Get报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 HTTP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.143 ATK_IP4_IMPOSSIBLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到源目的地址相同的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_IMPOSSIBLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.144 ATK_IP4_IMPOSSIBLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到源目的地址相同的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.145 ATK_IP4_IMPOSSIBLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到源目的地址相同的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.146 ATK_IP4_IMPOSSIBLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到源目的地址相同的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_IMPOSSIBLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.147 ATK_IP4_IPSWEEP

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足ip sweep的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_IPSWEEP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009060657.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	报文满足ipsweep时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.148 ATK_IP4_IPSWEEP_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足ip sweep的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_IPSWEEP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009060657.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	报文满足ipsweep时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.149 ATK_IP4_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];DstIPAddr(1007)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足port scan的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：目的IP地址 $8：动作类型 $9：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;DstIPAddr(1007)=6.1.1.5;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	报文满足portscan时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.150 ATK_IP4_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];DstIPAddr(1007)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足port scan的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：目的IP地址 $8：动作类型 $9：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;DstIPAddr(1007)=6.1.1.5;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	报文满足portscan时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.151 ATK_IP4_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为RST的IPV4报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_RST_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为RST的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 RST flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.152 ATK_IP4_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为RST的IPV4报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_RST_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为RST的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 RST flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.153 ATK_IP4_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为SYN的IPV4报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_SYN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为SYN的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.154 ATK_IP4_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为SYN的IPV4报文攻击
参数解释	$1：入域名称 $2：源IP地址 $3：目的IP地址 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_SYN_FLOOD_SZ:SrcZoneName(1025)=Trust;SrcIPAddr(1003)=2.3.3.1;DstIPAddr(1007)=6.1.1.5;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为SYN的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.155 ATK_IP4_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为SYN+ACK的IPV4报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_SYNACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN-ACK flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.156 ATK_IP4_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到TCP标志位为SYN+ACK的IPV4报文攻击
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_SYNACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV4报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN-ACK flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.157 ATK_IP4_TCP_ALLFLAGS

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位全置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.158 ATK_IP4_TCP_ALLFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位全置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.159 ATK_IP4_TCP_ALLFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位全置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.160 ATK_IP4_TCP_ALLFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位全置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.161 ATK_IP4_TCP_FINONLY

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_FINONLY:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.162 ATK_IP4_TCP_FINONLY_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.163 ATK_IP4_TCP_FINONLY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.164 ATK_IP4_TCP_FINONLY_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_FINONLY_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.165 ATK_IP4_TCP_INVALIDFLAGS

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为无效的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20130111074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.166 ATK_IP4_TCP_INVALIDFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为无效的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.167 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为无效的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.168 ATK_IP4_TCP_INVALIDFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为无效的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.169 ATK_IP4_TCP_LAND

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV4源目的地址相同的TCP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_LAND:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.170 ATK_IP4_TCP_LAND_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV4源目的地址相同的TCP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_LAND_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV4源目的地址相同的TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.171 ATK_IP4_TCP_LAND_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV4源目的地址相同的TCP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_LAND_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV4源目的地址相同的TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.172 ATK_IP4_TCP_LAND_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV4源目的地址相同的TCP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_LAND_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.173 ATK_IP4_TCP_NULLFLAG

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位未置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_NULLFLAG:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=4.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.174 ATK_IP4_TCP_NULLFLAG_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位未置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.175 ATK_IP4_TCP_NULLFLAG_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位未置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.176 ATK_IP4_TCP_NULLFLAG_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位未置位的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=4.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.177 ATK_IP4_TCP_SYNFIN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_SYNFIN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.178 ATK_IP4_TCP_SYNFIN_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.179 ATK_IP4_TCP_SYNFIN_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.180 ATK_IP4_TCP_SYNFIN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_SYNFIN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.181 ATK_IP4_TCP_WINNUKE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_WINNUKE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=5.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.182 ATK_IP4_TCP_WINNUKE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.183 ATK_IP4_TCP_WINNUKE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.184 ATK_IP4_TCP_WINNUKE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TCP_WINNUKE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=5.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.185 ATK_IP4_TEARDROP

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到重叠偏移的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TEARDROP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，重叠偏移的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.186 ATK_IP4_TEARDROP_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到重叠偏移的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TEARDROP_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，重叠偏移的报文首包触发日志；日志聚合开关关闭，每个重叠偏移的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.187 ATK_IP4_TEARDROP_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到重叠偏移的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TEARDROP_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，重叠偏移的报文首包触发日志；日志聚合开关关闭，每个重叠偏移的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.188 ATK_IP4_TEARDROP_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到重叠偏移的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_TEARDROP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，重叠偏移的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.189 ATK_IP4_TINY_FRAGMENT

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到分片标志位IP_MF置位且IP数据包的长度小于68的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_TINY_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=6.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.190 ATK_IP4_TINY_FRAGMENT_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到分片标志位IP_MF置位且IP数据包的长度小于68的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_TINY_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文首包触发日志；日志聚合开关关闭，每个分片标志位IP_MF置位且IP数据包的长度小于68的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.191 ATK_IP4_TINY_FRAGMENT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到分片标志位IP_MF置位且IP数据包的长度小于68的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_TINY_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文首包触发日志；日志聚合开关关闭，每个分片标志位IP_MF置位且IP数据包的长度小于68的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.192 ATK_IP4_TINY_FRAGMENT_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到分片标志位IP_MF置位且IP数据包的长度小于68的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_IP4_TINY_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=6.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.193 ATK_IP4_UDP_BOMB

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到满足IP报文长度-IP首部>数据报长度的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_BOMB:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.194 ATK_IP4_UDP_BOMB_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到满足IP报文长度-IP首部>数据报长度的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文首包触发日志；日志聚合开关关闭，每个满足IP报文长度-IP首部>数据报长度的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.195 ATK_IP4_UDP_BOMB_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到满足IP报文长度-IP首部>数据报长度的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文首包触发日志；日志聚合开关关闭，每个满足IP报文长度-IP首部>数据报长度的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.196 ATK_IP4_UDP_BOMB_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到满足IP报文长度-IP首部>数据报长度的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_BOMB_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.197 ATK_IP4_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定IPV4目的地址的UDP报文攻击
参数解释	$1：入接口名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定IPV4目的地址的UDP报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 UDP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.198 ATK_IP4_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定IPV4目的地址的UDP报文攻击
参数解释	$1：入域名称 $2：源IP地址 $3：目的IP地址 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_FLOOD_SZ:SrcZoneName(1025)=Trust;SrcIPAddr(1003)=2.3.3.1;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定IPV4目的地址的UDP报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 UDP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.199 ATK_IP4_UDP_FRAGGLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到满足IPV4源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_FRAGGLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=11.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，满足IPV4源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.200 ATK_IP4_UDP_FRAGGLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到满足IPV4源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.201 ATK_IP4_UDP_FRAGGLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到满足IPV4源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.202 ATK_IP4_UDP_FRAGGLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到满足IPV4源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=11.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，满足IPV4源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.203 ATK_IP4_UDP_SNORK

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV4源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_SNORK:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.204 ATK_IP4_UDP_SNORK_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV4源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.205 ATK_IP4_UDP_SNORK_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV4源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.206 ATK_IP4_UDP_SNORK_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV4源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP4_UDP_SNORK_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.207 ATK_IP6_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的地址的TCP标志位为ACK的IPV6报文攻击
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_ACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为ACK的IPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ACK flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.208 ATK_IP6_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的地址的TCP标志位为ACK的IPV6报文攻击
参数解释	$1：入域名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_ACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定目的地址的TCP标志位为ACK的IPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 ACK flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.209 ATK_IP6_DIS_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足分布式port scan的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_DIS_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009100928.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	IPV6报文满足分布式portscan时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.210 ATK_IP6_DIS_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足分布式port scan的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_DIS_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009100928.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	IPV6报文满足分布式portscan时触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.211 ATK_IP6_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的IP发送DNS Query的IPV6报文攻击
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_DNS_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送DNSQuery的IPV6报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 DNS flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.212 ATK_IP6_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的IP发送DNS Query的IPV6报文攻击
参数解释	$1：入域名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_DNS_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送DNSQuery的IPV6报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 DNS flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.213 ATK_IP6_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文攻击
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_FIN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 FIN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.214 ATK_IP6_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文攻击
参数解释	$1：入域名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_FIN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 FIN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.215 ATK_IP6_FRAGMENT

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_IP6_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.216 ATK_IP6_FRAGMENT_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_IP6_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.217 ATK_IP6_FRAGMENT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	4 (Warning)
举例	ATK/4/ATK_IP6_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.218 ATK_IP6_FRAGMENT_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到偏移量OffSet值在(0,5)之间的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	4 (Warning)
举例	ATK/4/ATK_IP6_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.219 ATK_IP6_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的IP发送的HTTP的IPV6 Get报文攻击
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_HTTP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的HTTP的IPV6Get报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 HTTP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.220 ATK_IP6_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定目的IP发送的HTTP的IPV6 Get报文攻击
参数解释	$1：入域名称 $2：目的IPv6地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_HTTP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内向指定目的IP发送的HTTP的IPV6Get报文数超过阈值，触发日志发送
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 HTTP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.221 ATK_IP6_IMPOSSIBLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到源目的地址相同的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_IMPOSSIBLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.222 ATK_IP6_IMPOSSIBLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到源目的地址相同的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.223 ATK_IP6_IMPOSSIBLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到源目的地址相同的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.224 ATK_IP6_IMPOSSIBLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到源目的地址相同的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_IMPOSSIBLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，源目的地址相同的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.225 ATK_IP6_IPSWEEP

日志内容	SubModule(1127)=SCAN;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到IPv6地址扫描攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_IPSWEEP:SubModule(1127)=SCAN;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100639.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	IPV6报文满足地址扫描攻击的检测条件时触发日志
处理建议	• 请确保扫描攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.226 ATK_IP6_IPSWEEP_SZ

日志内容	SubModule(1127)=SCAN;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到IPv6地址扫描攻击
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_IPSWEEP_SZ:SubModule(1127)=SCAN;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100639.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	IPV6报文满足地址扫描攻击的检测条件时触发日志
处理建议	• 请确保扫描攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.227 ATK_IP6_PORTSCAN

日志内容	SubModule(1127)=SCAN;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];DstIPv6Addr(1037)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足IPv6报文端口扫描攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IPv6地址 $5：VPN名称 $6：目的IPv6地址 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_PORTSCAN:SubModule(1127)=SCAN;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;DstIPv6Addr(1037)=2::2;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100455.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	IPV6报文满足端口扫描攻击的检测条件时触发日志
处理建议	• 请确保扫描攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.228 ATK_IP6_PORTSCAN_SZ

日志内容	SubModule(1127)=SCAN;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];DstIPv6Addr(1037)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足IPv6报文端口扫描攻击
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IPv6地址 $5：VPN名称 $6：目的IPv6地址 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_PORTSCAN_SZ:SubModule(1127)=SCAN;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;DstIPv6Addr(1037)=2::2;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100455.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	IPV6报文满足端口扫描攻击的检测条件时触发日志
处理建议	• 请确保扫描攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.229 ATK_IP6_RST_FLOOD

日志内容	AtkDirection(1134)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定基于源或目的地址统计的TCP标志位为RST的IPV6报文攻击
参数解释	$1：攻击方向 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_RST_FLOOD:AtkDirection(1134)=Destination;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定基于源或目的地址统计的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	• 请断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 RST flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.230 ATK_IP6_RST_FLOOD_SZ

日志内容	AtkDirection(1134)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定基于源或目的地址统计的TCP标志位为RST的IPV6报文攻击
参数解释	$1：攻击方向 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_RST_FLOOD_SZ:AtkDirection(1134)=Destination;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定基于源或目的地址统计的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	• 请断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 RST flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.231 ATK_IP6_SYN_FLOOD

日志内容	AtkDirection(1134)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足周期内指定基于源或目的地址统计的TCP标志位为SYN的IPV6报文攻击
参数解释	$1：攻击方向 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_SYN_FLOOD:AtkDirection(1134)=Destination;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	满足周期内指定基于源或目的地址统计的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.232 ATK_IP6_SYN_FLOOD_SZ

日志内容	AtkDirection(1134)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到满足周期内指定基于源或目的地址统计的TCP标志位为SYN的IPV6报文攻击
参数解释	$1：攻击方向 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_SYN_FLOOD_SZ:AtkDirection(1134)=Destination;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	满足周期内指定基于源或目的地址统计的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.233 ATK_IP6_SYNACK_FLOOD

日志内容	AtkDirection(1134)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定基于源或目的地址统计的TCP标志位为SYN+ACK的IPV6报文攻击
参数解释	$1：攻击方向 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_SYNACK_FLOOD:AtkDirection(1134)=Destination;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定基于源或目的地址统计的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.234 ATK_IP6_SYNACK_FLOOD_SZ

日志内容	AtkDirection(1134)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定基于源或目的地址统计的TCP标志位为SYN+ACK的IPV6报文攻击
参数解释	$1：攻击方向 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_SYNACK_FLOOD_SZ:AtkDirection(1134)=Destination;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定基于源或目的地址统计的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 SYN flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.235 ATK_IP6_TCP_ALLFLAGS

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位全置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.236 ATK_IP6_TCP_ALLFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位全置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.237 ATK_IP6_TCP_ALLFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位全置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.238 ATK_IP6_TCP_ALLFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位全置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位全置位的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.239 ATK_IP6_TCP_FINONLY

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_FINONLY:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.240 ATK_IP6_TCP_FINONLY_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.241 ATK_IP6_TCP_FINONLY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.242 ATK_IP6_TCP_FINONLY_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_FINONLY_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为FIN的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.243 ATK_IP6_TCP_INVALIDFLAGS

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为无效的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.244 ATK_IP6_TCP_INVALIDFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为无效的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6TCP报文首包触发日志 日志聚合开关关闭，每个TCP标志位为无效时的IPV6TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.245 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为无效的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6TCP报文首包触发日志 日志聚合开关关闭，每个TCP标志位为无效时的IPV6TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.246 ATK_IP6_TCP_INVALIDFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为无效的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.247 ATK_IP6_TCP_LAND

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV6源和目的地址都是目标主机自身的TCP SYN报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_LAND:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源和目的地址都是目标主机自身的TCP SYN报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.248 ATK_IP6_TCP_LAND_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV6源和目的地址都是目标主机自身的TCP SYN报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_LAND_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源和目的地址都是目标主机自身的TCP SYN报文首包触发日志；日志聚合开关关闭，每个IPV6源目的地址相同的TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.249 ATK_IP6_TCP_LAND_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV6源和目的地址都是目标主机自身的TCP SYN报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_LAND_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源和目的地址都是目标主机自身的TCP SYN报文首包触发日志；日志聚合开关关闭，每个IPV6源目的地址相同的TCP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.250 ATK_IP6_TCP_LAND_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV6源和目的地址都是目标主机自身的TCP SYN报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_LAND_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源和目的地址都是目标主机自身的TCP SYN报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.251 ATK_IP6_TCP_NULLFLAG

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位未置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_NULLFLAG:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.252 ATK_IP6_TCP_NULLFLAG_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位未置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.253 ATK_IP6_TCP_NULLFLAG_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位未置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.254 ATK_IP6_TCP_NULLFLAG_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位未置位的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位未置位的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.255 ATK_IP6_TCP_SYNFIN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_SYNFIN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.256 ATK_IP6_TCP_SYNFIN_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.257 ATK_IP6_TCP_SYNFIN_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.258 ATK_IP6_TCP_SYNFIN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP标志位为SYN+FIN的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_SYNFIN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.259 ATK_IP6_TCP_WINNUKE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_WINNUKE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.260 ATK_IP6_TCP_WINNUKE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.261 ATK_IP6_TCP_WINNUKE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.262 ATK_IP6_TCP_WINNUKE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_TCP_WINNUKE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.263 ATK_IP6_UDP_FLOOD

日志内容	AtkDirection(1134)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定IPV6基于源或目的地址统计的UDP报文攻击
参数解释	$1：攻击方向 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_FLOOD:AtkDirection(1134)=Source;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::2;DstIPv6Addr(1037)=;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定IPV6基于源或目的地址统计的UDP报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 UDP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.264 ATK_IP6_UDP_FLOOD_SZ

日志内容	AtkDirection(1134)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
日志含义	设备检测到指定IPV6基于源或目的地址统计的UDP报文攻击
参数解释	$1：攻击方向 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：速率上限 $7：动作类型 $8：攻击开始时间
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_FLOOD_SZ:AtkDirection(1134)=Source;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::2;DstIPv6Addr(1037)=;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	单位时间内指定IPV6基于源或目的地址统计的UDP报文数超过阈值，触发日志
处理建议	• 请判断是否为攻击报文，若为正常业务报文，请调整阈值配置，避免触发此日志；若为攻击报文，请确保 UDP flood 攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.265 ATK_IP6_UDP_FRAGGLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV6源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_FRAGGLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.266 ATK_IP6_UDP_FRAGGLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV6源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.267 ATK_IP6_UDP_FRAGGLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV6源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.268 ATK_IP6_UDP_FRAGGLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV6源端口为7，目的端口为19的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.269 ATK_IP6_UDP_SNORK

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV6源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_SNORK:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.270 ATK_IP6_UDP_SNORK_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV6源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.271 ATK_IP6_UDP_SNORK_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IPV6源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.272 ATK_IP6_UDP_SNORK_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IPV6源端口为7、19或135，目的端口为135的UDP报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IP6_UDP_SNORK_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.273 ATK_IPOPT_ABNORMAL

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项异常的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IPOPT_ABNORMAL:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011072002;EndTime_c(1012)=20131011072502;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项异常的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.274 ATK_IPOPT_ABNORMAL_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项异常的报文攻击
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项异常的报文首包触发日志；日志聚合开关关闭，每个IP选项异常的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.275 ATK_IPOPT_ABNORMAL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项异常的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	3 (Error)
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项异常的报文首包触发日志；日志聚合开关关闭，每个IP选项异常的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.276 ATK_IPOPT_ABNORMAL_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项异常的报文攻击
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	3 (Error)
举例	ATK/3/ATK_IPOPT_ABNORMAL_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011072002;EndTime_c(1012)=20131011072502;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项异常的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.277 ATK_IPOPT_LOOSESRCROUTE

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为131的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为131的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.278 ATK_IPOPT_LOOSESRCROUTE_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为131的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为131的报文首包触发日志；日志聚合开关关闭，每个IP选项为131的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.279 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为131的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=131;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为131的报文首包触发日志；日志聚合开关关闭，每个IP选项为131的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.280 ATK_IPOPT_LOOSESRCROUTE_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为131的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=131;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为131的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.281 ATK_IPOPT_RECORDROUTE

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为7的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_RECORDROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=7;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为7的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.282 ATK_IPOPT_RECORDROUTE_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为7的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=7;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为7的报文首包触发日志；日志聚合开关关闭，每个IP选项为7的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.283 ATK_IPOPT_RECORDROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为7的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=7;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为7的报文首包触发日志；日志聚合开关关闭，每个IP选项为7的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.284 ATK_IPOPT_RECORDROUTE_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为7的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_RECORDROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=7;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为7的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.285 ATK_IPOPT_ROUTEALERT

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为148的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_ROUTEALERT:SubModule(1127)=SINGLE;IPOptValue(1061)=148;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为148的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.286 ATK_IPOPT_ROUTEALERT_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为148的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=148;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为148的报文首包触发日志；日志聚合开关关闭，每个IP选项为148的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.287 ATK_IPOPT_ROUTEALERT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为148的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=148;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为148的报文首包触发日志；日志聚合开关关闭，每个IP选项为148的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.288 ATK_IPOPT_ROUTEALERT_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为148的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_ROUTEALERT_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=148;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为148的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.289 ATK_IPOPT_SECURITY

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为130的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_SECURITY:SubModule(1127)=SINGLE;IPOptValue(1061)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131009091022;EndTime_c(1012)=20131009091522;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为130的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.290 ATK_IPOPT_SECURITY_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为130的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_SECURITY_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为130的报文首包触发日志；日志聚合开关关闭，每个IP选项为130的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.291 ATK_IPOPT_SECURITY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为130的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_SECURITY_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=130;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为130的报文首包触发日志；日志聚合开关关闭，每个IP选项为130的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.292 ATK_IPOPT_SECURITY_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为130的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_SECURITY_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=130;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131009091022;EndTime_c(1012)=20131009091522;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为130的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.293 ATK_IPOPT_STREAMID

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为136的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $11：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STREAMID:SubModule(1127)=SINGLE;IPOptValue(1061)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为136的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.294 ATK_IPOPT_STREAMID_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为136的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STREAMID_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为136的报文首包触发日志；日志聚合开关关闭，每个IP选项为136的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.295 ATK_IPOPT_STREAMID_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为136的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STREAMID_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=136;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为136的报文首包触发日志；日志聚合开关关闭，每个IP选项为136的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.296 ATK_IPOPT_STREAMID_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为136的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STREAMID_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=136;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为136的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.297 ATK_IPOPT_STRICTSRCROUTE

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为137的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=137;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为137的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.298 ATK_IPOPT_STRICTSRCROUTE_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为137的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=137;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为137的报文首包触发日志；日志聚合开关关闭，每个IP选项为137的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.299 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为137的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=137;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为137的报文首包触发日志；日志聚合开关关闭，每个IP选项为137的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.300 ATK_IPOPT_STRICTSRCROUTE_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为137的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=137;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为137的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.301 ATK_IPOPT_TIMESTAMP

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为68的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_TIMESTAMP:SubModule(1127)=SINGLE;IPOptValue(1061)=68;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为68的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.302 ATK_IPOPT_TIMESTAMP_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为68的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=68;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAW IP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为68的报文首包触发日志；日志聚合开关关闭，每个IP选项为68的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.303 ATK_IPOPT_TIMESTAMP_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到IP选项为68的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=68;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，IP选项为68的报文首包触发日志；日志聚合开关关闭，每个IP选项为68的报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.304 ATK_IPOPT_TIMESTAMP_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到IP选项为68的报文攻击
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPOPT_TIMESTAMP_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=68;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，IP选项为68的报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.305 ATK_IPV6_EXT_HEADER

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到自定义扩展头的IPV6报文攻击
参数解释	$1：子模块名称 $2：IPv6扩展头 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：入接口VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPV6_EXT_HEADER:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，自定义扩展头的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.306 ATK_IPV6_EXT_HEADER_RAW

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到自定义扩展头的IPV6报文攻击
参数解释	$1：子模块名称 $2：IPv6扩展头 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，自定义扩展头的IPV6报文首包触发日志；日志聚合开关关闭，每个自定义扩展头的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.307 ATK_IPV6_EXT_HEADER_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
日志含义	设备检测到自定义扩展头的IPV6报文攻击
参数解释	$1：子模块名称 $2：IPv6扩展头 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5 (Notification)
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW_SZ:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关开启，自定义扩展头的IPV6报文首包触发日志；日志聚合开关关闭，每个自定义扩展头的IPV6报文触发一个日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

7.308 ATK_IPV6_EXT_HEADER_SZ

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
日志含义	设备检测到自定义扩展头的IPV6报文攻击
参数解释	$1：子模块名称 $2：IPv6扩展头 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：入接口VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5 (Notification)
举例	ATK/5/ATK_IPV6_EXT_HEADER_SZ:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	日志聚合开关打开，自定义扩展头的IPV6报文数超过1，聚合后触发日志
处理建议	• 请确保单包攻击防范策略已配置报文丢弃动作，具体配置方法请参见攻击检测与防范配置指导 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

8 ATM

本节介绍 ATM 模块输出的日志信息。

8.1 ATM_PVCDOWN

日志内容	Interface [STRING] PVC [UINT16]/[UINT16] status is down.
日志含义	PVC的状态转变为down
参数解释	$1：PVC所属接口的名称 $2：PVC的VPI值 $3：PVC的VCI值
日志等级	5 (Notification)
举例	ATM/5/ATM_PVCDOWN: Interface ATM2/0/2 PVC 0/100 status is down.
对系统的影响	基于该PVC的ATM功能不可用
日志产生原因	• PVC 所属 ATM 接口状态转变为 down • PVC 的 OAM 状态转变为 down • PVC 被 shutdown

处理建议	**1.** 使用 **display atm pvc-info**命令查看指定接口的PVC详细信息，根据显示信息进行如下处理：
	2. 如果 Interface State 字段显示为 DOWN
	• 使用 **display interface atm**命令分别检查本端和对端的ATM接口是否被手动 **shutdown**，若是，可通过在接口上执行 **undo shutdown**命令解决该问题
	• 检查接口之间的连线是否插好
	3. 如果 OAM State 字段显示为 DOWN
	• 当两台路由器直连时：
	  ○ 检查对端接口上创建的 PVC 的 VPI/VCI 是否与本端相同
	  ○ 检查对端接口上PVC的OAM配置是否与本端一致（比如本端配置了 **oam cc sink**，对端需配置 **oam cc source**）
	  ○ 检查对端的PVC是否被手动 **shutdown**，若是，可通过在PVC视图上执行 **undo shutdown**命令解决该问题
	  ○ 检查两端连线是否正确
	• 当两台路由器通过 ATM 交换网络连接时，除检查上述几点外，还需要检查交换网络中转发规则配置是否正确，如果两端 PVC 在交换网络中不可达，PVC 状态同样为 down
	4. 如果PVC State字段显示为DOWN，请检查本端的PVC是否被手动 **shutdown**，若是，可通过在PVC视图上执行 **undo shutdown**命令解决该问题
	5. 执行以上操作后，若问题仍未解决，请收集如下信息，并联系技术支持人员
	  ○ 上述步骤的执行结果
	  ○ 设备的配置文件、日志信息、告警信息

8.2 ATM_PVCUP

日志内容	Interface [STRING] PVC [UINT16]/[UINT16] status is up.
日志含义	PVC的状态转变为up
参数解释	$1：PVC所属接口的名称 $2：PVC的VPI值 $3：PVC的VCI值
日志等级	5 (Notification)
举例	ATM/5/ATM_PVCUP: Interface ATM2/0/2 PVC 0/100 status is up.
对系统的影响	基于该PVC的ATM功能恢复正常
日志产生原因	PVC的状态转变为up
处理建议	无需处理

9 BFD

本节介绍 BFD 模块输出的日志信息。

9.1 BFD_CHANGE_FSM

日志内容	Sess[STRING], Ver.[UINT32], Sta: [STRING]->[STRING], Diag: [STRING]
日志含义	BFD会话的状态机发生变化，由UP状态变成其他状态，或者由其他状态变成UP状态
参数解释	$1：BFD会话的源地址、目的地址、接口和消息类型 $2：BFD版本，取值包括0和1 $3：变化前状态机的名称 $4：变化后状态机的名称 $5：诊断信息，包括 • 0 (No Diagnostic)：表示无诊断信息 • 1 (Control Detection Time Expired)：表示 Ctrl 会话本端检测时间超时，会话 down • 2 (Echo Function Failed)：表示 Echo 会话本端检测时间超时或 echo 报文的源 IP 地址被删除，会话 down • 3 (Neighbor Signaled Session Down)：表示对端通知本端 BFD 会话 down • 7 (Administratively Down)：表示本端系统阻止 BFD 会话的建立
日志等级	5 (Notification)
举例	BFD/5/BFD_CHANGE_FSM:Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface:Vlan204, SessType:Ctrl, LinkType:INET], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic).
对系统的影响	• 如果会话从非 Down 状态变为 Down，说明会话状态异常，进而影响联动该会话的上层业务。 • 如果会话从非 Up 状态变为 Up，说明会话状态恢复，则绑定的业务也随之恢复。 • 如果会话发生如下状态变化，包括从 Down 变为 Init，从 Down/Init/Up 变为 AdminDown，则对绑定的业务无影响。
日志产生原因	BFD会话由其他状态变成Up状态，产生此告警的可能原因包括： • BFD 会话创建或者故障恢复，BFD 会话由 Down 状态变为 Up 状态。 • BFD 会话创建或者故障恢复，BFD 会话由 Init 状态变为 Up 状态。 • BFD 相关配置变化，BFD 会话由 AdminDown 状态变为 Up 状态。 BFD会话由Up状态变成其他状态，产生此告警的可能原因包括： • BFD 会话所检测的路径故障，导致 BFD 报文无法正常交互。 • 会话绑定的接口状态变为 Down。 • 会话绑定的其他 BFD 会话状态变为 Down。 • 对端会话被 Shutdown 或者被删除。 BFD会话由其他状态变成AdminDown状态，产生此告警的可能原因为：会话被删除。
处理建议	1. 如果会话最终状态不是 Down，则为正常运行信息，无需处理。 2. 如果会话从非 Down 状态变为 Down，则请执行步骤 3。 3. 请使用 **display interface** *interface-type interface-number*命令查看会话所在接口的物理状态是否为Up。 o 如果是，则请执行步骤 4。 o 如果否，请查看物理链接是否正常（包括网线、光模块等硬件是否松动或脱落），可以重新正确连接物理线路，然后使用 **display bfd session**命令查看会话的状态。如果会话的“State”字段取值仍为非“Up”，则请执行步骤 4。

	4. 请使用 **display bfd session**命令检查两端的BFD会话是否被删除。 o 如果是，则请正确配置两端的会话，然后使用 **display bfd session**命令查看会话的状态。如果会话的“State”字段取值仍为非“Up”，则请执行步骤5。 o 如果否，则请执行步骤5。 **5.** 请用 **ping**命令检查是否BFD会话所检测的链路是否能够正常转发报文。 o 如果否，请检查链路是否存在故障，路由是否部署正确，可以重新部署转发路径，然后使用 **display bfd session**命令查看会话的状态。如果会话的“State”字段取值仍为非“Up”，则请执行步骤6。 o 如果是，则请执行步骤6。 **6.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

9.2 BFD_HARDWARE_SWITCHTO_SOFTWARE

日志内容	Sess[STRING], after you switch the BFD mode from hardware to software, the interval between BFD packet sending and receiving is too small and BFD does not perform session negotiation. If BFD session negotiation is required, increase the interval between BFD packet sending and receiving on the local device.
日志含义	硬件BFD切换为软件BFD后，本端当前发送/接收BFD报文的时间间隔太小，导致BFD不会进行会话协商。如需会话协商，请将本端发送/接收BFD报文的时间间隔调大
参数解释	$1：BFD会话的源地址、目的地址、接口、消息类型和MPLS FEC信息。LSP会话中包含LSP目的IP、掩码及下一跳IP；PW会话中包含Peer IP和PW ID；TE Tunnel会话中包含源IP、目的IP、Tunnel ID及LSP ID
日志等级	5 (Notification)
举例	BFD/5/BFD_HARDWARE_SWITCHTO_SOFTWARE: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface:Vlan204, SessType:Ctrl, LinkType:INET], after you switch the BFD mode from hardware to software, the interval between BFD packet sending and receiving is too small and BFD does not perform session negotiation. If BFD session negotiation is required, increase the interval between BFD packet sending and receiving on the local device.
对系统的影响	BFD不会进行会话协商，导致会话无法Up
日志产生原因	硬件BFD切换为软件BFD后，本端当前发送/接收BFD报文的时间间隔太小，导致BFD不会进行会话协商
处理建议	1. 请执行 **display bfd session verbose**命令，查看“Hardware mode”的取值。 o 如果“Hardware mode”取值为“Disable”，说明硬件处理 BFD 报文模式处于关闭状态，此时由软件处理 BFD 报文。对于单跳 BFD 会话，请执行步骤 2 或步骤 3。对于多跳 BFD 会话，请执行步骤 3 或步骤 4。 o 如果“Hardware mode”取值为“Enabled”，说明硬件处理 BFD 报文模式处于开启状态。这种情况下如果不再产生此日志，则处理过程结束。如果还会产生此日志，则请执行步骤 6。 2. 请执行如下命令将本端发送/接收 BFD 报文的时间间隔调大。（仅部分产品支持） o 请通过 **bfd min-transmit-interval**命令将本端发送单跳BFD控制报文的最小时间间隔调大。 o 请通过 **bfd min-receive-interval**命令将本端接收单跳BFD控制报文的最小时间间隔调大。 3. 请通过 **bfd min-control-interval**命令将本端发送和接收单跳BFD控制报文的最小时间间隔调大。（仅部分产品支持） 4. 请执行如下命令将本端发送/接收 BFD 报文的时间间隔调大。（仅部分产品支持） o 请通过 **bfd multi-hop min-transmit-interval**命令将本端发送多跳BFD控制报文的最小时间间隔调大。 o 请通过 **bfd multi-hop min-receive-interval**命令将本端接收多跳BFD控制报文的最小时间间隔调大。 5. 请通过 **bfd multi-hop min-control-interval**命令将本端发送和接收多跳BFD控制报文的最小时间间隔调大。（仅部分产品支持） 6. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

9.3 BFD_RD_ADD_DRIVER_FAILED

日志内容	Failed to add the remote identifiers to the driver: [STRING]. Reason: [STRING].
日志含义	设备将远端标识符添加到驱动失败，以及失败的原因
参数解释	$1：显示未处理成功的远端标识符，形式为value1, value2 to value3, value4，最多显示10段 $2：未处理成功原因 • Insufficient resources：设备资源不足 • Unknown：未知原因
日志等级	5 (Notification)
举例	BFD/5/BFD_RD_ADD_FAILED: Failed to add the remote identifiers to the driver: 1, 2 to 10, 1000. Reason: Insufficient resources.
对系统的影响	M-LAG组网且使用echo报文方式的静态BFD会话的场景中，可能会出现BFD会话状态异常的问题
日志产生原因	通过**bfd forwarding match remote-discriminator**命令添加BFD会话远端标识符时，由于设备资源不足或其他未知原因，导致设备将远端标识符添加到驱动失败
处理建议	1. 请在Probe视图下执行 **display system internal bfd capability**命令查看“Forwarding match remote discriminator limit”字段的取值，该值为设备允许配置的远端标识符的最大数量。 2. 请执行 **display current-configuration**命令查看 **bfd forwarding match remote-discriminator**命令配置的远端标识符的数量是否已经达到设备支持的最大数量。 o 如果已经达到设备支持的最大数量，且需要新增远端标识符，则请减少不必要的远端标识符的配置数量。 o 如果未达到设备支持的最大数量，则请执行步骤 3。 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

9.4 BFD_RD_CHANGE_SUCCESS

日志内容	For the remote discriminators failed to be added to the driver due to insufficient resources, the device automatically added them again and the operation succeeded: [STRING]
日志含义	设备将远端标识符添加到驱动失败后，设备自动重新添加，且添加成功
参数解释	$1：显示处理成功的远端标识符，形式为value1, value2 to value3, value4，最多显示10段
日志等级	5 (Notification)
举例	BFD/5/BFD_RD_CHANGE_SUCCESS: For the remote discriminators failed to be added to the driver due to insufficient resources, the device automatically added them again and the operation succeeded: 1, 2 to 10, 1000.
对系统的影响	对系统无影响
日志产生原因	设备资源不足导致远端标识符未能成功添加到驱动，设备自动尝试将这部分标识符重新添加到驱动。当标识符成功添加到驱动时，会输出此日志
处理建议	无需处理

9.5 BFD_REACHED_UPPER_LIMIT

日志内容	The total number of BFD sessions [ULONG] reached the upper limit. Please avoid creating a new session.
日志含义	BFD会话的数量达到上限。请不要创建新的会话。
参数解释	$1：BFD会话总数
日志等级	5 (Notification)
举例	BFD/5/BFD_REACHED_UPPER_LIMIT: The total number of BFD sessions 100 reached the upper limit. Please avoid creating a new session.
对系统的影响	• BFD 会话数量达到上限后，无法创建新的会话。 • 产生此日志的设备掉电或对该设备执行复位操作可能会导致资源重新分配而影响业务，所以当设备产生此日志时，不建议进行掉电或复位操作。
日志产生原因	• 整机 BFD 会话数量已经达到设备支持的最大规格，仍继续提交新的 BFD 配置。 • 动态 BFD 会话创建的数量超过上限。
处理建议	1. 停止配置新的 BFD 会话。 2. 通过命令删除多余的或无用的BFD会话。例如，如果存在多余的OSPF联动BFD的会话，请通过 **undo ospf bfd enable**命令删除该会话。不同业务产生的BFD如何删除，请查看对应业务的命令手册。 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

10 BGP

本节介绍 BGP 模块输出的日志信息。

10.1 BGP_DYN_PEER_LIMIT_REACHED

日志内容	BGP.[STRING]: The number of dynamic peers has reached the upper limit [UINT32].
日志含义	动态对等体数量达到了允许建立的最大数量
参数解释	$1：BGP实例名称 $2：允许建立的最大动态对等体数量
日志等级	4 (Warning)
举例	BGP/4/BGP_DYN_PEER_LIMIT_REACHED: BGP.default: The number of dynamic peers has reached the upper limit 5.
对系统的影响	无法建立新的动态对等体
日志产生原因	动态对等体数量过多
处理建议	1. 检查动态对等体数量超限是否由网络攻击导致，如果是，需要管理员进行相应的攻击防御配置 2. 否则，请执行 **dynamic-peer-limit**命令增大允许建立的动态对等体的最大数量

10.2 BGP_DYN_PEER_LIMIT_REACHED_CLEAR

日志内容	形式一： BGP.[STRING]: The number of dynamic peers has dropped below the upper limit. (upper limit [UINT32], current [UINT32]) 形式二： BGP.[STRING]: The limit on the number of dynamic peers is canceled.
日志含义	形式一： 建立的动态对等体数量降低到了允许建立的最大数量以下 形式二： 不再限制允许建立的动态对等体的最大数量
参数解释	形式一： $1：BGP实例名称 $2：允许建立的最大动态对等体数量 $3：当前已建立的动态对等体数量 形式二： $1：BGP实例名称
日志等级	6 (Informational)
举例	形式一： BGP/6/BGP_DYN_PEER_LIMIT_REACHED_CLEAR: BGP.default: The number of dynamic peers has dropped below the upper limit.(upper limit 13, current 12) 形式二： BGP/6/BGP_DYN_PEER_LIMIT_REACHED_CLEAR: BGP.default: The limit on the number of dynamic peers is canceled.
对系统的影响	对系统无影响
日志产生原因	形式一：动态对等体的数量减少 形式二：在设备上执行**undo dynamic-peer-limit**命令，不再限制BGP动态对等体建立的最大数量。
处理建议	无需处理

10.3 BGP_EXCEED_ROA_LIMIT

日志内容	BGP [STRING].[STRING]: The number of ROAs ([UINT32]) from server [STRING] exceeds the limit [UINT32].
日志含义	从RPKI服务器接收的ROA数量超过了允许的最大ROA数量
参数解释	$1：BGP实例名称 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：从RPKI服务器接收到的ROA数量 $4：RPKI服务器的IP地址 $5：允许从RPKI服务器接收的最大ROA数量
日志等级	4 (Warning)
举例	BGP/4/BGP_EXCEED_ROA_LIMIT: BGP default.vpn1: The number of ROAs (101) from server 192.168.56.10 exceeds the limit 100.
对系统的影响	根据**rpki-limit**命令配置的参数不同，对系统造成的影响不同： • 如果未指定 **alert-only**参数，则设备与RPKI服务器的TCP连接断开 • 如果指定了 **alert-only**参数，则对系统无影响
日志产生原因	从指定RPKI服务器接收的ROA数量超过了为其配置的最大ROA数量
处理建议	1. 执行 **display bgp rpki server**命令，通过“ROAs(IPv4/IPv6)”字段，查看设备当前收到ROA数量是否超过本地 **rpki-limit**命令配置的最大数量 o 如果超过了最大数量，请执行步骤 2 o 如果未超过最大数量，请执行步骤 6 2. 确认此时接收到的超过最大数量限制的 ROA 数量是否符合实际应用需求 o 如果符合实际应用需求，请执行步骤 5 o 如果不符合实际应用需求，请执行步骤 3 3. 联系 RPKI 服务器的管理员，确认 RPKI 服务器发布给设备的 ROA 是否均为必要 o 如果发布的 ROA 均为必要，请执行步骤 5 o 如果发布的 ROA 非均必要，请执行步骤 4 4. 联系 RPKI 服务器的管理员撤销发布不必要的 RPKI。如果问题仍未解决，请执行步骤 6 5. 在设备上执行 **rpki-limit**命令调大允许接收的ROA最大数量。如果问题仍未解决，请执行步骤 6 6. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

10.4 BGP_EXCEED_ROA_LIMIT_CLEAR

日志内容	BGP [STRING].[STRING]: The number of ROAs ([UINT32]) from server [STRING] fell below the limit [UINT32].
日志含义	从RPKI服务器接收的ROA数量降低到了允许的最大ROA数量以下
参数解释	$1：BGP实例名称 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：从RPKI服务器已接收到的ROA数量 $4：RPKI服务器的IP地址 $5：允许从RPKI服务器接收的最大ROA数量
日志等级	6 (Informational)
举例	BGP/6/BGP_EXCEED_ROA_LIMIT_CLEAR: BGP default.vpn1: The number of ROAs (99) from server 192.168.56.10 fell below the limit 100.
对系统的影响	对系统无影响
日志产生原因	从指定RPKI服务器接收的ROA数量降低到了为其配置的最大ROA数量以下
处理建议	无需处理

10.5 BGP_EXCEED_ROUTE_LIMIT

日志内容	BGP.[STRING]: The number of routes from peer [STRING] ([STRING]) exceeds the limit [UINT32].
日志含义	从对等体收到的路由数量超过了允许的最大路由数量
参数解释	$1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：BGP对等体的地址族 $4：允许从对等体接收的最大路由前缀数量
日志等级	4 (Warning)
举例	BGP/4/BGP_EXCEED_ROUTE_LIMIT: BGP.vpn1: The number of routes from peer 1.1.1.1 (IPv4-UNC) exceeds the limit 100.
对系统的影响	造成设备与该邻居间的BGP会话中断，或者无法再从该邻居接收新的路由，导致业务中断
日志产生原因	从指定对等体收到的路由数量超过了为其配置的最大路由数量
处理建议	1. 确认此时接收到的超过最大限制的路由数量是否符合实际应用需求 o 如果符合实际应用需求，请执行步骤 7 o 如果不符合实际应用需求，请执行步骤 2 2. 执行 **display current-configuration configuration bgp**命令查看BGP模块的当前配置，检查是否存在影响路由接收策略的配置，导致本端设备接收了不必要的过多路由。能造成影响命令包括 **peer prefix-list**、**peer filter-policy**、**peer as-path-acl**、**filter-policy**和 **peer route-policy**等 o 如果影响路由接收策略的配置，请执行步骤 3 o 如果不存在影响路由接收策略的配置，请执行步骤 4 3. 修改影响路由接受策略的配置，以减少本端设备接收的路由数量。此后请执行步骤 8 4. 联系邻居设备的管理员，确认邻居设备发布给本端设备的路由数量是否合理 o 如果发布的路由数量合理，请执行步骤 5 o 如果发布的路由数量不合理，请执行步骤 6 5. 联系邻居设备的管理员对 BGP 路由的发布进行聚合处理，并抑制具体路由的发布，以减少路由的发布数量。此后请执行步骤 8 6. 联系邻居设备的管理员更改对本端设备的路由发布策略，减少不必要的 BGP 路由发布。此后请执行步骤 8 7. 执行 **peer route-limit**命令，增大允许从邻居接收到的最大路由数量。此后请执行步骤 8 8. 查看设备是否已经打印 BGP/6/BGP_EXCEED_ROUTE_LIMIT_CLEAR 日志信息 o 如果打印了日志信息，表明故障已清除，故障处理流程结束 o 如果未打印日志信息，请执行步骤 9 9. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

10.6 BGP_REACHED_THRESHOLD

日志内容	BGP.[STRING]: The ratio of the number of routes received from peer [STRING] ([STRING]) to the number of allowed routes [UINT32] has reached the threshold ([UINT32]%).
日志含义	接收的路由数量达到告警阈值
参数解释	$1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：BGP对等体的地址族 $4：允许从对等体接收的最大路由数量 $5：接收的路由数量占允许的最大路由数量百分比的阈值
日志等级	5 (Notification)
举例	BGP/5/BGP_REACHED_THRESHOLD: BGP.vpn1: The ratio of the number of routes received from peer 1.1.1.1 (IPv4-UNC) to the number of allowed routes 100 has reached the threshold (60%).
对系统的影响	根据**peer route-limit**命令配置的告警阈值参数不同，对系统造成的影响不同： • 对于配置了告警阈值为 100%的邻居，会造成设备与该邻居间的 BGP 会话中断，或者无法再从该邻居接收新的路由。 • 对于配置了告警阈值为其他值的邻居，对系统无影响，但该告警会提醒用户注意潜在的影响，即收到的路由可能即将超过上限。
日志产生原因	从指定BGP对等体接收的路由数量占为其配置的最大路由数量的百分比达到了告警阈值
处理建议	**1.** 执行 **display bgp peer verbose**命令，通过显示信息中“NLRI statistics”以及“Message statistics”字段，查看从邻居收到的路由数量占允许从该邻居收到的最大路由数量的比例是否达到了告警阈值 o 如果达到了告警阈值，请执行步骤 2 o 如果未达到告警阈值，请执行步骤 10 **2.** 确认此时接收到的超过告警阈值的路由数量是否符合实际应用需求 o 如果符合实际应用需求，请执行步骤 8 o 如果不符合实际应用需求，请执行步骤 3 **3.** 执行 **display current-configuration configuration bgp**命令查看BGP模块的当前配置，检查是否存在影响路由接收策略的配置，导致本端设备接收了不必要的过多路由。能造成影响命令包括 **peer prefix-list**、**peer filter-policy**、**peer as-path-acl**、**filter-policy**和 **peer route-policy**等 o 如果影响路由接收策略的配置，请执行步骤 4 o 如果不存在影响路由接收策略的配置，请执行步骤 5 **4.** 修改影响路由接受策略的配置，以减少本端设备接收的路由数量。此后请执行步骤 9 **5.** 联系邻居设备的管理员，确认邻居设备发布给本端设备的路由数量是否合理 o 如果发布的路由数量合理，请执行步骤 6 o 如果发布的路由数量不合理，请执行步骤 7 **6.** 联系邻居设备的管理员对 BGP 路由的发布进行聚合处理，并抑制具体路由的发布，以减少路由的发布数量。此后请执行步骤 9 **7.** 联系邻居设备的管理员更改对本端设备的路由发布策略，减少不必要的 BGP 路由发布。此后请执行步骤 9 **8.** 执行 **peer route-limit**命令，增大允许从邻居接收到的最大路由数量，或者增大

	告警阈值。此后请执行步骤 9 **9.** 查看设备是否已经打印 BGP/4/BGP_PEER_RT_NUM_THR_EX_CLEAR 日志信息 ○ 如果打印了日志信息，表明故障已清除，故障处理流程结束 ○ 如果未打印日志信息，请执行步骤 10 **10.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

10.7 BGP_LOG_ROUTE_FLAP

日志内容	BGP.[STRING]: The route [STRING] [STRING]/[UINT32] learned from peer [STRING] ([STRING]) flapped.
日志含义	从BGP对等体学习到的BGP路由发生震荡
参数解释	$1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP路由的RD值。不带RD的路由则显示为空 $3：BGP路由的前缀地址 $4：BGP路由的前缀掩码 $5：BGP对等体的IP地址 $6：BGP对等体的地址族
日志等级	4 (Warning)
举例	BGP/4/BGP_LOG_ROUTE_FLAP: BGP.vpn1: The route 15.1.1.1/24 learned from peer 1.1.1.1 (IPv4-UNC) flapped.
对系统的影响	BGP路由的频繁震荡会造成系统CPU利用率增高，并且，可能造成业务的中断
日志产生原因	组网中的设备存在不合理的配置或其他问题，导致本端设备从指定BGP对等体学到的指定BGP路由发生震荡
处理建议	**1.** 配置 BGP 路由衰减功能就，减少路由震荡对系统的影响 **2.** 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

10.8 BGP_MEM_ALERT

日志内容	BGP process received system memory alert [STRING] event.
日志含义	BGP模块收到内存告警事件
参数解释	$1：内存告警的类型，包括stop、start
日志等级	5 (Notification)
举例	BGP/5/BGP_MEM_ALERT: BGP process received system memory alert start event.
对系统的影响	BGP进程无法正常运行
日志产生原因	BGP模块收到内存告警事件
处理建议	执行**display memory-threshold**命令，获取内存告警门限相关信息；并收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

10.9 BGP_PEER_LICENSE_REACHED

日志内容	Number of peers in Established state reached the license limit.
日志含义	处于Established状态的对等体数量达到license规格上限
参数解释	无
日志等级	5 (Notification)
举例	BGP/5/BGP_PEER_LICENSE_REACHED: Number of peers in Established state reached the license limit.
对系统的影响	无法建立更多处于Established状态的对等体
日志产生原因	处于Established状态的对等体数量达到license规格上限
处理建议	检查目前安装的license规定的Established状态对等体数量规格上限是否已经满足需求： • 如果是，请配置删除无需建立 BGP 会话的 BGP 对等体 • 如果否，请购买并安装规格上限更高的 license

10.10 BGP_REMOTE_RTID_CONFLICT

日志内容	The local router ID conflicts with the remote router ID. (Router ID = [STRING], instance = [STRING], VPN instance = [STRING], peer = [STRING])
日志含义	远端BGP对等体使用的Router ID与本端相同，导致Router ID冲突，BGP会话建立失败
参数解释	$1：发生冲突的Router ID $2：BGP实例名称 $3：VPN实例名称。如果是公网内的日志信息，则显示为空 $4：BGP对等体的IP地址
日志等级	3 (Error)
举例	BGP/3/BGP_REMOTE_RTID_CONFLICT: The local router ID conflicts with the remote router ID. (Router ID = 2.2.2.2, instance = default, VPN instance = vpn1, peer = 192.168.1.1)
对系统的影响	本端与远端的BGP会话无法建立
日志产生原因	远端BGP对等体使用的Router ID与本端相同
处理建议	检查组网中各设备的Router ID，确保各设备的Router ID唯一

10.11 BGP_ROUTE_LICENSE_REACHED

日志内容	Number of [STRING] routes reached the license limit.
日志含义	路由数量达到license规格上限
参数解释	$1：BGP地址族，取值包括： • IPv4-UNC public：表示公网 IPv4 单播路由 • IPv6-UNC public：表示公网 IPv6 单播路由 • IPv4 private：表示私网 IPv4 单播路由，VPNv4 路由和嵌套 VPN 路由 • IPv6 private：表示私网 IPv6 单播路由，VPNv6 路由
日志等级	5 (Notification)
举例	BGP/5/BGP_ROUTE_LICENSE_REACHED: Number of IPv4-UNC public routes reached the license limit.
对系统的影响	无法支持更多的路由数量
日志产生原因	指定类型的BGP路由数量达到license规格的上限值
处理建议	检查目前安装的license规定的路由数量规格上限是否已经满足需求： • 如果是，请配置路由的发布、接收策略，以减少不需要的 BGP 路由的数量 • 如果否，请购买并安装规格上限更高的 license 需要注意的是，通过配置减少了BGP路由数量或安装了规格上限更高的license之后，之前被丢弃的路由不能自动恢复，需要用户手工配置以重新学习路由

10.12 BGP_RTID_CONFLICT

日志内容	Local router ID conflicts with the originator ID carried by a route. (Router ID=[STRING], instance=[STRING], VPN instance=[STRING], Peer=[STRING])
日志含义	BGP路由中携带的ORIGINATOR_ID属性与本地设备的Router ID相同，导致该路由无法被接收
参数解释	$1：Router ID $2：BGP实例名称 $3：VPN实例名称。如果是公网内的日志信息，则显示为空 $4：BGP对等体的IP地址
日志等级	3 (Error)
举例	BGP/3/BGP_RTID_CONFLICT: Local router ID conflicts with the originator ID carried by a route. (Router ID=2.2.2.2, instance=default, VPN instance=vpn1,Peer=192.168.1.1)
对系统的影响	路由无法被接收
日志产生原因	BGP路由中携带的ORIGINATOR_ID属性与本地设备的Router ID相同
处理建议	检查组网中各设备的Router ID，确保各设备的Router ID唯一

10.13 BGP_STATE_CHANGED

日志内容	形式一： BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING]. 形式二： BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING] for [STRING].
日志含义	BGP会话的状态发生改变
参数解释	形式一： $1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体。可能为以下形式： • 对等体的 IP 地址 • 对等体的链路本地地址以及连接该对等体的接口 $3：变化前的状态名称 $4：变化后的状态名称 形式二： $1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体。可能为以下形式： • 对等体的 IP 地址 • 对等体的链路本地地址以及连接该对等体的接口 $3：变化前的状态名称 $4：变化后的状态名称 $5：状态变化的原因
日志等级	5 (Notification)
举例	BGP/5/BGP_STATE_CHANGED: BGP.vpn1: 192.99.0.2 state has changed from OPENCONFIRM to ESTABLISHED.
对系统的影响	形式一： 对系统无影响 形式二： 表示BGP会话断开，设备可能缺少指导流量转发的BGP路由，导致转发业务中断
日志产生原因	形式一： 与指定对等体的BGP会话进入Established状态 形式二： 与指定对等体的BGP会话从Established状态进入其他状态
处理建议	形式一： 无需处理 形式二： 3. 执行 **display current-configuration configuration bgp**命令，检查是否存在影响BGP会话状态的配置： o 如果存在造成 BGP 会话断开的配置，请执行相应的命令取消该配置 o 如果BGP会话使用Loopback接口作为TCP连接的源接口，则需要执行 **peer connect-interface**或 **peer source-address**命令配置BGP会话建立TCP连接的源地址为Loopback接口的地址

- 如果BGP会话为多跳EBGP会话，请确保会话两端设备都配置了 **peer ebgp-max-hop**命令
- 如果设备上配置了 **peer ttl-security**命令开启BGP GTSM功能，则该设备只会接收TTL满足“255-最大跳数+1≤TTL≤255”的BGP报文
- 如果不存在影响 BGP 会话状态的配置，请执行步骤 2

4. 进行短暂等待，排除复位 BGP 会话造成的连接断开。如果长时间 BGP 会话状态未恢复 Established，请执行步骤 3

5. 执行 **display current-configuration configuration bgp**命令，检查是否存在 **peer route-limit**命令的配置，且设备是否打印 BGP/4/BGP_EXCEED_ROUTE_LIMIT日志

- 如果均是，则表明BGP会话由于收到过多的BGP路由而断开。此时需要判断通过 **peer route-limit**命令配置的接收路由最大数量是否合理：如果合理，请通知对端BGP设备管理员降低发送的BGP路由数量。如果不合理，请增大本端允许接收的BGP路由最大数量
- 如果任意一项为否，则表明 BGP 会话不是由于接收到过多 BGP 路由而断开，请执行步骤 4

6. 执行 **display bgp peer log-info**命令，根据显示信息中的“Notification Error/SubError”字段打印的错误码和子错误码判断BGP连接断开的具体原因

如果错误码（Error）为4，表示BGP会话保持时间内本端未能收到对端的Keepalive或Update消息，导致BGP会话断开。如果错误码为5或6，表示TCP连接错误或主动关闭连接。可以通过如下方式进行排查：

- 执行Ping命令查看本端是否能到达BGP对等体建立TCP连接使用的源地址。如果Ping不通，请执行 **display ip routing-table**命令查看是否存在能够到达BGP对等体地址的路由。如果不存在能够到达BGP对等体地址的路由，请排查IGP路由、静态路由或直连路由的相关配置
- 执行 **display memory-threshold**命令排查设备是否到达内存门限。如果内存到达门限，请执行步骤 5
- 执行 **display cpu-usage**命令排查设备CPU利用率是否过高。如果CPU利用率过高，请执行步骤 5
- 执行 **display acl all**命令，查看是否存在拒绝端口号为bgp或 179 的规则。如果存在这样的ACL，请配置删除该ACL
- 执行 **display interface**命令，查看到达BGP对等体地址的路由下一跳出接口是否UP。如果出接口DOWN，请尝试在该接口视图下执行 **undo shutdown**命令开启该接口。如果接口开启失败或接口处于UP状态但告警仍未消除，请执行步骤 5

如果错误码（Error）为1或3，表示设备收到了错误的BGP报文。请执行步骤5

7. 如果执行上述所有操作后问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

10.14 BGP_STATE_CHANGED_REASON

日志内容	BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING]. ([STRING])
日志含义	BG会话断开，以及断开的原因
参数解释	$1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：变化前BGP会话的状态 $4：变化后BGP会话的状态 $5：BGP会话断开相关信息： • Reason：BGP 会话断开的原因 • Error code：发送或者接收的 Notification 错误码/子错误码（TCP 连接失败导致 BGP 会话断开时不显示本字段） • Local interface：建立 BGP 会话使用的物理接口（本字段仅在由于接口不通导致直连对等体间的 BGP 会话断开时显示）
日志等级	5 (Notification)
举例	BGP/5/BGP_STATE_CHANGED_REASON: BGP.vpn1: 192.99.0.2 state has changed from ESTABLISHED to IDLE. (Reason: Directly connected physical interface was down, Error code: Send Notificationcode 6/0, Local interface: GigabitEthernet1/0/1)
对系统的影响	表示BGP会话断开，设备可能缺少指导流量转发的BGP路由，导致转发业务中断
日志产生原因	与指定对等体的BGP会话从Established状态进入其他状态
处理建议	1. 执行 **display current-configuration configuration bgp**命令，检查是否存在影响BGP会话状态的配置： ○ 如果存在造成 BGP 会话断开的配置，请执行相应的命令取消该配置 ○ 如果BGP会话使用Loopback接口作为TCP连接的源接口，则需要执行 **peer connect-interface**或 **peer source-address**命令配置BGP会话建立TCP连接的源地址为Loopback接口的地址 ○ 如果BGP会话为多跳EBGP会话，请确保会话两端设备都配置了 **peer ebgp-max-hop**命令 ○ 如果设备上配置了 **peer ttl-security**命令开启BGP GTSM功能，则该设备只会接收TTL满足“255-最大跳数+1≤TTL≤255”的BGP报文 ○ 如果不存在影响 BGP 会话状态的配置，请执行步骤 2 2. 进行短暂等待，排除复位 BGP 会话造成的连接断开。如果长时间 BGP 会话状态未恢复 Established，请执行步骤 3 3. 执行 **display current-configuration configuration bgp**命令，检查是否存在 **peer route-limit**命令的配置，且设备是否打印 BGP/4/BGP_EXCEED_ROUTE_LIMIT日志 ○ 如果均是，则表明BGP会话由于收到过多的BGP路由而断开。此时需要判断通过 **peer route-limit**命令配置的接收路由最大数量是否合理：如果合理，请通知对端BGP设备管理员降低发送的BGP路由数量。如果不合理，请增大本端允许接收的BGP路由最大数量 ○ 如果任意一项为否，则表明 BGP 会话不是由于接收到过多 BGP 路由而断开，请执行步骤 4 4. 执行 **display bgp peer log-info**命令，根据显示信息中的“Notification Error/SubError”字段打印的错误码和子错误码判断BGP连接断开的具体原因 如果错误码（Error）为4，表示BGP会话保持时间内本端未能收到对端的Keepalive或Update消息，导致BGP会话断开。如果错误码为5或6，表示TCP连接错误或主动关闭连

	接。可以通过如下方式进行排查： ○ 执行Ping命令查看本端是否能到达BGP对等体建立TCP连接使用的源地址。如果Ping不通，请执行 **display ip routing-table**命令查看是否存在能够到达BGP对等体地址的路由。如果不存在能够到达BGP对等体地址的路由，请排查IGP路由、静态路由或直连路由的相关配置 ○ 执行 **display memory-threshold**命令排查设备是否到达内存门限。如果内存到达门限，请执行步骤 5 ○ 执行 **display cpu-usage**命令排查设备CPU利用率是否过高。如果CPU利用率过高，请执行步骤 5 ○ 执行 **display acl all**命令，查看是否存在拒绝端口号为bgp或 179 的规则。如果存在这样的ACL，请配置删除该ACL ○ 执行 **display interface**命令，查看到达BGP对等体地址的路由下一跳出接口是否UP。如果出接口DOWN，请尝试在该接口视图下执行 **undo shutdown**命令开启该接口。如果接口开启失败或接口处于UP状态但告警仍未消除，请执行步骤 5 如果错误码（Error）为1或3，表示设备收到了错误的BGP报文。请执行步骤5 **5.** 如果执行上述所有操作后问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

11 BLS

本节介绍 BLS 模块输出的日志信息。

11.1 BLS_ENTRY_ADD

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
日志含义	添加黑名单表项
参数解释	$1：黑名单IP地址 $2：DS-Lite Tunnel 对端地址 $3：VPN名称 $4：老化时间 $5：添加原因
日志等级	5 (Notification)
举例	BLS/5/BLS_ENTRY_ADD: SrcIPAddr(1003)=1.1.1.6; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=; TTL(1051)=; Reason(1052)=Configuration. BLS/5/BLS_ENTRY_ADD: SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; TTL(1051)=10; Reason(1052)=Scan behavior detected.
对系统的影响	对系统无影响
日志产生原因	当日志开关打开时，手动配置一个黑名单或动态添加一个黑名单会触发此日志发送
处理建议	系统正常运行时产生的信息，无需处理

11.2 BLS_ENTRY_DEL

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
日志含义	删除黑名单表项
参数解释	$1：黑名单IP地址 $2：DS-Lite Tunnel对端地址 $3：VPN名称 $4：删除原因
日志等级	5 (Notification)
举例	BLS/5/BLS_ENTRY_DEL: SrcIPAddr(1003)=1.1.1.3; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=; Reason(1052)=Configuration. BLS/5/BLS_ENTRY_DEL: SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Reason(1052)=Aging.
对系统的影响	对系统无影响
日志产生原因	当日志开关打开时，手动删除一个黑名单或老化删除一个黑名单触发此日志发送
处理建议	系统正常运行时产生的信息，无需处理

11.3 BLS_IPV6_ENTRY_ADD

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
日志含义	添加IPv6黑名单表项
参数解释	$1：黑名单IPv6地址 $2：VPN名称 $3：老化时间 $4：添加原因
日志等级	5 (Notification)
举例	BLS/5/BLS_IPV6_ENTRY_ADD: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; TTL(1051)=; Reason(1052)=Configuration. BLS/5/BLS_IPV6_ENTRY_ADD: SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; TTL(1051)=10; Reason(1052)=Scan behavior detected.
对系统的影响	对系统无影响
日志产生原因	当日志开关打开时，手动配置一个IPv6黑名单或动态添加一个IPv6黑名单会触发此日志发送
处理建议	系统正常运行时产生的信息，无需处理

11.4 BLS_IPV6_ENTRY_DEL

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
日志含义	删除IPv6黑名单表项
参数解释	$1：黑名单IPv6地址 $2：VPN名称 $3：删除原因
日志等级	5 (Notification)
举例	BLS/5/BLS_IPV6_ENTRY_DEL: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; Reason(1052)=Configuration.
对系统的影响	对系统无影响
日志产生原因	当日志开关打开时，手动删除一个IPv6黑名单或老化删除一个IPv6黑名单会触发此日志发送
处理建议	系统正常运行时产生的信息，无需处理

12 CFD

本节介绍 CFD 模块输出的日志信息。

12.1 CFD_CROSS_CCM

日志内容	MEP [UINT16] in SI [INT32] received a cross-connect CCM. Its SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
日志含义	MEP收到交叉连接的CCM报文，该报文包含与本端不同的MA ID或MD ID
参数解释	$1：服务实例的ID $2：本地MEP的ID $3：源MAC地址 $4：序列号 $5：远端MEP的ID $6：MD的ID。如果不存在，会显示“without ID” $7：MA的ID
日志等级	6 (Informational)
举例	CFD/6/CFD_CROSS_CCM: MEP 13 in SI 10 received a cross-connect CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 78, RMEP is 12, MD ID is without ID, MA ID is 0.
对系统的影响	无法建立连通性检查
日志产生原因	两端MEP所属的MD和MA的配置不一致，两端MEP级别不相同、方向不相同
处理建议	检查两端MEP的配置。让MEP所属的MD和MA的配置一致，且两端MEP级别相同、方向都相同

12.2 CFD_ERROR_CCM

日志内容	MEP [UINT16] in SI [INT32] received an error CCM. Its SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
日志含义	MEP收到错误的CCM报文，该报文包含错误的MEP ID或生存时间
参数解释	$1：服务实例的ID $2：本地MEP的ID $3：源MAC地址 $4：序列号 $5：远端MEP的ID $6：MD的ID。如果不存在，会显示“without ID” $7：MA的ID
日志等级	6 (Informational)
举例	CFD/6/CFD_ERROR_CCM: MEP 2 in SI 7 received an error CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 21, RMEP is 2, MD ID is 7, MA ID is 1.
对系统的影响	无法建立连通性检查
日志产生原因	• 两端的 CC 检测周期配置不一致 • 远端 MEP ID 不在本端允许的 MEP 列表中
处理建议	检查CCM配置。让两端的CC检测周期配置一致，并配置远端MEP ID在本端允许的MEP列表中

12.3 CFD_LOST_CCM

日志内容	MEP [UINT16] in SI [INT32] failed to receive CCMs from RMEP [UINT16].
日志含义	MEP在3.5个CCM报文发送周期内没有收到CCM报文
参数解释	$1：本地MEP的ID $2：服务实例ID $3：远端MEP的ID
日志等级	6 (Informational)
举例	CFD/6/CFD_LOST_CCM: MEP 1 in SI 7 failed to receive CCMs from RMEP 2.
对系统的影响	无法建立连通性检测
日志产生原因	• 链路故障 • 两端的 CC 检测周期配置不一致
处理建议	检查链路状态和远端MEP的配置。如果链路down了或有其它的故障，例如单通故障，则恢复此链路。如果远端配置了同一服务实例的MEP，则确认两端的CC发送周期是一致的

12.4 CFD_RECEIVE_CCM

日志内容	MEP [UINT16] in SI [INT32] received CCMs from RMEP [UINT16]
日志含义	MEP收到远端MEP发送的CCM报文
参数解释	$1：本地MEP的ID $2：服务实例ID $3：远端MEP的ID
日志等级	6 (Informational)
举例	CFD/6/CFD_RECEIVE_CCM: MEP 1 in SI 7 received CCMs from RMEP 2.
对系统的影响	无
日志产生原因	MEP收到远端MEP发送的CCM报文
处理建议	无需处理

13 CFGMAN

本节介绍配置管理模块输出的日志信息。

13.1 CFGMAN_ARCHIVE_SCP_FAIL

日志内容	Archive configuration to SCP server failed: IP = [STRING], Directory = [STRING], Username = [STRING]
日志含义	设备向SCP服务器保存配置文件失败
参数解释	$1：SCP服务器的IP地址 $2：备份配置文件在SCP服务器上的保存目录 $3：登录SCP服务器的用户名
日志等级	5 (Notification)
举例	CFGMAN/5/CFGMAN_ARCHIVE_SCP_FAIL: Archive configuration to SCP server failed: IP = 192.168.21.21, Directory = /test/, Username = admin
对系统的影响	后续从SCP服务器进行配置回滚动作会操作失败
日志产生原因	• 配置文件在本地保存失败 • 服务器无法登录 • 服务器的存储空间不足
处理建议	1. 确认配置文件是否在本地保存成功 2. 确认服务器能否成功登录 3. 确认服务器的存储空间是否充足

13.2 CFGMAN_CFGCHANGED

日志内容	-EventIndex=[INT32]-CommandSource=[INT32]-ConfigSource=[INT32]-ConfigDestination=[INT32]; Configuration changed.
日志含义	设备将记录事件索引、引起配置变化的来源、源配置以及目的配置
参数解释	$1：事件索引，取值范围为1到2147483647 $2：引起配置变化的来源，取值为： • cli：表示引起配置变化的来源为命令行 • snmp：表示引起配置变化的来源为 SNMP 或者 SNMP 监控到配置数据库发生变化 • other：表示引起配置变化的来源为其它途径 $3：源配置，取值为： • erase：配置删除或重命名 • running：保存正在运行的配置 • commandSource：拷贝配置文件 • startup：保存运行配置到下次启动配置文件 • local：保存运行配置到本地文件 • networkFtp：通过 FTP 方式将网络上的某个配置文件保存到设备作为运行配置或者下次启动配置 • hotPlugging：热插拔板卡导致配置被删除或者失效 $4：目的配置，取值为： • erase：配置删除或重命名 • running：保存正在运行的配置 • commandSource：拷贝配置文件 • startup：保存运行配置到下次启动配置文件 • local：保存运行配置到本地文件 • networkFtp：通过 FTP 方式将网络上的某个配置文件保存到设备作为运行配置或者下次启动配置 • hotPlugging：热插拔板卡导致配置被删除或者失效
日志等级	5 (Notification)
举例	CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=6-CommandSource=snmp-ConfigSource=startup-ConfigDestination=running; Configuration changed.
对系统的影响	若为业务模块自发访问的DBM，可能会导致系统不断打印此日志
日志产生原因	• 用户执行了操作，例如下发了某条命令，或者执行了 snmp、netconf 操作，导致 dbm 中的配置发生变化 • 操作当前配置文件，例如删除、重命名、移动、保存配置文件 • 通过 FTP/TFTP 下载并覆盖配置文件 • 业务模块自发的访问 DBM，导致 DBM 中的配置发生变化
处理建议	• 若是用户执行操作，无需处理 • 若为业务模块自发访问的 DBM，表示业务模块出现问题，请联系技术支持

13.3 CFGMAN_EXIT_FROM_CONFIGURE

日志内容	Line=[STRING], IP address=[STRING], user=[STRING]; Exit from the system view or a feature view to the user view.
日志含义	记录交互模式下用户从系统视图、功能视图退出到用户视图
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**）
日志等级	5 (Notification)
举例	CFGMAN/5/CFGMAN_EXIT_FROM_CONFIGURE: Line=con0, IP address=**, user=**; Exit from the system view or a feature view to the user view.
对系统的影响	对系统无影响
日志产生原因	交互模式下，用户从系统视图、功能视图退出到用户视图
处理建议	无需处理

13.4 CFGMAN_OPTCOMPLETION

日志内容	-OperateType=[INT32]-OperateTime=[INT32]-OperateState=[INT32]-OperateEndTime=[INT32]; Operation completed.
日志含义	操作完成后记录操作的类型、状态以及时间
参数解释	$1：操作类型，取值为： • running2startup：将运行配置保存为下次启动配置 • startup2running：将下次启动配置设置为运行配置 • running2net：将运行配置保存到网络 • net2running：将网络上的配置文件上传到设备，并作为当前配置运行 • net2startup：将网络上的配置文件上传到设备，并保存为下次启动配置文件 • startup2net：将下次启动配置文件保存到网络 $2：操作时间 $3：操作状态，取值为： • InProcess：正在执行 • success：执行成功 • InvalidOperation：无效的操作 • InvalidProtocol：无效的协议 • InvalidSource：无效的源文件名 • InvalidDestination：无效的目的文件名 • InvalidServer：无效的服务器地址 • DeviceBusy：设备繁忙 • InvalidDevice：设备地址无效 • DeviceError：设备出错 • DeviceNotWritable：设备不可写 • DeviceFull：设备的存储空间不足 • FileOpenError：文件打开出错 • FileTransferError：文件传输出错 • ChecksumError：文件校验和错误 • LowMemory：没有内存 • AuthFailed：用户验证失败 • TransferTimeout：传输超时 • UnknownError：未知原因 • invalidConfig：无效配置 $4：操作结束时间
日志等级	5 (Notification)
举例	CFGMAN/5/CFGMAN_OPTCOMPLETION: -OperateType=running2startup-OperateTime=248-OperateState=success-OperateEndTime=959983; Operation completed.
对系统的影响	无
日志产生原因	用户操作完成后打印此日志

处理建议	请根据OperateState的值定位、处理问题

13.5 CFG_SAVE_FAILED

日志内容	形式一： Failed to save the current configuration. 形式二： Failed to save the current configuration on [STRING]. 形式三： Failed to save the current configuration. Reason: [STRING]. 形式四： Failed to save the current configuration for [STRING]. 形式五： Failed to save the current configuration on [STRING]. Reason: [STRING]. 形式六： Failed to save the current configuration [STRING].
日志含义	保存当前配置失败
参数解释	形式二： $1：当Slot仅支持单CPU时，表示Slot所在位置；当Slot支持多CPU时，表示CPU所在位置 形式三： $1：失败原因，取值包括： • No space available on the device：磁盘空间不足 • Failed to save the current configuration in binary format：二进制类型配置文件保存失败 • the memory is insufficient：内存不足 • Failed to set the next-startup configuration on *location*：设置板卡的下次启动配置文件失败。当Slot仅支持单CPU时，*location*表示Slot所在位置；当Slot支持多CPU时，*location*表示CPU所在位置 • the system is rebooting：正在重启中 • Operation not supported：操作不支持 • the memory on the memory file system is insufficient：内存文件系统空间不足 形式四： $1：MDC/Context *mdc-name*/*context-name* 形式五： $1：当Slot仅支持单CPU时，表示Slot所在位置；当Slot支持多CPU时，表示CPU所在位置 $2：失败原因，取值同形式三的失败原因 形式六： $1：失败原因
日志等级	4 (Warning)
举例	CFGMAN/4/CFG_SAVE_FAILED: Failed to save the current configuration because no space available on device.
对系统的影响	对系统无影响
日志产生原因	• 配置保存失败的原因，原因不明确的提示形式一

	• 对于形式二，一般在如下情况下输出：由于磁盘读写慢、磁盘损坏等原因，将配置文件备份到备用主控板失败 • 不提示板卡表示主用主控板和备用主控板配置保存失败，提示板卡表示指定板卡配置保存失败 • MDC/Context内的配置保存失败，具体信息请登录MDC/Context，执行 **display logbuffer**命令查看
处理建议	1. 执行 **dir**命令查看主用主控板和备用主控板的磁盘空间是否充足 2. 执行 **copy**命令检查主用主控板和备用主控板的磁盘是否可以正常Copy文件 3. 执行 **display memory**和 **display process memory**命令 查看内存信息，检查设备内存空间是否充足 4. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

13.6 CFG_SET_NEXTCFG_FAILED

日志内容	Failed to set [STRINT] as the [STRING] next-startup file on [STRING].
日志含义	设置下次启动配置文件失败
参数解释	$1：文件名 $2：主备属性，取值包括： • main：表示设置为主用下次启动配置文件 • backup：表示设置为备用下次启动配置文件 $3：当Slot仅支持单CPU时，表示Slot所在位置；当Slot支持多CPU时，表示CPU所在位置
日志等级	4 (Warning)
举例	CFGMAN/4/CFG_SET_NEXTCFG_FAILED: Failed to set startup.cfg as the main next-startup file on slot 1.
对系统的影响	对系统无影响
日志产生原因	• 配置文件不存在 • 配置文件内容不合法
处理建议	1. 请确认文件是否存在，文件内容是否合法 2. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

14 CGROUP

本节介绍 CGROUP（接口组联动）模块输出的日志信息。

14.1 CGROUP_STATUS_CHANGE

日志内容	The status of collaboration group [UINT32] is [STRING].
日志含义	显示接口组联动链路的状态
参数解释	$1：接口组联动ID $2：接口组联动状态 ○ down：故障 ○ up：正常
日志等级	6 (Informational)
举例	CGROUP/6/CGROUP_STATUS_CHANGE: The status of collaboration group 1 is up.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	接口组联动链路的状态发生变化
处理建议	通过**display collaboration-group**命令检查是由哪个接口故障导致的接口组故障，然后通过**display interface**命令中Cause字段的提示来恢复接口状态，从而恢复接口组联动链路的状态

15 CONNLMT

本节介绍连接数限制模块输出的日志信息。

15.1 CONNLMT_IPV4_OVERLOAD

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];UpperLimit(1049)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
日志含义	某IPv4连接数限制规则匹配流量的并发连接数超过阈值上限
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IP地址 $4：目的IP地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：上限值 $10：规则ID $11：Event信息
日志等级	6 (Informational)
举例	CONNLMT/6/CONNLMT_IPV4_OVERLOAD: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=10.10.10.1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;UpperLimit(1049)=1000;LimitRuleNum(1051)=1;Event(1048)=Exceeds upper threshold;
对系统的影响	符合该规则的流量无法新建连接
日志产生原因	当连接数的并发数超过策略中配置的上限时触发日志输出
处理建议	无需处理

15.2 CONNLMT_IPV4_RECOVER

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];DropPktCount(1052)=[UINT32];LowerLimit(1050)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
日志含义	某IPv4连接数限制规则匹配流量的并发连接数恢复至阈值下限
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IP地址 $4：目的IP地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：丢包数 $10：下限值 $11：规则ID $12：Event信息
日志等级	6 (Informational)
举例	CONNLMT/6/CONNLMT_IPV4_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=10.10.10.1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;DropPktCount(1052)=306004;LowerLimit(1050)=10;LimitRuleNum(1051)=1;Event(1048)=Reduces below lower threshold;
对系统的影响	无
日志产生原因	当连接数的并发数从达到上限恢复到下限时触发日志输出
处理建议	无需处理

15.3 CONNLMT_IPV6_OVERLOAD

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];UpperLimit(1049)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
日志含义	某IPv6连接数限制规则匹配流量的并发连接数超过阈值上限
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IPv6地址 $4：目的IPv6地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：上限值 $10：规则ID $11：Event信息
日志等级	6 (Informational)
举例	CONNLMT/6/CONNLMT_IPV6_OVERLOAD: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;UpperLimit(1049)=1000;LimitRuleNum(1051)=1;Event(1048)=Exceeds upper threshold;
对系统的影响	符合该规则的流量无法新建连接
日志产生原因	当连接数的并发数超过策略中配置的上限时触发日志输出
处理建议	无需处理

15.4 CONNLMT_IPV6_RECOVER

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];DropPktCount(1052)=[UINT32];LowerLimit(1050)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
日志含义	某IPv6连接数限制规则匹配流量的并发连接数恢复至阈值下限
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IPv6地址 $4：目的IPv6地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：丢包数 $10：下限值 $11：规则ID $12：Event信息
日志等级	6 (Informational)
举例	CONNLMT/6/CONNLMT_IPV6_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;DropPktCount(1052)=306004;LowerLimit(1050)=10;LimitRuleNum(1051)=1;Event(1048)=Reduces below lower threshold;
对系统的影响	无
日志产生原因	当连接数的并发数从达到上限恢复到下限时触发日志输出
处理建议	无需处理

16 DEV

本节介绍 DEV（设备管理）模块输出的日志信息。

16.1 AUTOSWITCH_FAULT

日志内容	[STRING] automatically switches between active and standby, and a fault occurs during the switching.
日志含义	设备自动切换主备的过程中出现故障
参数解释	$1：chassis编号
日志等级	1 (Alert)
举例	DEV/1/AUTOSWITCH_FAULT: Chassis 1 automatically switches between active and standby, and a fault occurs during the switching.
对系统的影响	设备主备倒换失败
日志产生原因	设备自动发生主备倒换，倒换过程中发生故障时，打印该日志
处理建议	• 用户可手工重启设备来尝试恢复故障。重启设备前，请执行 **display diagnostic-information**命令收集并保存诊断信息，以便定位故障 • 重启设备后，可执行 **display device**命令查看设备状态。如果状态不是Normal，表示故障未解除，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.2 AUTOSWITCH_FAULT_REBOOT

日志内容	[STRING] automatically switches between active and standby, and a fault occurs during the switching, the device will immediately restart [STRING] to restore the fault.
日志含义	设备自动切换主备的过程中出现故障，设备会立即自动重启故障单板来恢复故障
参数解释	$1：chassis编号 $2：chassis编号+slot编号或slot编号
日志等级	1 (Alert)
举例	DEV/1/AUTOSWITCH_FAULT_REBOOT: Chassis 1 automatically switches between active and standby, and a fault occurs during the switching, the device will immediately restart chassis 1 slot 0 to restore the fault.
对系统的影响	单板即将重启，单板将暂时无法工作
日志产生原因	设备自动发生主备倒换，倒换过程中出现故障，设备会立即自动重启故障单板来恢复故障时，打印该日志
处理建议	故障单板重启后，可执行**display device**命令查看单板状态。如果状态不是Normal，表示故障未解除，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.3 BOARD_ALARM_CLEAR

日志内容	Board alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[UINT], Reason=[STRING])
日志含义	单板重要告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/BOARD_ALARM_CLEAR: Board alarm cleared. (PhysicalIndex=140, PhysicalName=Level 1 Module 9 on Chassis 1, RelativeResource=(boardtype: LSXM1SFP08F1,chasiss:0,slot:6), ErrorCode=440013, Reason=FPGA SGMII interface came up.)
对系统的影响	对系统无影响
日志产生原因	单板重要告警恢复
处理建议	无需处理

表16-1 BOARD_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
540001	FPGA on subcard loading failure resolved.
500012	Subcard registration failure cleared.
500011	Subcard auto-power-off failure removed.
500010	Subcard power-up failure removed.
500007	$1 recovered from remote fault. $1：接口索引（框/槽/子卡/接口） The subcard recovered from the remote fault condition.
500006	PHY chip link recovered on $1. $1：接口索引（框/槽/子卡/接口） PHY chip link recovered on the subcard.
500005	MAC chip link recovered on $1. $1：接口索引（框/槽/子卡/接口） MAC chip link recovered on the subcard.
500004	Subcard in subslot $1 removed. $1：子卡槽位号 The unrecognized subcard was removed.
500003	PHY initialization failure was fixed on interface $1. $1：接口索引（框/槽/子卡/接口） Failure of initializing the connection between the PHY chip and interface was cleared.

故障码	故障原因描述
500001	The link status of $1 restored. $1：接口索引（框/槽/子卡/接口) The link status of the subcard restored.
486001	USB overcurrent error removed.
483003	Issue of mismatched sequence numbers in received packets was removed.
483002	The packet receive error was removed from the port.
483001	The port self-loop error was removed.
482010	License insufficiency-caused inoperative interface error removed.
478008	The PCIe BAR initialization failure was resolved.
478007	The PCIe initialization failure was resolved.
474016	No more broadcast IPC packets sent from itself were received.
474015	Verification failure of control channel detection packets from multiple boards cleared.
474014	Control channel detection packet verification failure cleared.
474013	No more unicast IPC packets sent from itself were received.
474010	Control plane restored the fully meshed state.
474009	Alarm condition cleared for the alarm that port $1 was connected to an MPU. $1：集群控制通道邻居端口 MPU-interconnect error removed.
474008	Alarm condition cleared for the alarm that port $1 was connected to $2. $1：集群控制通道邻居端口 $2：取值如下： • itself 本端口环回 • a port on the same MPU 本 MPU 的两个端口互联 • a port on the same MCCU 本 CCU 两个端口互联 • a port on the other MPU in the same chassis 本框两个 MPU 互联
474007	Neighbor chassis $1 slot $2 on port $3 changed from Init to Up. $1：集群控制通道邻居框号 $2：集群邻居控制通道槽位号 $3：集群控制通道邻居端口 Control channel neighbor up.
474006	Control channel port $1 did not receive error packets in the last 30 seconds. $1：集群控制通道端口 CRC error removed from the control channel.
474005	Control channel port $1 came up. $1：集群控制通道端口 Control channel port came up.
473007	Verification failure of data channel detection packets from multiple NPs cleared.
473006	Data channel self-loop packet verification failure cleared.

故障码	故障原因描述
473005	NP detection timeout ratio fell below the threshold.
473004	Data channel detection packet verification failure cleared.
447001	BITS PHY register read/write recovered.
446001	Channel selection failure was cleared from the I2C switch chip.
445002	SerDes MUX chip loss of lock error cleared.
445001	SerDes MUX chip read/write recovered.
444004	Number of MMU parity and ECC errors on the switch fabric chip dropped below the threshold.
444003	Number of unrecoverable parity and ECC errors in important entries on the switch fabric chip dropped below the threshold.
443001	Restored read/write access to the EMMC.
442001	Retimer read/write recovered.
441001	EEPROM read/write recovered.
440020	FPGA QSGMII interface came up.
440019	FPGA Interlaken interface resumed packet receiving.
440018	CRC error on the FPGA dead lock detection packet cleared.
440016	Restored access to the FPGA custom bus.
440015	FPGA 25GAUI interface came up.
440014	FPGA XAUI interface came up.
440013	FPGA SGMII interface came up.
440012	FPGA HiGig PTR FIFO overflow or underflow error removed.
440011	FPGA HiGig FIFO overflow error removed.
440009	FPGA SEU error removed.
440003	FPGA local bus error removed.
439003	Port on the Ethernet controller chip restored from half duplex mode to full duplex mode.
439002	Port speed decrease error removed from the Ethernet controller chip.
439001	Ethernet interface on the Ethernet controller chip came up.
438004	Port on the Ethernet switch chip restored from half duplex to full duplex mode.
438003	Port speed decrease error cleared from the Ethernet switch chip.
438001	Restored access to the GE switching chip.
435002	DDR initialization failure fixed.
434006	QAT resumed response to heartbeat detection.
434004	Board CPU restored communication with NP specific CPU.
434003	CPU node startup timeout error removed.
434002	CPU node came present.
434001	CPU node powered on.

故障码	故障原因描述
433003	$1 temperature chip restored to normal. $1：温度点描述 Restored access to the temperature sensor.
432034	Reference clock available for the clock board.
432033	Clock DPLL from holdover to locked.
432032	Clock DPLL from loss of lock to locked.
432031	Local clock input out of frequency error removed.
432030	Local clock input loss of signal error removed.
432029	Downstream clock input $1 out of frequency error removed. $1：时钟信号输入来源的描述，如：from MPU0、from MPU1等
432028	Downstream clock input $1 loss of signal error removed. $1：时钟信号输入来源的描述，如：from MPU0、from MPU1等
432027	Upstream clock input $1 out of frequency error removed. $1：时钟信号输入来源的描述，如：from MPU0、from MPU1等
432026	Upstream clock input $1 loss of signal error removed. $1：时钟信号输入来源的描述，如：from NP、,from interface等
432023	The clock chip initialization failure was resolved.
432016	Clock chip read/write recovered.
430002	RTC voltage increased to the acceptable range.
430001	RTC read/write recovered.
429003	The CPLD chip initialization failure was resolved.
428015	PHY line side loss of lock error cleared.
428014	PHY system side loss of lock error cleared.
428013	Interlaken link went up on the PHY chip.
428012	Number of CRC errors on the Interlaken link dropped below the threshold on the PHY chip.
428011	SDH SFBER alarm was removed.
428010	SDH SDBER alarm was removed.
428009	SDH MS-RDI alarm was removed.
428008	SDH TU-AIS alarm was removed.
428007	SDH MS-AIS alarm was removed.
428006	SDH LOP alarm was removed.
428005	SDH LOF alarm was removed.
428004	SDH LOS alarm was removed.
428003	The PHY chip initialization failure was resolved.
427003	The MAC chip initialization failure was resolved.

故障码	故障原因描述
425029	Number of CRC errors on TCAM Interlaken LA interface dropped below the threshold.
425028	TCAM Interlaken LA interface went up.
425027	Entry resources became sufficient on TCAM.
425026	Result FIFO parity error removed from TCAM.
425025	Context buffer parity error removed from TCAM.
425024	LTR error removed from TCAM.
425023	Memory read error removed on TCAM.
425022	Compare instruction lookup through LTR failure cleared on TCAM.
425021	PCIe request FIFO parity error removed from TCAM.
425020	TCAM Interlaken LA interface receive error removed: CRC24 error.
425019	TCAM Interlaken LA interface receive error removed: Framing bit error occurred on the PCS.
425018	EOP missing in the burst removed on the TCAM Interlaken LA interface.
425017	MAC FIFO parity error was removed from the TCAM Interlaken LA interface.
425016	SOP lost in the burst error removed from the TCAM Interlaken LA interface.
425015	TCAM Interlaken LA interface receive error removed: Received Interlaken packet instead of Interlaken look-aside packet.
425014	TCAM Interlaken LA interface receive error removed: No data burst.
425013	BurstMax error was removed from the TCAM Interlaken LA interface.
425012	TCAM Interlaken LA interface receive error removed: EOP error.
425011	TCAM Interlaken LA interface receive error removed: Illegitimate instruction.
425010	TCAM Interlaken LA interface receive error removed: Invalid instruction length.
425009	TCAM Interlaken LA interface transmit error removed.
425008	TCAM database error removed.
425007	TCAM Root Prefix Table (RPT) error removed.
425006	TCAM UDA (User Data) memory error removed.
425005	TCAM Unified Information Table (UIT) error removed.
425004	TCAM Interlaken LA interface error removed.
425003	TCAM core error removed.
425002	TCAM memory error removed.
425001	TCAM error removed on chip $2. Detailed information:$2. $1：芯片号 $2：None TCAM error removed.
423032	Fabric data receive FIFO full error removed from the switch chip.
423031	Virtual output queue idle error removed from the switch chip.

故障码	故障原因描述
423027	FE error removed, detailed information:ECC or parity error occurred on chip $1 memory $2. $1：芯片号 $2：寄存器表项名 ECC or parity error removed from the fabric chip.
423026	Switch error removed, detailed information:ECC or parity error occurred on chip $1 memory $2. $1：芯片号 $2：寄存器表项名 ECC or parity error removed from the switch chip.
423024	Rx power increased to normal range in cluster port $1 subport $2. $1：集群端口号 $2：集群子端口号 Rx power on the bundle subport increased to the normal range.
423022	No less than two ports are in up state. No port is in up state.
423017	Chip $1 was released from isolation. $1：Chip ID，芯片编号 The number of up bundle ports increased by the threshold, and the FE chip was released from isolation.
423016	Chassis $1 slot $2 has $3 uplink ports. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 $3：Port ID：端口编号 The large up bundle port quantity difference was removed because the quantity difference decreased to 2 or smaller. No fabric module is present in Chassis $1 slot $2. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 The large up bundle port quantity difference was removed because the fabric module is not present. Chassis $1 slot $2 is abnormal. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 The large up bundle port quantity difference was removed because the fabric module is abnormal. Chassis $1 is not connected to a peer chassis. $1：Chassis ID，机框编号 The large up bundle port quantity difference was removed because the fabric module is not connected to a peer chassis. Chassis $1 is abnormal. $1：Chassis ID，机框编号 The large up bundle port quantity difference was removed because the chassis is abnormal. User executed command to forcibly change the error status to be fixed.

故障码	故障原因描述
423015	Chip $1 port $2 recovered. $1：Chip ID，芯片编号 $2：Port ID，端口编号 CRC error removed from the chip port, and the chip port was released from isolation.
423014	Bundle port $1 fiber $2 connection error removed. $1：Port ID,集群捆绑口编号 $2：SubPort ID,集群捆绑子接口编号 The bundle port connection error was removed.
423013	The hardware resources were freed up. Hardware resources on the switch chip restored.
423010	Chip $1 port $2 recovered. $1：Chip ID，芯片编号 $2：Port ID，端口编号 The port recovered.
423001	The connection error detected for the bundle port in slot $1/$2 was removed. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 The bundle port connection error was removed.
422022	PMU blocking issue removed from NP $1 side. $1：取值如下： • west • east
422021	TND blocking issue removed from NP $1 side. $1：取值如下： • Link：子卡侧接口 • fabric：交换网侧接口 • host：主机接口 • host loopback：主机环回接口
422020	Receive FIFO blocking issue removed from NP $1 side. $1：取值如下： • Link：子卡侧接口 • fabric：交换网侧接口 • host：主机接口 • host loopback：主机环回接口
422019	NP CPU hardware thread recovered.
422018	Internal memory BIST test failure removed from NP.
422017	DDR BIST test failure removed from NP.
421003	The PD recovered from the overcurrent condition.
421002	Invalid PD class issue cleared.

故障码	故障原因描述
420001	Restored access to voltage chip channel $1 on $2 chip $3. $1：电压芯片通道号 $2：chassis编号+slot编号或slot编号 $3：电压芯片编号 Restored access to the voltage monitor chip.
400009	The fabric board communication failure with the slave MPU over the control channel at startup was cleared.
400005	Board powered up.
400003	Card in slot $1 removed. $1：槽位号 The board not recognized by the system was removed.
200029	No enough power to power on the subcard. Subcard insufficient power issue resolved.
185003	Detected signals from the ToD port.
185002	Detected signals from the 1PPS port.
185001	Detected signals from the BITS port.
100049	Fan trays are available for dissipating heat for the board.
100048	Subcard present/absent state became stable.
100046	Board offline alarm cleared.
100045	Board startup timeout error removed.
100044	Board auto-power-off error removed.
100043	Board present/absent signal error cleared: The board is absent, and the IPC port is down. Board present/absent signal error removed: The board is present, and the IPC port is up.
100042	Board present/absent state became stable.
100041	Current board type consistent with the previous one.
100039	MPU present/absent state inconsistency error removed.
100038	No more incorrect slot ID information sent from the board. The board that reported absent slot information was rebooted or removed.
100037	The removal misreport error was removed.
100036	The reset misreport error was removed.
100032	Incorrect signal indication of the active/standby MPU role error removed.
100031	The microswitches of the board were turned off. Microswitch turned-on error cleared.
100022	The port was disconnected from the port on the same MCCU.
100021	The port was disconnected from the port on the same MPU.
100020	The port was disconnected from the port on the other MPU in the same chassis.

16.4 BOARD_ALARM_OCCUR

日志内容	Board alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	单板重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/BOARD_ALARM_OCCUR: Board alarm occurred. (PhysicalIndex=140, PhysicalName=Level 1 Module 9 on Chassis 1, RelativeResource=(boardtype: LSXM1SFP08F1,chasiss:0,slot:6), ErrorCode=540001, Reason=FPGA on subcard loading failed.)
对系统的影响	单板上的业务可能会受到影响
日志产生原因	单板重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	1. 请使用 **display device**命令检查机框单板工作状态，确保单板处于正常运行状态 2. 如果本机框内的单板处于正常运行状态，但故障未恢复，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-2 BOARD_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
540001	FPGA on subcard loading failed.
500012	Subcard failed to register with the system.
500011	Subcard auto powered off.
500010	Subcard failed to power up.
500007	$1 received remote fault from its peer interface. $1：接口索引（框/槽/子卡/接口） The subcard port received remote fault signal from its peer interface.
500006	PHY chip link failure detected on $1. $1：接口索引（框/槽/子卡/接口） PHY chip link failure detected on the subcard.
500005	MAC chip link failure detected on $1. $1：接口索引（框/槽/子卡/接口） MAC chip link failure detected on the subcard.
500004	Subcard in subslot $1 is not identified. Model = $2, OEM = $3.

故障码	故障原因描述
	$1：子卡槽位号； $2：读取到的子卡硬件ID； $3：读取到的子卡OEM ID。 Subcard is not recognized. Subcard ID = $1, OEM = $2. $1：读取到的子卡硬件ID； $2：读取到的子卡OEM ID。
500003	PHY initialization failed on interface $1. $1：接口索引（框/槽/子卡/接口） Failed to initialize the connection between the interface and the PHY chip.
500002	An error occurred on the subcard in $1/$2: $3. $1：槽号 $2：子槽号 $3：原因 Initiation error occurred on the subcard. An error removed from the subcard in $1/$2. $1：槽号 $2：子槽号 Initiation error removed from the subcard.
500001	The link of $1 remained down after interface initialization. Reason: $2. $1：接口索引（框/槽/子卡/接口） $2 接口down的原因 The link of the subcard remained down after interface initialization.
486001	USB overcurrent error.
483003	The port received packets with mismatched sequence numbers.
483002	The port failed to receive packets from its peer.
483001	The port was self-looped.
482010	The interface is up but inoperative because of insufficient licenses.
478008	The PCIe BAR failed to initialize.
478007	The PCIe failed to initialize.
474016	Received broadcast IPC packets sent from itself. $1：IPC报文中的目的MAC地址。
474015	Control channel detection packets from multiple boards failed to be verified.
474014	Control channel detection packet verification failure.
474013	Received unicast IPC packets sent from itself: Dest MAC=$1. $1：IPC报文中的目的MAC地址。
474010	Control plane changed to a non-full-mesh state. Please examine the connections.
474009	Port $1 was connected to an MPU. Please connect it to an MCCU. $1：集群控制通道邻居端口 The port was connected to an MPU. Please connect it to an MCCU.

故障码	故障原因描述
474008	Port $1 was connected to $2. $1：集群控制通道邻居端口 $2：取值如下： • itself 本端口环回 • a port on the same MPU 本 MPU 的两个端口互联 • a port on the same MCCU 本 CCU 两个端口互联 • a port on the other MPU in the same chassis 本框两个 MPU 互联
474007	Neighbor chassis $1 slot $2 on port $3 changed from Up to Down. $1：集群控制通道邻居框号 $2：集群邻居控制通道槽位号 $3：集群控制通道邻居端口 Control channel neighbor down.
474006	Control channel port $1 received error packets. $1：集群控制通道端口 CRC error occurred on the control channel.
474005	Control channel port $1 went down. $1：集群控制通道端口 Control channel port went down.
473007	Data channel detection packets from multiple NPs failed to be verified.
473006	Data channel self-loop packet verification failure.
473005	NP detection timeout ratio exceeded the threshold.
473004	Data channel detection packet verification failure.
447001	BITS PHY register read/write failed.
446001	Channel selection failed on the I2C switch chip.
445002	SerDes MUX chip loss of lock.
445001	SerDes MUX chip read/write failed.
444004	Number of MMU parity and ECC errors on the switch fabric chip reached or exceeded the threshold.
444003	Number of unrecoverable parity and ECC errors in important entries on the switch fabric chip reached or exceeded the threshold.
443001	Failed to read/write the EMCC.
442001	Retimer read/write failed.
441001	EEPROM read/write failed.
440020	FPGA QSGMII interface went down.
440019	FPGA Interlaken interface failed to receive packets.
440018	CRC error occurred on the FPGA dead lock detection packet.
440016	Failed to access the FPGA custom bus.
440015	FPGA 25GAUI interface went down.

故障码	故障原因描述
440014	FPGA XAUI interface went down.
440013	FPGA SGMII interface went down.
440012	FPGA HiGig PTR FIFO overflow or underflow error.
440011	FPGA HiGig FIFO overflow error.
440009	FPGA SEU error.
440003	FPGA local bus error.
439003	Port on the Ethernet controller chip changed to half duplex mode.
439002	Port speed on the Ethernet controller chip decreased below $1. $1：端口支持的速率，如1Gbps等。
439001	Ethernet interface on the Ethernet controller chip went down.
438004	Port on the Ethernet switch chip changed to half duplex mode.
438003	Port speed on the Ethernet switch chip decreased below $1. $1：端口支持的速率，如1Gbps等。
438001	Failed to access the GE switching chip.
435002	DDR initialization failed.
434006	QAT unresponsive to heartbeat detection.
434004	Board CPU failed to communicate with NP specific CPU.
434003	CPU node startup timeout error.
434002	CPU node went absent.
434001	CPU node powered off.
433003	$1 temperature chip became faulty. $1：温度点描述 Failed to access the temperature sensor.
432034	No reference clock available for the clock board.
432033	Clock DPLL holdover.
432032	Clock DPLL loss of lock.
432031	Local clock input out of frequency error.
432030	Local clock input loss of signal error.
432029	Downstream clock input $1 out of frequency error. $1：时钟信号输入来源的描述，如：from MPU0、from MPU1等等，
432028	Downstream clock input $1 loss of signal. $1：时钟信号输入来源的描述，如：from MPU0、from MPU1等等，
432027	Upstream clock input $1 out of frequency. $1：时钟信号输入来源的描述，如：from NP,from interface等等
432026	Downstream 8 KHz clock signal error. Upstream clock input $1 loss of signal.

故障码	故障原因描述
	$1：时钟信号输入来源的描述，如：from NP,from interface等等
432023	The clock chip failed to initialize.
432016	Clock chip read/write failed.
430002	RTC voltage low.
430001	RTC read/write failed.
429003	The CPLD chip failed to initialize.
428015	PHY line side loss of lock.
428014	PHY system side loss of lock.
428013	Interlaken link went down on the PHY chip.
428012	Number of CRC errors on the Interlaken link reached or exceeded the threshold on the PHY chip.
428011	SDH SFBER alarm occurred.
428010	SDH SDBER alarm occurred.
428009	SDH MS-RDI alarm occurred.
428008	SDH TU-AIS alarm occurred.
428007	SDH MS-AIS alarm occurred.
428006	SDH LOP alarm occurred.
428005	SDH LOF alarm occurred.
428004	SDH LOS alarm occurred.
428003	The PHY chip failed to initialize.
427003	The MAC chip failed to initialize.
425029	Number of CRC errors on TCAM Interlaken LA interface reached or exceeded the threshold.
425028	TCAM Interlaken LA interface went down.
425027	Insufficient entry resources on TCAM.
425026	Result FIFO parity error on TCAM.
425025	Context buffer parity error on TCAM.
425024	LTR error on TCAM.
425023	Memory read error on TCAM.
425022	Compare instruction lookup through LTR failed on TCAM.
425021	PCIe request FIFO parity error occurred on TCAM.
425020	TCAM Interlaken LA interface receive error: CRC24 error.
425019	TCAM Interlaken LA interface receive error: Framing bit error occurred on the PCS.
425018	EOP was found missing in the burst on the TCAM Interlaken LA interface.
425017	MAC FIFO parity error occurred on the TCAM Interlaken LA interface.
425016	SOP lost in the burst received on the TCAM Interlaken LA interface.

故障码	故障原因描述
425015	TCAM Interlaken LA interface receive error: Received Interlaken packet instead of Interlaken look-aside packet.
425014	TCAM Interlaken LA interface receive error: No data burst.
425013	BurstMax error occurred on the TCAM Interlaken LA interface.
425012	TCAM Interlaken LA interface receive error: EOP error.
425011	TCAM Interlaken LA interface receive error: Illegitimate instruction.
425010	TCAM Interlaken LA interface receive error: Invalid instruction length.
425009	TCAM Interlaken LA interface transmit error.
425008	TCAM database error.
425007	TCAM Root Prefix Table (RPT) error.
425006	TCAM UDA (User Data) memory error.
425005	TCAM Unified Information Table (UIT) error.
425004	TCAM Interlaken LA interface error.
425003	TCAM core error.
425002	TCAM memory error.
425001	TCAM error on chip $1. Detailed information:$2. $1：芯片号 $2：SoftErr TCAM error.
423032	Fabric data receive FIFO full error on the switch chip.
423031	Virtual output queue idle error on the switch chip.
423027	FE error, detailed information: ECC or parity error occurred on chip $1 memory $1. $1：芯片号 $2：寄存器表项名 ECC or parity error occurred on the fabric chip.
423026	Switch error, detailed information:ECC or parity error occurred on chip $1 memory $2. $1：芯片号 $2：寄存器表项名 ECC or parity error occurred on the switch chip.
423024	Low Rx power in cluster port $1 subport $2. $1：集群端口号 $2：集群子端口号 Low Rx power on the bundle subport.
423022	Only port $1 is up. A minimum of two ports must be in up state. $1：Port ID，端口编号 The number of up bundle ports is less than 2.
423017	Chip $1 was isolated. Reason: The number of up ports fell below the threshold. $1：Chip ID，芯片编号

故障码	故障原因描述
	The number of up bundle ports fell below the threshold, and the FE chip was isolated.
423016	Number of system maximum uplink ports is $1. Chassis $2 slot $3 has only $4 uplink ports. The difference between the numbers must be equal to or less than two. $1：Port ID：端口编号 $2：Chassis ID，机框编号 $3：Slot ID，槽位编号 $4：Port Number：端口数量 Number of system maximum uplink ports is $1.The board has only $2 uplink ports. The difference between the numbers must be equal to or less than two. $1：Port Number：最大端口数量 $2：Port Number：端口数量
423015	Chip $1 port $2 was disabled. Reason: The port received data with CRC errors.$3 $1：Chip ID，芯片编号 $2：Port ID，端口编号 $3：The peer cannot be recognized.（获取不到对端端口信息时打印） The peer is chassis %s slot %u bundle port %u subport %u chip %u port %u.（能获取到对端端口信息时打印） CRC error occurred on the chip port of the bundle port and the chip port was isolated.
423014	Bundle port $1 subport $2 connected to an incorrect subport. Please check. $1：Port ID,集群捆绑口编号 $2：SubPort ID,集群捆绑子接口编号 The bundle port was connected to a bundle port operating in the same mode. Please check.
423013	The hardware resources were exhausted. • Hardware resources on the switch chip were exhausted because of too many multicast outgoing interfaces.
423010	Chip $1 port $2 went down or flapped. Please secure the cards in chassis $3 slot $4 and chassis$3 slot $4 firmly. $1：Chip ID，芯片编号 $2：Port ID，端口编号 $3：Chassis ID，机框编号 $4：Slot ID，槽位编号 • The port went down or flapped. Please ensure firm installation of the board.
423001	A connection error was detected for the bundle port in slot $1/$2. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 • The bundle port was connected to a wrong bundle port.
422022	PMU blocked on NP $1 side. $1：取值如下： • west • east
422021	TND blocked on NP $1 side.

故障码	故障原因描述
	$1：取值如下： • link：子卡侧接口 • fabric：交换网侧接口 • host：主机接口 host loopback：主机环回接口
422020	Receive FIFO blocked on NP $1 side. $1：取值如下： • link：子卡侧接口 • fabric：交换网侧接口 • host：主机接口 • host loopback：主机环回接口
422019	NP CPU hardware thread failure.
422018	Internal memory BIST test failed on NP.
422017	DDR BIST test failed on NP.
421003	Overcurrent occurred on the PD.
421002	Invalid PD class.
420001	Failed to access voltage chip channel $1 on $2 chip $3. $1：电压芯片通道号 $2：chassis编号+slot编号或slot编号 $3：电压芯片编号 Failed to access the voltage monitor chip.
400009	The fabric board failed to communicate with the slave MPU over the control channel at startup.
400005	Board failed to power up.
400003	Card in slot $1 is not identified. Model = $2, OEM = $3. $1：槽位号 $2：单板ID $3：制造信息 The board is not recognized. Board ID = $1, OEM ID = $2 . $1：读取到的子卡硬件ID； $2：读取到的子卡OEM ID。
200029	No enough power to power on the subcard. The required power is $1 W. $1：整机需要的功率数值
185003	Lost signals from the ToD port.
185002	Lost signals from the 1PPS port.
185001	Lost signals from the BITS port.
100049	No fan trays are available for dissipating heat for the board.
100048	Subcard present/absent state flapped.

故障码	故障原因描述
100046	Board went offline.
100045	Board startup timeout error.
100044	Board auto powered off.
100043	Board present/absent signal error: The board is absent, but the IPC port is up.
100042	Board present/absent state flapped.
100041	Current board type inconsistent with the previous one.
100039	MPU present/absent state inconsistent between hardware and software.
100038	Received slot ID information of another normal board from a board. Received slot ID information of an absent slot from a board.
100037	A removal was misreported for the board.
100036	A reset was misreported for the board.
100032	Incorrect signal indication of the active/standby MPU role.
100031	Only one microswitch of the board was turned on. Both microswitch of the board were turned on.
100022	The port was connected to a port on the same MCCU.
100021	The port was connected to a port on the same MPU.
100020	The port was connected to a port on the other MPU in the same chassis.
100001	Board removed.

16.5 BOARD_FATALALARM_CLEAR

日志内容	Board fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	单板紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/BOARD_FATALALARM_CLEAR: Board fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
对系统的影响	对系统无影响
日志产生原因	单板紧急故障恢复
处理建议	无需处理

表16-3 BOARD_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
493002	Leak sensors rope breaking issue removed.
493001	Issue that leak sensors rope detected leakage was removed.
474012	Control channe $1 switching failure cleared. $1：控制通道功能名称，如used for IPC等
440017	FPGA HG interface came up.
440010	FPGA PCIe access failure resolved.
440008	FPGA PLL locked.
440007	FPGA dead lock error removed.
440006	FPGA CAUI interface came up.
440005	FPGA XFI interface came up.
440004	FPGA Interlaken interface came up.
438002	One or more ports on the Ethernet switch chip came up.
429002	CPLD bus error removed.
429001	CPLD register read/write recovered.
423029	All interfaces on the switch fabric came up.
423023	PCIe link faults fixed on chip $1. $1：Chip ID，芯片编号 PCIe channel of the switch chip recovered. PCIe link fixed from configuration loss: chip $1, type $2. $1：Chip ID，芯片编号 $2：Type，故障消息类型 PCIe channel of the switch chip recovered after a reconfiguration.
423021	Transceiver module $1 connection error removed. $1：Module ID,光模块编号 The bundle port was connected to the correct port.
423020	Chip $1 was released from isolation. $1：Chip ID，芯片编号 The fabric chip was released from isolation.
423019	Fabric port $1/$2/$3/$4 was released from isolation. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 $3：Chip ID，芯片编号 $4：Port ID，端口编号 SFI port on the fabric chip was connected correctly, and the port was released from isolation.
423018	Port $1 subport $2 was released from isolation. $1：Port ID,集群捆绑口编号

故障码	故障原因描述
	$2：SubPort ID,集群捆绑子接口编号 The bundle subport was released from isolation because the data channel port recovered.
423012	Chip $1 was release from isolation. $1：Chip ID，芯片编号 The switch chip was release from isolation, because the number of down ports dropped below the threshold.
423011	Failed to clear CRC errors on the OCB of FAP $1, and the NP was isolated. $1：Chip ID，芯片编号 Failed to clear CRC errors on the switch chip OCB, and the NP connected to the switch chip was isolated. CRC errors on the OCB of the switch chip were cleared.
423003	Forward path between FAP and FE error removed.Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 One or more SFI ports on the switch chip recovered.
423002	CRC errors on the DRAM that the switch chip connects were cleared.
422015	NP HG interface came up.
422011	NP CAUI interface came up.
422010	NP XLAUI interface came up.
422009	NP XFI interface came up.
422008	NP SGMII interface came up.
422007	NP QSGMII interface came up.
422004	Deadlock error removed from chip $1. $1：芯片号。 The NP recovered from deadlock.
422003	PCI_OFFLOAD error removed from chip $1. $1：芯片号 PCI_OFFLOAD error removed from NP.
422002	Uncorrectable ECC error removed from chip $1. $1：芯片号 Uncorrectable ECC error removed from the NP.
400006	The temperature of the card in slot $1 restored. $1：槽位号 The temperature of the board restored.
100035	Active MPU information inconsistency between the board and the chassis cleared.
100004	Active/standby MPU information signal anomaly cleared.
100003	System status change to normal because the $1 board inserted. $1：单板类型

16.6 BOARD_FATALALARM_OCCUR

日志内容	Board fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	单板紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/BOARD_FATALALARM_OCCUR: Board fatal alarm occurred. (PhysicalIndex=180136, PhysicalName=Level 1 Module 5 on Chassis 2, RelativeResource=(2/5/0), ErrorCode=10035, Reason=Active MPU information on the board inconsistent with that of the real active MPU in the chassis.)
对系统的影响	单板上的业务可能会受到影响
日志产生原因	单板紧急故障产生时，打印该日志，详情请参见故障原因描述
处理建议	1. 请使用 display device命令检查机框单板工作状态，确保单板处于正常运行状态 2. 如果本机框内的单板处于正常运行状态，但故障未恢复，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-4 BOARD_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
493002	Leak sensors rope broke.
493001	Leakage detected by leak sensors rope.
474012	Failed to switch control channel $1 from port $2. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 Failed to switch control channel $1 from port $2 to port $3 because isolation configuration switchover failed. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 $3：控制通道切换的目的端口号 Failed to switch control channel $1 from port $2 to port $3 because of insufficient VLAN resources. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 $3：控制通道切换的目的端口号 Failed to switch control channel $1 from port $2 to port $3 because of insufficient MAC entry resources. $1：控制通道功能名称，如used for IPC等

故障码	故障原因描述
	$2：原控制通道端口号 $3：控制通道切换的目的端口号 Failed to switch control channel $1 from port $2 to port $3 because of insufficient MAC cache resources. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 $3：控制通道切换的目的端口号 Failed to switch control channel $1 from port $2 to port $3 because of insufficient multicast resources. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 $3：控制通道切换的目的端口号 Failed to switch control channel $1 from port $2 to port $3 because inter-board notification failed. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 $3：控制通道切换的目的端口号 Failed to switch control channel $1 from port $2 to port $3 because of insufficient software resources. $1：控制通道功能名称，如used for IPC等 $2：原控制通道端口号 $3：控制通道切换的目的端口号
440017	FPGA HG interface went down.
440010	FPGA PCIe access failure.
440008	FPGA PLL unlocked.
440007	FPGA dead lock error.
440006	FPGA CAUI interface went down.
440005	FPGA XFI interface went down.
440004	FPGA Interlaken interface went down.
440001	FPGA loading failed.
438002	All ports on the Ethernet switch chip went down.
429002	CPLD bus error.
429001	CPLD register read/write failed.
423029	All interfaces on the switch fabric went down.
423023	PCIe link faults occurred: chip $1, fault count $2. $1：Chip ID，芯片编号 $2：Counter，错误计数 PCIe channel of the switch chip is faulty.
423021	Transceiver module $1 connection error. $1：Module ID，光模块编号 The bundle port was connected to a bundle port operating in the same mode.

故障码	故障原因描述
423020	Chip $1 was isolated. Reason: No internal ports are up. $1：Chip ID，芯片编号 No internal ports on the fabric chip are up, and the fabric chip is isolated.
423019	Fabric port $1/$2/$3/$4 connected to port $1/$2/$3/$4 incorrectly. The fabric port was isolated. $1：Chassis ID，机框编号 $2：Slot ID，槽位编号 $3：Chip ID，芯片编号 $4：Port ID，端口编号 SFI port on the fabric chip connected to a wrong chip, and the port was isolated.
423018	Port $1 subport $2 was isolated. $1：Port ID,集群捆绑口编号 $2：SubPort ID,集群捆绑子接口编号 The bundle subport was isolated because an error occurred on the data channel port.
423012	Chip $1 was isolated. Reason: $2 ports of the chip are down. The ports are connected to $3/$4 fabric modules. $1：Chip ID，芯片编号 $2：Port Number，端口数量 $3：Fabric Module Number：芯片上处于down状态端口连接网板的数量 $4：Total Fabric Module Number：机框内网板的总数量 $1 ports on the switch chip went down, and the switch chip was isolated. $1：Port Number，端口数量 The switch chip was isolated because of system expansion.
423011	CRC errors occurred on the OCB of FAP $1, and the FAP was reset. $1：Chip ID，芯片编号 CRC error occurred on the switch chip OCB.
423003	Forward path between FAP and FE error occurred. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 All SFI ports on the switch chip are faulty.
423002	CRC errors on DRAM $1 connected to FAP $2 exceeded the threshold. The system made $3 CRC error corrections. $1：Path ID,DRAM芯片编号 $2：Chip ID,FAP交换芯片编号 $3：Counter,系统矫正DRAM芯片参数的次数 CRC errors on the DRAM connected to the switch chip exceeded the threshold. CRC errors on DRAM $1 connected to FAP $2 exceeded the threshold. The system made $3 CRC error corrections but failed. $1：Path ID,DRAM芯片编号 $2：Chip ID,FAP交换芯片编号 $3：Counter,系统矫正DRAM芯片参数的次数 CRC errors on the DRAM connected to the switch chip exceeded the threshold. The

故障码	故障原因描述
	system made $1 CRC error corrections but failed. $1：Counter,系统矫正DRAM芯片参数的次数
422015	NP HG interface went down.
422011	NP CAUI interface went down.
422010	NP XLAUI interface went down.
422009	NP XFI interface went down.
422008	NP SGMII interface went down.
422007	NP QSGMII interface went down.
422004	Deadlock error occurred on chip $1, and chip isolation $2. $1：芯片号 $2：隔离结果，取值如下： • succeeded • failed The NP ran into deadlock, and NP isolation $1. $1：隔离结果，取值如下： • succeeded • failed Deadlock error occurred on the NP. The NP rebooted automatically for self-healing and $1. $1：重启结果，取值如下： • succeeded • failed The NP ran into deadlock, and the NP was reset.
422003	PCI_OFFLOAD error occurred on chip $1, and chip isolation $2. $1：芯片号 $2：隔离结果，取值如下： • succeeded • failed PCI_OFFLOAD error occurred on the NP, and NP isolation $1. $1：隔离结果，取值如下： • succeeded • failed PCI_OFFLOAD error occurred on the NP. The NP rebooted automatically for self-healing and $1. $1：重启结果，取值如下： • succeeded • failed PCI_OFFLOAD error occurred on NP, and the NP was reseted.
422002	Uncorrectable ECC error occurred on chip $1, and chip isolation $2. $1：芯片号 $2：隔离结果，取值如下：

故障码	故障原因描述
	• succeeded • failed Uncorrectable ECC error occurred on the NP, and NP isolation $1. $1：隔离结果，取值如下： • succeeded • failed Uncorrectable ECC error occurred on the NP. The NP rebooted automatically for self-healing and $1. $1：重启结果，取值如下： • succeeded • failed Uncorrectable ECC error occurred on the NP, and the NP was reset.
400006	The card in slot $1 was powered off because the temperature exceeded the high temperature shutdown threshold. $1：槽位号 The board in slot $1 was powered off because the temperature exceeded the high temperature shutdown threshold. $1：槽位号
100035	Active MPU information on the board inconsistent with that of the real active MPU in the chassis.
100004	Active/standby MPU information signal anomaly.
100003	System can't work without the $1 board. $1：单板类型

16.7 BOARD_INSERTED

日志内容	Board was inserted on [STRING], type is unknown.
日志含义	有单板插入设备，但单板类型未知
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5 (Notification)
举例	DEV/5/BOARD_INSERTED: Board was inserted on slot 1, type is unknown.
对系统的影响	对系统无影响
日志产生原因	单板插入设备后，需要一段时间才能完成启动，这段时间内打印该日志
处理建议	无需处理

16.8 BOARD_REBOOT

日志内容	Board is rebooting on [STRING].
日志含义	单板正在重新启动
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5 (Notification)
举例	DEV/5/BOARD_REBOOT: Board is rebooting on slot 1.
对系统的影响	单板即将停止服务，重新启动
日志产生原因	用户在重启指定单板，或者指定单板因为异常而重启
处理建议	1. 检查是否有用户在重启指定单板 2. 如果没有用户重启单板，等待指定单板重新启动后，通过 display version命令、对应指定单板信息中的Last reboot reason字段，查看重启原因 3. 如果重启原因为异常重启，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.9 BOARD_REMOVED

日志内容	Board was removed from [STRING], type is [STRING].
日志含义	一块LPU或者备用MPU从设备中拔出
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	3 (Error)
举例	DEV/3/BOARD_REMOVED: Board was removed from slot 1, type is LSQ1FV48SA.
对系统的影响	单板不可用
日志产生原因	一块LPU或者备用MPU从设备中拔出，设备退出IRF
处理建议	1. 如果单板被拔出，无需处理 2. 如果单板没有被拔出，检查单板是否正确安装，重新安装单板；检查单板是否损坏，如果损坏，请更换单板；重新将设备加入 IRF 3. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.10 BOARD_STATE_FAULT

日志内容	Board state changed to Fault on [STRING], type is [STRING].
日志含义	单板状态转为Fault状态
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	2 (Critical)
举例	DEV/2/BOARD_STATE_FAULT: Board state changed to Fault on slot 1, type is LSQ1FV48SA.
对系统的影响	单板不可用
日志产生原因	单板在以下情况会处于Fault（故障）状态： • 单板处于启动阶段（正在初始化或者加载软件版本），单板不可用 • 单板不能正常工作
处理建议	根据日志产生的情况，处理建议如下： • 对于第一种情况：单板型号不同，加载的软件版本不同，启动所需的时间不同。一般不超过 10 分钟，请以设备的实际情况为准 • 对于第二种情况：请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.11 BOARD_STATE_NORMAL

日志内容	Board state changed to Normal on [STRING], type is [STRING].
日志含义	一块新插入的LPU或者备用MPU完成了初始化
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	5 (Notification)
举例	DEV/5/BOARD_STATE_NORMAL: Board state changed to Normal on slot 1, type is LSQ1FV48SA.
对系统的影响	对系统无影响
日志产生原因	一块新插入的LPU或者备用MPU完成了初始化。打印该日志，并不代表配置恢复完成，不能进行主备倒换
处理建议	无需处理

16.12 BOARD_STATE_STARTING

日志内容	Board state changed to Starting on [STRING], type is unknown.
日志含义	单板状态切换到启动阶段，单板状态为未知
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5 (Notification)
举例	DEV/5/BOARD_STATE_STARTING: Board state changed to Starting on slot 1, type is unknown.
对系统的影响	单板不可用
日志产生原因	单板处于启动阶段（正在初始化或者加载软件版本），不能正常工作时，打印该日志
处理建议	1. 查看单板型号和设备型号是否适配 2. 查看启动文件和设备软件版本以及硬件是否适配 3. 单板型号不同，加载的软件版本不同，启动所需的时间不同。一般不超过 10 分钟，请以设备的实际情况为准

16.13 BOARD_WARNING_CLEAR

日志内容	Board warning alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	单板告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/BOARD_WARNING_CLEAR: Board warning alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
对系统的影响	对系统无影响
日志产生原因	单板告警恢复
处理建议	无需处理

表16-5 BOARD_WARNING_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
700009	CF card read/write error fixed.
448001	TPM chip error removed.
444006	The transmit bandwidth usage of the switch fabric chip link (connecting the switch chip)

故障码	故障原因描述
	dropped below $1. $1：带宽使用率门限
444005	The receive bandwidth usage of the switch fabric chip link (connecting the switch chip) dropped below $1. $1：带宽使用率门限
444002	Number of hardware and software entry inconsistency errors on the switch fabric chip dropped below the threshold.
444001	Number of parity and ECC errors on the switch fabric chip dropped below the threshold.
436001	Flash read/write error fixed.
435001	CPU DDR ECC error removed.
434005	CPU Cache error removed.
428016	SDH OOF alarm was removed.
428002	Restored read/write access to the PHY chip.
427002	Restored access to the MAC chip.
423037	The transmit bandwidth usage of the switch chip link (connecting the switch fabric chip) dropped below $1. $1：带宽使用率门限
423036	The receive bandwidth usage of the switch chip link (connecting the switch fabric chip) dropped below $1. $1：带宽使用率门限
423035	The switch chip Interlaken transmit bandwidth usage dropped below $1. $1：带宽使用率门限
423034	The switch chip Interlaken receive bandwidth usage dropped below $1. $1：带宽使用率门限
423033	Number of parity and ECC errors on the switch chip dropped below the threshold.
422001	Correctable ECC error removed from chip $1. $1：芯片号 Correctable ECC error removed from the NP.
400004	Card in slot $1 registered with the system successfully. $1：槽位号 Board registered with the system successfully.
400002	$1 at chassis $2 slot $3 unsupport error removed. $1：单板名称 $2：框号 $3：槽位号 Board unsupported error was removed.
423033	Number of parity and ECC errors on the switch chip reached or exceeded the threshold.
100007	Subcard supported in the specified slot on the card.
100002	Board inserted.

16.14 BOARD_WARNING_OCCUR

日志内容	Board warning alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	单板告警产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/BOARD_WARNING_OCCUR: Board warning alarm occurred. (PhysicalIndex=180136, PhysicalName=Level 1 Module 5 on Chassis 2, RelativeResource=(2/5/0), ErrorCode=700009, Reason=Failed to read/write the CF card.)
对系统的影响	单板上的业务可能会受到影响
日志产生原因	单板告警产生时，打印该日志，详情请参见故障原因描述
处理建议	1. 请使用 **display device**命令检查机框单板工作状态，确保单板处于正常运行状态 2. 如果本机框内的单板处于正常运行状态，但故障未恢复，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-6 BOARD_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
700009	Failed to read/write the CF card.
448001	TPM chip error.
444006	The transmit bandwidth usage of the switch fabric chip link (connecting the switch chip) exceeded $1. $1：带宽使用率门限
444005	The receive bandwidth usage of the switch fabric chip link (connecting the switch chip) exceeded $1. $1：带宽使用率门限
444002	Number of hardware and software entry inconsistency errors on the switch fabric chip reached or exceeded the threshold.
444001	Number of parity and ECC errors on the switch fabric chip reached or exceeded the threshold.
436003	Too many bad blocks on the NAND flash.
436001	Failed to read/write the flash.
435001	CPU DDR ECC error.
434005	CPU Cache error.

故障码	故障原因描述
428016	SDH OOF alarm occurred.
428002	Failed to read/write the PHY chip.
427002	Failed to access the MAC chip.
423037	The transmit bandwidth usage of the switch chip link (connecting the switch fabric chip) exceeded $1. $1：带宽使用率门限
423036	The receive bandwidth usage of the switch chip link (connecting the switch fabric chip) exceeded $1. $1：带宽使用率门限
423035	The switch chip Interlaken transmit bandwidth usage exceeded $1. $1：带宽使用率门限
423034	The switch chip Interlaken receive bandwidth usage exceeded $1. $1：带宽使用率门限
423033	Number of parity and ECC errors on the switch chip reached or exceeded the threshold.
422001	Correctable ECC error occurred on chip $1. $1：芯片号 Correctable ECC error occurred on the NP.
400004	Card in slot $1 failed to register with the system. $1：槽位号 Board failed to register with the system.
400002	$1 at chassis $2 slot $3 can not be supported. $1：单板名称 $2：框号 $3：槽位号 The board is not supported.
100008	Subcard incompatible with the card.
100007	Subcard not supported in the specified slot on the card.

16.15 CFCARD_INSERTED

日志内容	CF card was inserted in [STRING] [STRING].
日志含义	CF卡安装到了指定槽位
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	4 (Warning)
举例	DEV/4/CFCARD_INSERTED: CF card was inserted in slot 1 CF card slot 1.
对系统的影响	对系统无影响
日志产生原因	CF卡安装到了指定槽位，打印该日志
处理建议	无需处理

16.16 CFCARD_REMOVED

日志内容	CF card was removed from [STRING] [STRING].
日志含义	CF卡从设备中拔出
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	3 (Error)
举例	DEV/3/CFCARD_REMOVED: CF card was removed from slot 1 CF card slot 1.
对系统的影响	CF卡不可用
日志产生原因	CF卡从设备中拔出时，打印该日志
处理建议	**1.** 如果 CF 卡被拔出，无需处理 **2.** 如果 CF 卡没有被拔出，检查 CF 卡是否正确安装，重新安装 CF 卡；检查 CF 卡是否损坏，如果损坏，请更换 CF 卡 **3.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.17 CLOCK_ALARM_CLEAR

日志内容	Clock alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	时钟重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/CLOCK_ALARM_CLEAR: Clock alarm cleared. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:clock,chasiss:0,slot:5,subslot:5,chipid:0,port:5), ErrorCode=432025, Reason=Downstream clock signal error removed.)
对系统的影响	对系统无影响
日志产生原因	时钟重要故障恢复
处理建议	无需处理

表16-7 CLOCK_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
432025	Downstream clock signal error removed.
432024	Upstream clock signal error removed.
432022	Clock PLL chip locked.
432021	Upstream 8 KHz clock signal error removed.
432020	Downstream 8 KHz clock signal error removed.
432019	Downstream TOD signal error removed.
432018	Downstream IPPS signal error removed.
432017	Clock synchronization tracing recovered between the chassis in a cluster.
432011	Frequency offset decreased to the normal range.
432009	PLL clock locked on the downstream clock signal channel.
432008	PLL clock locked on the upstream clock signal channel.
432007	PLL clock incorrect frequency error removed from the downstream clock signal channel.
432006	PLL clock incorrect frequency error removed from the upstream clock signal channel.
432005	PLL clock output resumed on the downstream clock signal channel.
432004	PLL clock output resumed on the upstream clock signal channel.
432002	Error removed from downstream clock signal channel: Oscillator output restored.
432001	Oscillator clock output resumed on the upstream clock signal channel.

16.18 CLOCK_ALARM_OCCUR

日志内容	Clock alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	时钟重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/CLOCK_ALARM_OCCUR: Clock alarm occurred. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:clock,chasiss:0,slot:5,subslot:5,chipid:0,port:5), ErrorCode=432025, Reason=Downstream clock signal error.)
对系统的影响	系统业务可能会受到影响
日志产生原因	时钟重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-8 CLOCK_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
432025	Downstream clock signal error.
432024	Upstream clock signal error.
432022	Clock PLL chip unlocked.
432021	Upstream 8 KHz clock signal error.
432020	Downstream 8 KHz clock signal error.
432019	Downstream TOD signal error.
432018	Downstream IPPS signal error.
432017	Clock synchronization tracing failed between the chassis in a cluster.
432011	Frequency offset exceeded the threshold.
432009	PLL clock unlocked on the downstream clock signal channel.
432008	PLL clock unlocked on the upstream clock signal channel.
432007	PLL clock incorrect frequency error on the downstream clock signal channel.
432006	PLL clock incorrect frequency error on the upstream clock signal channel.
432005	No PLL clock output on the downstream clock signal channel.
432004	No PLL clock output on the upstream clock signal channel.

故障码	故障原因描述
432002	Error occurred on downstream clock signal channel: No output from the oscillator.
432001	No oscillator clock output on the upstream clock signal channel.

16.19 CLOCK_FATALALARM_CLEAR

日志内容	Clock fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	时钟紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/CLOCK_FATALALARM_CLEAR: Clock fatal alarm cleared. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:clock,chasiss:0,slot:5,subslot:5,chipid:0,port:5), ErrorCode=432003, Reason=The board local clock recovered.)
对系统的影响	对系统无影响
日志产生原因	时钟紧急故障恢复
处理建议	无需处理

表16-9 CLOCK_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
432003	The board local clock recovered.

16.20 CLOCK_FATALALARM_OCCUR

日志内容	Clock fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	时钟紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/CLOCK_FATALALARM_OCCUR: Clock fatal alarm occurred. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:clock,chasiss:0,slot:5,subslot:5,chipid:0,port:5), ErrorCode=432003, Reason=The board local clock failed.)
对系统的影响	系统业务可能会受到影响
日志产生原因	时钟紧急故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-10 CLOCK_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
432003	The board local clock failed.

16.21 CHASSIS_REBOOT

日志内容	Chassis [STRING] is rebooting now.
日志含义	成员设备正在重新启动
参数解释	$1：chassis编号
日志等级	5 (Notification)
举例	DEV/5/CHASSIS_REBOOT: Chassis 1 is rebooting now.
对系统的影响	成员设备即将停止服务，重新启动
日志产生原因	用户在重启成员设备，或者成员设备因为异常而重启，打印该日志
处理建议	1. 检查是否有用户在重启成员设备 2. 如果没有用户在重启成员设备，等待成员设备重新启动后，通过 **display version** 命令、对应成员设备单板信息中的Last reboot reason字段，查看重启原因 3. 如果重启原因为异常重启，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.22 DEV_BOARD_RUNNING_FAULT

日志内容	[STRING] is detected to be faulty.
日志含义	检测到单板故障
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	1 (Alert)
举例	DEV/1/DEV_BOARD_RUNNING_FAULT: Chassis 1 slot 0 is detected to be faulty.
对系统的影响	单板上的业务可能会受到影响
日志产生原因	设备运行过程中检测到单板发生故障时，打印该日志
处理建议	• 用户可手工重启故障单板来尝试恢复故障。重启单板前，可以执行 **display diagnostic-information**命令收集并保存诊断信息，以便定位故障 • 重启单板后，可执行 **display device**命令查看单板状态。如果状态不是Normal，表示故障未解除，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.23 DEV_BOARD_RUNNING_FAULT_REBOOT

日志内容	[STRING] is detected to be faulty, the device will immediately restart [STRING] to recover from the fault.
日志含义	设备运行过程中检测到单板发生故障，设备将立即重启单板来恢复故障
参数解释	$1：chassis编号+slot编号或slot编号 $2：chassis编号+slot编号或slot编号
日志等级	1 (Alert)
举例	DEV/1/DEV_BOARD_RUNNING_FAULT_REBOOT: Chassis 1 slot 0 is detected to be faulty, the device will immediately restart chassis 1 slot 0 to recover from the fault.
对系统的影响	单板即将重启，单板将暂时无法工作
日志产生原因	设备运行过程中检测到单板发生故障，设备将立即重启单板来恢复故障时，打印该日志
处理建议	单板自动重启后，可执行**display device**命令查看设备状态。如果单板的状态不是Normal，表示故障未解除，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.24 DEV_CLOCK_CHANGE

日志内容	-User=[STRING]-IPAddr=[IPADDR]; System clock changed from [STRING] to [STRING].
日志含义	系统时间发生改变
参数解释	$1：当前登录用户的用户名 $2：当前登录用户的IP地址 $3：老时间 $4：新时间
日志等级	5 (Notification)
举例	DEV/5/DEV_CLOCK_CHANGE: -User=admin-IPAddr=192.168.1.2; System clock changed from 15:49:52 01/02/2013 to 15:50:00 01/02/2013.
对系统的影响	可能导致后台定时程序失效
日志产生原因	系统时间发生改变时，打印该日志。可能原因包括： • 管理员手工修改系统时间 • 时钟协议自动修改系统时间
处理建议	1. 检查后台定时程序配置 2. 修改自动失效的后台定时程序

16.25 DEV_FAULT_TOOLONG

日志内容	Card in [STRING] is still in Fault state for [INT32] minutes.
日志含义	单板长期处于Fault状态
参数解释	$1：chassis编号+slot编号或slot编号 $2：状态的持续时间
日志等级	4 (Warning)
举例	DEV/4/DEV_FAULT_TOOLONG: Card in slot 1 is still in Fault state for 60 minutes.
对系统的影响	单板不可用
日志产生原因	单板长期处于Fault状态，打印该日志
处理建议	1. 重启单板，尝试恢复单板状态 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.26 DISK_ALARM_CLEAR

日志内容	Disk alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	硬盘重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/DISK_ALARM_CLEAR: Disk alarm cleared. (PhysicalIndex=9, PhysicalName=HDD, RelativeResource=(disktype:HDD,chasiss:2,slot:3,subslot:1,diskid:0001:00:08.0 - 1), ErrorCode=700005, Reason=Restored read/write access to the disk.)
对系统的影响	对系统无影响
日志产生原因	硬盘重要故障恢复
处理建议	无需处理

表16-11 DISK_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
700005	Restored read/write access to the disk.
486002	Errors causing read/write failure to the USB storage medium were rectified.

16.27 DISK_ALARM_OCCUR

日志内容	Disk alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	硬盘重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/DISK_ALARM_OCCUR: Disk alarm occurred. (PhysicalIndex=9, PhysicalName=HDD, RelativeResource=(disktype:HDD,chasiss:2,slot:3,subslot:1,diskid:0001:00:08.0 - 1), ErrorCode=700005, Reason=Failed to read/write the disk.)
对系统的影响	硬盘上的业务可能会受到影响
日志产生原因	硬盘重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	如果本机框内的单板处于正常运行状态，但故障未恢复，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-12 DISK_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
700005	Failed to read/write the disk.
486002	Failed to read/write the USB storage medium.

16.28 DISK_WARNING_CLEAR

日志内容	Disk warning alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	硬盘告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/DISK_WARNING_CLEAR: Disk warning alarm cleared. (PhysicalIndex=9, PhysicalName=HDD, RelativeResource=(disktype:HDD,chasiss:2,slot:3,subslot:1,diskid:0001:00:08.0 - 1), ErrorCode=700003, Reason=Disk inserted.)
对系统的影响	对系统无影响
日志产生原因	硬盘告警恢复
处理建议	无需处理

表16-13 DISK_WARNING_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
700003	Disk inserted.
486004	USB storage medium inserted.

16.29 DISK_WARNING_OCCUR

日志内容	Disk warning alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	硬盘告警产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/DISK_WARNING_OCCUR: Disk warning alarm occurred. (PhysicalIndex=9, PhysicalName=HDD, RelativeResource=(disktype:HDD,chasiss:2,slot:3,subslot:1,diskid:0001:00:08.0 - 1), ErrorCode=70000, Reason=Disk removed.)
对系统的影响	硬盘上的业务可能会受到影响
日志产生原因	硬盘告警产生时，打印该日志，详情请参见故障原因描述
处理建议	如果本机框内的单板处于正常运行状态，但故障未恢复，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-14 DISK_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
700002	Disk removed.
486003	USB storage medium removed.

16.30 FAN_ABSENT

日志内容	形式一： Fan [INT32] is absent. 形式二： Chassis [STRING] fan [INT32] is absent.
日志含义	风扇模块从设备中拔出
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	3 (Error)
举例	DEV/3/FAN_ABSENT: Fan 2 is absent.
对系统的影响	可能影响系统散热
日志产生原因	指定位置未安装风扇模块，或风扇模块从设备中拔出时，打印该日志
处理建议	**1.** 如果指定位置未安装风扇模块，则可能因散热不好，引起设备温度升高，建议安装风扇 **2.** 如果风扇模块被拔出，无需处理 **3.** 如果风扇模块没有被拔出，请检查风扇模块是否正确安装，如风扇模块未插紧等，并确认风扇模块是否损坏，如果损坏，请更换风扇模块 **4.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.31 FAN_ALARM_CLEAR

日志内容	Fan alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	风扇重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/FAN_ALARM_CLEAR: Fan alarm cleared. (PhysicalIndex=7, PhysicalName=fan, RelativeResource=(fantype:type, chasiss:2,fantray:1,fanid:8), ErrorCode=300005, Reason=Consistent fan tray model.)
对系统的影响	对系统无影响
日志产生原因	风扇重要故障恢复
处理建议	无需处理

表16-15 FAN_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
300008	Fan speed calibrated with the configured value: Actual speed = $1 RPM, Configured speed = $2 RPM. $1：风扇实际转速 $2：风扇调速转速要求 Fan with large speed deviation was removed.
300006	Fan tray configuration now meets the heat dissipation requirements.
300005	Consistent fan tray model.
300004	The fan tray $1 is compatible with the system now. $1：风扇框编号 Fan tray incompatibility issue removed. The incompatibale fan tray $1 is removed. $1：风扇框编号 The incompatible fan tray was removed.
300002	Fan $1 speed increased to the normal range. $1：风扇框编号+风扇编号或风扇编号 Fan speed increased to the normal range. Low speed fan was removed.
300001	Fan tray $1 recovered. $1：风扇框编号 Fan tray anomaly removed.

16.32 FAN_ALARM_OCCUR

日志内容	Fan alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	风扇重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/FAN_ALARM_OCCUR: Fan alarm occurred. (PhysicalIndex=7, PhysicalName=fan, RelativeResource=(fantype:type, chasiss:2,fantray:1,fanid:8), ErrorCode=300005, Reason=Inconsistent fan tray models.)
对系统的影响	可能影响系统散热
日志产生原因	风扇重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-16 FAN_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
300008	Fan speed deviated largely from the configured value: Actual speed = $1 RPM, Configured speed = $2 RPM. $1：风扇实际转速 $2：风扇调速转速要求
300006	Fan tray configuration does not meet the heat dissipation requirements.
300005	Inconsistent fan tray models.
300004	The fan tray $1 is not compatible with the system. $1：风扇框编号 Fan tray not compatible with the system.
300002	Fan $1 speed fell below the lower speed threshold. $1：风扇框编号+风扇编号或风扇编号 Fan speed fell below the lower speed threshold.
300001	Fan tray $1 failed. $1：风扇框编号 Fan tray is faulty. Fan tray $1 is absent. $1：风扇框编号 Fan tray is absent.

16.33 FAN_DIRECTION_NOT_PREFERRED

日志内容	Fan [INT32] airflow direction is not preferred [STRING], please check it.
日志含义	风扇的风道方向不适合，请检查
参数解释	$1：风扇ID $2：chassis编号+slot编号或slot编号
日志等级	1 (Alert)
举例	DEV/1/FAN_DIRECTION_NOT_PREFERRED: Fan 1 airflow direction is not preferred slot 1, please check it.
对系统的影响	可能影响系统散热
日志产生原因	风扇的风道方向不是用户期望的方向。风扇方向配置出错或者插错风扇
处理建议	**1.** 根据机房通风系统的风向，选择风向一致的型号的风扇 **2.** 如果风扇风向和机房通风系统风向一致，请调整风扇风向的配置

16.34 FAN_FAILED

日志内容	形式一： Fan [INT32] failed. 形式二： Chassis [STRING] fan [INT32] failed.
日志含义	风扇出现故障
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	2 (Critical)
举例	DEV/2/FAN_FAILED: Fan 2 failed.
对系统的影响	可能影响系统散热
日志产生原因	风扇出现了故障，停止工作
处理建议	请更换风扇

16.35 FAN_FATALALARM_CLEAR

日志内容	Fan fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	风扇紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/FAN_FATALALARM_CLEAR: Fan fatal alarm cleared. (PhysicalIndex=7, PhysicalName=fan, RelativeResource=(fantype:type, chasiss:2,fantray:1,fanid:8), ErrorCode=300007, Reason=Fan that had stopped running was removed.)
对系统的影响	对系统无影响
日志产生原因	风扇紧急故障恢复
处理建议	无需处理

表16-17 FAN_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
300007	The fan $1 resumed running. $1：风扇框编号+风扇编号或风扇编号 Fan resumed running. Fan that had stopped running was removed.

16.36 FAN_FATALALARM_OCCUR

日志内容	Fan fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	风扇紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/FAN_FATALALARM_OCCUR: Fan fatal alarm occurred. (PhysicalIndex=7, PhysicalName=fan, RelativeResource=(fantype:type, chasiss:2,fantray:1,fanid:8), ErrorCode=300007, Reason=Fan stopped running.)
对系统的影响	可能影响系统散热
日志产生原因	风扇紧急故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-18 FAN_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
300007	The fan $1 stopped running. $1：风扇框编号+风扇编号或风扇编号 Fan stopped running.

16.37 FAN_RECOVERED

日志内容	形式一： Fan [INT32] recovered. 形式二： Chassis [INT32] fan [INT32] recovered.
日志含义	风扇状态转为正常工作状态
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	2 (Critical)
举例	DEV/2/FAN_RECOVERED: Fan 2 recovered.
对系统的影响	对系统无影响
日志产生原因	插入风扇，稍后，风扇转为正常工作状态
处理建议	无需处理

16.38 INTERNALLINK_ALARM_CLEAR

日志内容	Internal link alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	内部接口重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/INTERNALLINK_ALARM_CLEAR: Internal link alarm cleared. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(subcard:type,chasiss:0,slot:9.1,subslot:1), ErrorCode=484001, Reason=Subport came up.)
对系统的影响	对系统无影响
日志产生原因	内部接口重要故障恢复
处理建议	无需处理

表16-19 INTERNALLINK_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
484001	Subport came up.
482008	FEC enabling status matches the transceiver type.
482007	Traffic statistics decreased to the normal range. CurrentValue = $1, Threshold =$2. $1：当前端口流量值，一般用百分比表示 $2：端口流量上限阈值
482006	FCS error removed from IRF link.
482005	Number of CRC errors dropped below the threshold.
482004	IRF link flapping issue removed.
482003	The IRF interface came up.
482002	The interface Physical state changed to up.
482001	Recovered from remote fault.
481003	Number of CRC errors on HiGig link dropped below the threshold.
481002	HiGig link flapping issue removed.
481001	HiGig link came up.
479003	Number of CRC errors on the Interlaken link dropped below the threshold.
474004	Packet loss error removed. Source port = $1, Destination port =$2. $1：链路源端信息 $2：链路目的端信息 Packet loss error removed from the inter-board IPC channel. IPC destination board was removed. Source port = $1, Destination port = $2. $1：链路源端信息 $2：链路目的端信息 Packet loss error removed from the inter-board IPC channel because the destination board was removed.
474002	Number of errors on the $1 link $2 dropped below the fault threshold. Source port = $3, Destination port = $4. $1：链路名称前缀 $2：链路名称，取值如下： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP n：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot n：连接 slot n 的链路，n 为 slot 号 • to NP n：连接 NP n 的链路，n 为 NP 号，取值为 0～5 $3：链路源端信息 $4：链路目的端信息

故障码	故障原因描述
	Number of errors on the IPC channel dropped below the fault threshold.
473003	SGMII interface came up.
473002	Error removed from the data channel between switch chips.
473001	Error removed from the data channel between switch chip and switch fabric chip.
428001	PHY chip link recovered.
427001	MAC chip link recovered.
423009	Interlaken link flapping issue removed. Source port = $1. $1：链路源端口描述 The switch chip Interlaken port stopped flapping.
423008	Number of CRC errors on Interlaken link dropped below the threshold. Source port = $1. $1：链路源端口描述 Interlaken link CRC error dropped below the threshold on switch chip.
423007	Chip $1 port $2 was released from isolation. $1：Chip ID，芯片编号 $2：Port ID，端口编号 The switch chip SFI port was released from isolation.
423006	The SFI link Recovered from an error-down state. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 The switch chip SFI port came up.
423005	SFI link flapping issue removed. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 The switch chip SFI port stopped flapping.
423004	FCS error removed on SFI link. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 CRC error removed from the switch chip SFI port.
422014	Number of CRC errors on NP Interlaken LA interface dropped below the threshold.
422013	NP interlaken LA interface came up.
422006	Number of CRC errors on Interlaken link dropped below the threshold. Source port =$1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 Number of CRC errors on the NP fabric Interlaken interface dropped below the threshold.
422005	Interlaken link came up. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述

故障码	故障原因描述
	NP fabric Interlaken interface came up.

16.39 INTERNALLINK_ALARM_OCCUR

日志内容	Internal link alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	内部接口重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/INTERNALLINK_ALARM_OCCUR: Internal link alarm occurred. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(subcard:type,chasiss:0,slot:9.1,subslot:1), ErrorCode=484001, Reason=Subport went down.)
对系统的影响	接口上的业务可能会受到影响
日志产生原因	内部接口重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-20 INTERNALLINK_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
484001	Subport went down.
482008	FEC enabling status does not match the transceiver type.
482007	Traffic statistics exceeded the threshold. CurrentValue = $1, Threshold =$2. $1：当前端口流量值，一般用百分比表示 $2：端口流量上限阈值，一般用百分比表示
482006	FCS error occurred on IRF link.
482005	Number of CRC errors reached or exceeded the threshold.
482004	IRF link flapped.
482003	The IRF interface went down.
482002	The interface Physical state changed to down.
482001	Remote fault error.
481003	Number of CRC errors on HiGig link reached or exceeded the threshold.
481002	HiGig link flapped.
481001	HiGig link went down.

故障码	故障原因描述
479003	Number of CRC errors on the Interlaken link reached or exceeded the threshold.
474004	Packet loss occurred on inter-board IPC channel. Source port = $1, Destination port = $2. Detailed information = $3. $1：链路源端信息 $2：链路目的端信息 $3：详细故障信息 Packet loss occurred on the inter-board IPC channel.
474002	Number of errors on the $1 link $2 reached or exceeded the fault threshold. Source port = $3, Destination port = $4. $1：链路名称前缀 $2：链路名称，取值如下： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP n：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot n：连接 slot n 的链路，n 为 slot 号 • to NP n：连接 NP n 的链路，n 为 NP 号，取值为 0～5 $3：链路源端信息 $4：链路目的端信息 Number of CRC errors on the IPC channel reached or exceeded the threshold.
473003	SGMII interface went down.
473002	An error occurred on the data channel between switch chips.
473001	An error occurred on the data channel between switch chip and switch fabric chip.
428001	PHY chip link failure detected.
427001	MAC chip link failure.
423009	Interlaken link flapped. Source port = $1. $1：链路源端口描述 The switch chip Interlaken port flapped.
423008	Number of CRC errors on Interlaken link reached or exceeded the threshold. Source port = $1. $1：链路源端口描述 CRC errors on the switch chip Interlaken port reached or exceeded the threshold.
423007	Chip $1 port $2 was isolated. Reason: The port went down. $1：Chip ID，芯片编号 $2：Port ID，端口编号 The switch chip SFI port went down and was isolated.
423006	The SFI link went down due to an error. Source port = $1, Destination port = $2. $1：链路源端口描述

故障码	故障原因描述
	$2：链路目的端口描述 The switch chip SFI port went down.
423005	SFI link flappings occurred. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 The switch chip SFI port flapped.
423004	FCS error occurred on SFI link. Source port = $1, Destination port = $2. $1：链路源端口描述 $2：链路目的端口描述 CRC error occurred on the switch chip SFI port.
422014	Number of CRC errors on NP Interlaken LA interface reached or exceeded the threshold.
422013	NP interlaken LA interface went down.
422006	Number of CRC errors on Interlaken link reached or exceeded the threshold. Source port = $1, Destination port =$2. $1：链路源端口描述 $2：链路目的端口描述 Number of CRC errors on the NP fabric Interlaken interface reached or exceeded the threshold.
422005	Interlaken link went down. Source port = $1, Destination port =$2. $1：链路源端口描述 $2：链路目的端口描述 NP fabric Interlaken interface went down.

16.40 INTERNALLINK_FATALALARM_CLEAR

日志内容	Internal link fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	内部接口紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/INTERNALLINK_FATALALARM_CLEAR: Internal link fatal alarm cleared. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(subcard:type,chasiss:0,slot:9.1,subslot:1), ErrorCode=479002, Reason=Interlaken link flapping issue removed.)
对系统的影响	对系统无影响
日志产生原因	内部接口紧急故障恢复
处理建议	无需处理

表16-21 INTERNALLINK_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
479002	Interlaken link flapping issue removed.
479001	Interlaken link came up.
478006	PCIe unknown link error removed.
478005	PCIe link status error removed.
478004	Restored access to the PCIe link.
478003	Configuration loss error removed from the PCIe link.
478002	PCIe link came up.
478001	PCIE $1 removed from chip $2 bus $3 dev $4 func $5. $1：PCIE故障详情，取值如下： • link down • config lost • memory access failure • status error • unkown error • $2：PCIE 芯片名称，如 bcm53406 0.1 • $3：PCIE bus 号 • $4：PCIE device 号 • $5：PCIE function 号

故障码	故障原因描述
	• PCIE $1 removed. $1：PCIE故障详情，取值如下： • link down error • config lost error • memory access failure • status error • unkown error
474011	IPC link flapping issue removed.
474003	Recovered packet receiving or sending over the $1 link $2. Source port = $3, Destination port = $4. $1：链路名称前缀 $2：链路名称，取值如下： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP n：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot n：连接 slot n 的链路，n 为 slot 号 • to NP n：连接 NP n 的链路，n 为 NP 号，取值为 0～5 $3：链路源端信息 $4：链路目的端信息 Recovered packet receiving or sending on the intra-board IPC channel.
474001	The $1 link $2 came up. Source port = $3, Destination port = $4. $1：链路名称前缀 $2：链路名称后缀，取值如下： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP n：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot n：连接 slot n 的链路，n 为 slot 号 • to NP n：连接 NP n 的链路，n 为 NP 号，取值为 0～5 $3：链路源端信息 $4：链路目的端信息 The IPC channel came up.

16.41 INTERNALLINK_FATALALARM_OCCUR

日志内容	Internal link fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	内部接口紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/INTERNALLINK_FATALALARM_OCCUR: Internal link fatal alarm occurred. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(subcard:type,chasiss:0,slot:9.1,subslot:1), ErrorCode=479002, Reason=Interlaken link flapped.)
对系统的影响	接口上的业务可能会受到影响
日志产生原因	内部接口紧急故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-22 INTERNALLINK_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
479002	Interlaken link flapped.
479001	Interlaken link went down.
478006	PCIe link unkown error.
478005	PCIe link status error.
478004	Failed to access the PCIe link.
478003	Configuration loss error occurred on the PCIe link.
478002	PCIe link went down.
478001	PCIE $1 occurred on chip $2 bus $3 dev $4 func $5. $1：PCIE故障详情，取值如下： • link down • config lost • memory access failure • status error • unkown error $2：PCIE芯片名称，如bcm53406 0.1 $3：PCIE bus号 $4：PCIE device号 $5：PCIE function号 PCIE $1 occurred.

故障码	故障原因描述
	$1：PCIE故障详情，取值如下： • link down • config lost • memory access failure • status error • unknown error
474011	IPC link flapped.
474003	Failed to receive or send packets over the $1 link $2. Source port = $3, Destination port = $4. $1：链路名称前缀 $2：链路名称，取值如下： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP n：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot n：连接 slot n 的链路，n 为 slot 号 • to NP n：连接 NP n 的链路，n 为 NP 号，取值为 0～5 $3：链路源端信息 $4：链路目的端信息 Failed to receive or send packets on the intra-board IPC channel.
474001	The $1 link $2 went down. Source port = $3, Destination port = $4. $1：链路名称前缀； $2：链路名称后缀，取值如下： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP n：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot n：连接 slot n 的链路，n 为 slot 号 • to NP n：连接 NP n 的链路，n 为 NP 号，取值为 0～5 $3：链路源端信息 $4：链路目的端信息 The IPC channel went down.

16.42 MAD_DETECT

日志内容	Multi-active devices detected, please fix it.
日志含义	检测到IRF分裂
参数解释	无
日志等级	1 (Alert)
举例	DEV/1/MAD_DETECT: Multi-active devices detected, please fix it.
对系统的影响	IRF分裂成两个IRF系统，只有其中一个IRF系统可以继续工作，另一个IRF系统无法工作
日志产生原因	IRF分裂导致一个IRF系统分裂成两个IRF系统，这两个IRF系统的配置发生冲突时，打印该日志
处理建议	1. 请使用 **display irf**查看当前IRF中有哪些成员设备，以便确定哪些成员设备分裂了 2. 请使用 **display irf link**查看IRF链路信息，确认故障的IRF链路 3. 手工修复状态为 DOWN 的 IRF 链路

16.43 MAD_PROC

日志内容	[STRING] protocol detected MAD conflict: Local health value=[UINT32], Peer health value=[UINT32].
日志含义	在IRF组网环境中，ARP、ND、LACP或BFD协议检测到IRF MAD冲突，显示本端和对端IRF的健康值
参数解释	$1：检测到MAD冲突的协议名称，取值为ARP、ND、LACP、BFD $2：本端IRF的健康值 $3：检测到MAD冲突时对端IRF的健康值
日志等级	6 (Informational)
举例	DEV/6/MAD_PROC: ARP protocol detected MAD conflict: Local health value=1, Peer health value=0.
对系统的影响	IRF分裂成两个IRF系统，只有其中一个IRF系统可以继续工作，另一个IRF系统无法工作
日志产生原因	在IRF组网环境中，ARP、ND、LACP或BFD协议检测到IRF MAD冲突时，打印该日志
处理建议	1. 请使用 **display irf**查看当前IRF中有哪些成员设备，以便确定哪些成员设备分裂了 2. 请使用 **display irf link**查看IRF链路信息，确认故障的IRF链路 3. 手工修复状态为 DOWN 的 IRF 链路

16.44 POWER_ABSENT

日志内容	形式一： Power [INT32] is absent. 形式二： Chassis [INT32] power [INT32] is absent.
日志含义	电源模块从设备中拔出
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	3 (Error)
举例	DEV/3/POWER_ABSENT: Power 1 is absent.
对系统的影响	可能影响系统供电
日志产生原因	电源模块从设备中拔出，或电源模块损坏
处理建议	**1.** 如果电源模块被拔出，无需处理 **2.** 如果电源模块没有被拔出，请检查设备电源模块连接情况，如电缆是否松动等，并确认电源模块是否损坏，如果损坏，请更换电源模块 **3.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.45 POWER_ALARM_CLEAR

日志内容	Power alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	电源重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/POWER_ALARM_CLEAR: Power alarm cleared. (PhysicalIndex=6, PhysicalName=power, RelativeResource=(powertype:type,chasiss:1,powertray:1,powerid:9), ErrorCode= 200031, Reason= A minimum of one PoE power supply is operating correctly.)
对系统的影响	对系统无影响
日志产生原因	电源重要故障恢复
处理建议	无需处理

表16-23 POWER_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
200031	A minimum of one PoE power supply is operating correctly.
200030	Mismatch of the rated power mode of the power graded power supply with the rated power required by the device was removed.
200028	No power input error was removed from the power board.
200027	The power board absence error was removed.
200026	The fault was removed from the power supply.
200025	Power supply model inconsistency issue removed.
200024	Fault removed from the dormant power supply.
200023	Communication between the power supply and system restored.
200022	Current fluctuation error removed.
200021	Input power is present on the power supply. Input power is present on power supply $1. $1：取值如下： • ""：单输入电源有输入 • input 0：双输入电源输入端口 0 • input 1：双输入电源输入端口 1
200020	Power supply was inserted.
200017	Fan in the power supply $1 resumed working.

故障码	故障原因描述
	$1：内部风扇故障恢复的电源编号 Fan in the power supply resumed working.
200016	Output overcurrent removed from power supply $1. CurrentValue = $2. $1：输出过流保护恢复电源编号 $2：实际输出电流 The power supply output power dropped below the output overcurrent shutdown threshold. CurrentValue = $1. $1：实际输出电流值，CurrentValue无法获取的填NA
200015	Output undervoltage removed from power supply $1. CurrentValue = $2. $1：输出欠压保护恢复电源编号 $2：实际输出电压值 The power supply output voltage increased above the output undervoltage shutdown threshold. CurrentValue = $1. $1：实际输出电压值，CurrentValue无法获取的填NA
200014	Output overvoltage removed from power supply $1. CurrentValue = $2. $1：输出过压恢复电源编号 $2：实际输出电压值 Output overvoltage exceed shutdown threshold alarm removed from power supply. CurrentValue = $1. $1：实际输出电压值，CurrentValue无法获取的填NA
200013	Input voltage on power $1 restored. $1：输入电压超范围恢复的电源编号 Input voltage for the power supply restored.
200012	$1 from insufficient power capacity. $1：恢复的相关描述 Insufficient power issue resolved.
200011	$1 from power redundancy failure. $1：恢复的相关描述 Insufficient redundant power issue resolved.
200010	The incompatible power supply $1 is removed. $1：不支持电源编号 The incompatible power supply was removed. The power supply $1 is compatible with the system now. $1：不支持电源编号 Power supply incompatibility issue removed.
200009	Incompatible power supply error removed.
200007	12V output voltage of the upper backplane restored to normal.
200006	12V output voltage of the lower backplane restored to normal.
200005	Backplane 3.3V output voltage restored to normal.
200004	Power tray $1 state changed to ok. $1：电源框编号

故障码	故障原因描述
	Power tray inserted.
200003	Unknown power supply $1 error removed. Reason: The power supply was removed. $1：未知电源编号 Unrecognized power supply was removed. Unknown power supply $1 error removed. $1：未知电源编号 Power supply unrecognition issue removed.
200018	Input undervoltage removed. CurrentValue = $1. $1：当前输入电压值，CurrentValue无法获取的填NA
200001	Input overvoltage removed. CurrentValue = $1V. $1：当前输入电压值，CurrentValue无法获取的填NA

16.46 POWER_ALARM_OCCUR

日志内容	Power alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	电源重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/POWER_ALARM_OCCUR: Power alarm occurred. (PhysicalIndex=6, PhysicalName=power, RelativeResource=(powertype:type,chasiss:1,powertray:1,powerid:9), ErrorCode= 200031, Reason=All PoE power supplies are fault or absent.)
对系统的影响	可能影响系统供电
日志产生原因	电源重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-24 POWER_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
200031	All PoE power supplies are fault or absent.
200030	Rated power mode of the power graded power supply did not match the rated power required by the device.
200028	No power input to the power board.
200027	No power board is present.

故障码	故障原因描述
200026	A fault occurred on the power supply.
200025	Inconsistent power supply models.
200024	Fault detected on the dormant power supply.
200023	Communication between the power supply and system failed.
200022	Current of the power supply fluctuated.
200021	No input power is present on the power supply. No input power is present on power supply $1. $1：取值如下： • ""：单输入电源无输入 • input 0：双输入电源输入端口 0 • input 1：双输入电源输入端口 1
200019	Power supply was removed.
200017	Fan in the power supply $1 stopped working. $1：内部风扇故障的电源编号 Fan in the power supply stopped working.
200016	Output overcurrent occurred on power supply $1. CurrentValue = $2. $1：输出过流保护电源编号 $2：实际输出电流 The power supply output power exceeded the output overcurrent shutdown threshold. CurrentValue = $1. $1：实际输出电流值，CurrentValue无法获取的填NA
200015	Output undervoltage occurred on power supply $1. CurrentValue = $2. $1：输出欠压保护电源编号 $2：实际输出电压值 The power supply output voltage dropped below the output undervoltage shutdown threshold. CurrentValue = $1. $1：实际输出电压值，CurrentValue无法获取的填NA
200014	Output overvoltage occurred on power supply $1. CurrentValue = $2. $1：输出过压电源编号 $2：实际输出电压值，CurrentValue无法获取的填NA The power supply output voltage exceeded the output overvoltage shutdown threshold. CurrentValue = $1. $1：实际输出电压值，CurrentValue无法获取的填NA
200013	Input voltage out of range on power $1. $1：输入电压超范围的电源编号 Input voltage for the power supply is out of range.
200012	No enough power to power on the board $1. Required power is $2 W, available power is $3 W. $1：单板描述 $2：需要的供电功率 $3：实际的供电功率

故障码	故障原因描述
	Power is insufficient. Required power: $1 W, Available power: $2 W. $1：需要的供电功率 $2：实际的供电功率
200011	Power redundancy $1 failed. Required redundant power is $2 W, redundant power is $3 W. $1：机框描述 $2：需要的冗余功率 $3：实际冗余功率 Redundant power is insufficient. Required redundant power: $1 W, Current redundant power: $2 W. $1：需要的冗余功率 $2：实际冗余功率
200010	The power supply $1 is not compatible with the system. $1：不支持电源编号 The power supply is not compatible with the system.
200009	Incompatible power supply detected.
200007	12V output voltage of the upper backplane became abnormal.
200006	12V output voltage of the lower backplane became abnormal.
200005	Backplane 3.3V output voltage became abnormal.
200004	Power tray $1 state changed to absent. $1：电源框编号 Power tray removed.
200003	Unknown power supply $1. $1：过温保护的电源编号 Power supply not recognized.
200018	Input undervoltage occurred . CurrentValue = $1. $1：当前输入电压值，CurrentValue无法获取的填NA
200001	Input overvoltage occurred. CurrentValue = $1V. $1：当前输入电压值，CurrentValue无法获取的填NA

16.47 POWER_FAILED

日志内容	形式一： Power [INT32] failed. 形式二： Chassis [INT32] power [INT32] failed.
日志含义	电源模块发生故障
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	2 (Critical)
举例	DEV/2/POWER_FAILED: Power 1 failed.
对系统的影响	如果是电源模块发生故障，可能影响设备供电
日志产生原因	在电源模块发生故障或刚插入电源模块时，打印该日志
处理建议	**1.** 如果是电源模块发生故障，请更换电源模块 **2.** 如果是刚插入电源模块，请确认电源模块是否正确安装

16.48 POWER_FATALALARM_CLEAR

日志内容	Power fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	电源紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/POWER_FATALALARM_CLEAR: Power fatal alarm cleared. (PhysicalIndex=6, PhysicalName=power, RelativeResource=(powertype:type,chasiss:1,powertray:1,powerid:9), ErrorCode=200002, Reason=Overtemperature removed from power supply 6.)
对系统的影响	对系统无影响
日志产生原因	电源紧急故障恢复
处理建议	无需处理

表16-25 POWER_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
200002	Overtemperature alarm for power supply $1 cleared. Reason: The power supply was removed. $1：过温保护的电源编号 Power supply that reached the overtemperature shutdown threshold was removed. Overtemperature removed from power supply $1. $1：过温保护的电源编号 Power supply fell below the overtemperature shutdown threshold. CurrentValue = $1 degrees centigrade. $1：当前电源温度值，CurrentValue无法获取的填NA

16.49 POWER_FATALALARM_OCCUR

日志内容	Power fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	电源紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/POWER_FATALALARM_OCCUR: Power fatal alarm occurred. (PhysicalIndex=6, PhysicalName=power, RelativeResource=(powertype:type,chasiss:1,powertray:1,powerid:9), ErrorCode= 200002, Reason=Overtemperature occurred on power supply 6.)
对系统的影响	可能影响系统供电
日志产生原因	电源紧急故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-26 POWER_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
200002	Overtemperature occurred on power supply $1. $1：过温保护的电源编号 Power supply reached the overtemperature shutdown threshold. CurrentValue = $1 degrees centigrade. $1：当前电源温度值，CurrentValue无法获取的填NA

16.50 POWER_MONITOR_ABSENT

日志内容	形式一： Power monitor unit [INT32] is absent. 形式二： Chassis [INT32] power monitor unit [INT32] is absent.
日志含义	电源监控模块从设备中拔出
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	3 (Error)
举例	DEV/3/POWER_MONITOR_ABSENT: Power monitor unit 1 is absent.
对系统的影响	可能影响系统供电
日志产生原因	电源监控模块从设备中拔出，或电源监控模块损坏
处理建议	**1.** 如果电源监控模块被拔出，无需处理 **2.** 如果电源监控模块没有被拔出，请检查电源监控模块连接情况，如电缆是否松动等，并确认电源监控模块是否损坏，如果损坏，请更换电源监控模块 **3.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.51 POWER_MONITOR_FAILED

日志内容	形式一： Power monitor unit [INT32] failed. 形式二： Chassis [INT32] power monitor unit [INT32] failed.
日志含义	电源监控模块出现故障
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	2 (Critical)
举例	DEV/2/POWER_MONITOR_FAILED: Power monitor unit 1 failed.
对系统的影响	可能影响系统供电
日志产生原因	电源监控模块出现故障
处理建议	**1.** 确认电源监控模块是否损坏，如果损坏，请更换电源监控模块 **2.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.52 POWER_MONITOR_RECOVERED

日志内容	形式一： Power monitor unit [INT32] recovered. 形式二： Chassis [INT32] power monitor unit [INT32] recovered.
日志含义	电源监控模块状态从Failed或者Absent状态转换为OK
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	2 (Critical)
举例	DEV/2/POWER_MONITOR_RECOVERED: Power monitor unit 1 recovered.
对系统的影响	对系统无影响
日志产生原因	电源监控模块插入后，状态从Failed或者Absent状态转换为OK
处理建议	无需处理

16.53 POWER_RECOVERED

日志内容	形式一： Power [INT32] recovered. 形式二： Chassis [INT32] power [INT32] recovered.
日志含义	电源模块状态从Failed或者Absent状态转换为OK
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	2 (Critical)
举例	DEV/2/POWER_RECOVERED: Power 1 recovered.
对系统的影响	对系统无影响
日志产生原因	电源模块插入后，状态从Failed或者Absent状态转换为OK
处理建议	无需处理

16.54 POWER_WARNING_CLEAR

日志内容	Power warning alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	电源告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/POWER_WARNING_CLEAR: Power warning alarm cleared. (PhysicalIndex=6, PhysicalName=power, RelativeResource=(powertype:type,chasiss:1,powertray:1,powerid:9), ErrorCode=200008, Reason=Both power switches turned on.)
对系统的影响	对系统无影响
日志产生原因	电源告警恢复
处理建议	无需处理

表16-27 POWER_WARNING_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
200032	The RPS power supply can provide sufficient power to meet the maximum PoE power requirements of the device.
200008	Both power switches turned on.

16.55 POWER_WARNING_OCCUR

日志内容	Power warning alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	电源告警产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/POWER_WARNING_OCCUR: Power warning alarm occurred. (PhysicalIndex=6, PhysicalName=power, RelativeResource=(powertype:type,chasiss:1,powertray:1,powerid:9), ErrorCode=200008, Reason=Only one power switch turned on.)
对系统的影响	可能影响系统供电
日志产生原因	电源告警产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-28 POWER_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
200032	The RPS power supply cannot provide sufficient power to meet the maximum PoE power requirements of the device.
200008	Only one power switch turned on.

16.56 RPS_ABSENT

日志内容	形式一： RPS [INT32] is absent. 形式二： Chassis [INT32] RPS [INT32] is absent.
日志含义	冗余电源模块从设备中拔出
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	3 (Error)
举例	DEV/3/RPS_ABSENT: RPS 1 is absent.
对系统的影响	可能影响系统供电
日志产生原因	冗余电源模块从设备中拔出，或冗余电源模块损坏
处理建议	**1.** 如果冗余电源模块被拔出，无需处理 **2.** 如果冗余电源模块没有被拔出，请检查设备冗余电源模块连接情况，如电缆是否松动等，并确认冗余电源模块是否损坏，如果损坏，请更换冗余电源模块 **3.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.57 RPS_FAILED

日志内容	形式一： RPS [INT32] failed. 形式二： Chassis [INT32] RPS [INT32] failed.
日志含义	冗余电源模块发生故障
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	2 (Critical)
举例	DEV/2/RPS_FAILED: RPS 2 failed.
对系统的影响	可能影响系统供电
日志产生原因	冗余电源模块未供电或发生故障时，打印该日志
处理建议	**1.** 如果冗余电源模块被拔出，无需处理 **2.** 如果冗余电源模块没有被拔出，请检查设备冗余电源模块连接情况，如电缆是否松动等，并确认冗余电源模块是否损坏，如果损坏，请更换冗余电源模块 **3.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.58 RPS_NORMAL

日志内容	形式一： RPS [INT32] is normal. 形式二： Chassis [INT32] RPS [INT32] is normal.
日志含义	冗余电源模块状态为正常
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	5 (Notification)
举例	DEV/5/RPS_NORMAL: RPS 1 is normal.
对系统的影响	对系统无影响
日志产生原因	冗余电源模块插入后，状态正常
处理建议	无需处理

16.59 SUBCARD_FAULT

日志内容	Subcard state changed to Fault on [STRING] subslot [INT32], type is [STRING].
日志含义	子卡状态转换为Fault
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	2 (Critical)
举例	DEV/2/SUBCARD_FAULT: Subcard state changed to Fault on slot 1 subslot 1, type is MIM-1ATM-OC3SML.
对系统的影响	如果是子卡故障，子卡不可用
日志产生原因	在子卡重启或发生故障时，打印该日志
处理建议	**1.** 如果后续子卡状态可以变为 Normal，则无需处理 **2.** 如果子卡一直处于 Falut 状态，则说明子卡故障，请更换子卡

16.60 SUBCARD_INSERTED

日志内容	Subcard was inserted in [STRING] subslot [INT32], type is [STRING].
日志含义	子卡安装到了指定槽位
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	4 (Warning)
举例	DEV/4/SUBCARD_INSERTED: Subcard was inserted in slot 1 subslot 1, type is MIM-1ATM-OC3SML.
对系统的影响	对系统无影响
日志产生原因	在子卡插入到设备时，打印该日志
处理建议	无需处理

16.61 SUBCARD_REBOOT

日志内容	Subcard is rebooting on [STRING] subslot [INT32].
日志含义	子卡正在重新启动
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号
日志等级	5 (Notification)
举例	DEV/5/SUBCARD_REBOOT: Subcard is rebooting on slot 1 subslot 1.
对系统的影响	子卡即将停止服务，重新启动
日志产生原因	用户在重启子卡，或者子卡因为运行异常自动重启
处理建议	**1.** 如果子卡重启后能正常运行，则无需处理 **2.** 如果您想进一步了解异常重启的原因或者子卡不断自动重启，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.62 SUBCARD_REMOVED

日志内容	Subcard was removed from [STRING] subslot [INT32], type is [STRING].
日志含义	子卡从设备中拔出
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	3 (Error)
举例	DEV/3/SUBCARD_REMOVED: Subcard was removed from slot 1 subslot 1, type is MIM-1ATM-OC3SML.
对系统的影响	子卡不可用
日志产生原因	子卡从设备中拔出时，打印该日志
处理建议	1. 如果子卡被拔出，无需处理 2. 如果子卡没有被拔出，检查子卡是否正确安装，重新安装子卡；检查子卡是否损坏，如果损坏，请更换子卡 3. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.63 SYSTEM_ALARM_CLEAR

日志内容	System alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	系统重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/SYSTEM_ALARM_CLEAR: System alarm cleared. (PhysicalIndex=3 PhysicalName=chasiss, RelativeResource=(devicetype:device,chasiss:0), ErrorCode=500009, Reason=Subcard removed.)
对系统的影响	对系统无影响
日志产生原因	系统重要故障恢复
处理建议	无需处理

表16-29 SYSTEM_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
500009	Subcard removed.

故障码	故障原因描述
423025	Fabric module capacity in chassis $1 restored. $1：Chassis ID，机框编号 Fabric module capacity restored. Sufficient fabric board quantity to support wire-speed forwarding.
400008	Incorrect port MAC addess error cleared from the board.
400007	Incorrect system MAC address error cleared.
400001	Inconsistent MPU type error removed.
100050	Fabric boards fully configured.
100040	MPUs fully configured.
100034	Connected or reconnected to each MPU on each chassis.
100030	The board insecure installation error was removed.
100026	The SFU was removed from the slot.
100023	The chassis was added.
100019	Peer chassis number conflict with another chassis removed.
100018	Peer chassis number conflict with port $1 removed. $1：本框另一端口
100017	Chassis number conflict removed.
100016	Connected or reconnected to chassis $1 slot $2. $1：另一CCU的所在的框框号 $2：另一CCU所在的槽位号 Connected or reconnected to the MCCU.
100013	The port was disconnected from the chassis that failed to be authenticated.
100011	The port was disconnected from the isolated chassis.
100010	Master misrecognition error removed from the port.

16.64 SYSTEM_ALARM_OCCUR

日志内容	System alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	系统重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	DEV/2/SYSTEM_ALARM_OCCUR: System alarm occurred. (PhysicalIndex=3 PhysicalName=chasiss, RelativeResource=(devicetype:device,chasiss:0), ErrorCode=500008, Reason=Subcard inserted.)
对系统的影响	系统业务可能会受到影响
日志产生原因	系统重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-30 SYSTEM_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
500008	Subcard inserted.
423025	Insufficient fabric module capacity in chassis $1. $1：Chassis ID，机框编号 Insufficient fabric module capacity. Insufficient fabric board quantity to support wire-speed forwarding.
400008	Incorrect port MAC address on the board.
400007	Incorrect system MAC address.
400001	Inconsistent MPU type.
100050	Fabric boards were not fully configured.
100040	MPUs not fully configured.
100034	Not connected to or disconnected from the MPU on chassis $1. $1：框号
100030	The board was installed insecurely.
100026	An SFU is installed. Please replace it with an MSFU.
100023	The chassis was removed.
100019	The port was connected to a chassis with the same number as another chassis.
100018	The port was connected to a chassis with the same number as the chassis to which port $1 was connected. $1：本框另一端口

故障码	故障原因描述
100017	The port was connected to a chassis with the same number as this chassis.
100016	Not connected to or disconnected from chassis $1 slot $2. $1：另一CCU的所在的框框号 $2：另一CCU所在的槽位号 Not connected to or disconnected from the MCCU on chassis $1. $1：另一CCU的所在的框框号
100013	The port was connected to a chassis that failed to be authenticated.
100011	The port was connected to chassis $1 which is isolated. $1：被隔离框框号
100010	The port recognized chassis $1 (slot $2) as the master, while the actual master is chassis $3 (slot $4). $1：邻框框号 $2：邻框主控槽位号 $3：端口所在框框号 $4：端口所在框主控槽位号 The port recognized chassis $1 slot $2 as the master, while the actual master is chassis $3 slot $4. $1：邻框框号 $2：邻框主控槽位号 $3：端口所在框框号 $4：端口所在框主控槽位号

16.65 SYSTEM_FATALALARM_CLEAR

日志内容	System fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	系统紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/SYSTEM_FATALALARM_CLEAR: System fatal alarm cleared. (PhysicalIndex=3 PhysicalName=chasiss, RelativeResource=(devicetype:device,chasiss:0), ErrorCode=100029, Reason=The board took the master role.)
对系统的影响	对系统无影响
日志产生原因	系统紧急故障恢复
处理建议	无需处理

表16-31 SYSTEM_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
100029	The board took the master role.
100027	The board recovered from reset.
100025	The chassis recovered from failure.
100024	Both MPUs on the chassis recovered from failure.

16.66 SYSTEM_FATALALARM_OCCUR

日志内容	System fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	系统紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	1 (Alert)
举例	DEV/1/SYSTEM_FATALALARM_OCCUR: System fatal alarm occurred. (PhysicalIndex=3 PhysicalName=chasiss, RelativeResource=(devicetype:device,chasiss:0), ErrorCode=100028, Reason=The board lost the master role.)
对系统的影响	系统业务可能会受到影响
日志产生原因	系统紧急故障产生，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-32 SYSTEM_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
100028	The board lost the master role.
100027	The board reset.
100025	The chassis failed.
100024	Both MPUs on the chassis failed.

16.67 SYSTEM_REBOOT

日志内容	System is rebooting now.
日志含义	系统正在重新启动
参数解释	无
日志等级	2 (Critical)
举例	DEV/2/SYSTEM_REBOOT: System is rebooting now.
对系统的影响	系统即将停止服务，重新启动
日志产生原因	用户在重启系统，或者系统因为异常而重启
处理建议	1. 检查是否有用户在重启系统。如果没有用户在重启系统，等待系统重新启动后，通过**display version**命令显示信息中的Last reboot reason字段，查看重启原因 2. 如果重启原因为异常重启，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.68 SYSTEM_WARNING_CLEAR

日志内容	System warning alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	系统告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/SYSTEM_WARNING_CLEAR: System warning alarm cleared. (PhysicalIndex=3 PhysicalName=chasiss, RelativeResource=(devicetype:device,chasiss:0), ErrorCode=100047, ReasonSubcard type consistent with the preconfigured type.)
对系统的影响	对系统无影响
日志产生原因	系统告警恢复
处理建议	无需处理

表16-33 SYSTEM_WARNING_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
482009	The original management interface port came up and assumed the active role.
100047	Subcard type consistent with the preconfigured type.
100033	Inconsistent SFC type error removed.

故障码	故障原因描述
100015	Peer chassis registration failure resolved.
100014	The chassis status changed from absent to present.
100012	Cluster mode conflict removed.
100006	Current subcard model consistent with the previous subcard model.
100005	Board type consistent with the preconfigured type.

16.69 SYSTEM_WARNING_OCCUR

日志内容	System warning alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	系统告警产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	DEV/4/SYSTEM_WARNING_OCCUR: System warning alarm occurred. (PhysicalIndex=3 PhysicalName=chasiss, RelativeResource=(devicetype:device,chasiss:0), ErrorCode=100047, Reason=Subcard type inconsistent with the preconfigured type.)
对系统的影响	系统业务可能会受到影响
日志产生原因	系统告警产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-34 SYSTEM_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
482009	The active management interface port went down, and the standby management interface port took over.
100047	Subcard type inconsistent with the preconfigured type.
100033	Inconsistent SFC type.
100015	The peer chassis failed in registration.
100014	The chassis is absent from the system.
100012	The port was connected to a chassis working in $1 mode, different from the cluster mode of this chassis. $1：集群模式，取值如下： • Back-to-back • Multi-chassis 2+2

故障码	故障原因描述
	• Multi-chassis 2+4 • Multi-chassis 3+6 • Single chassis
100006	Current subcard model inconsistent with the previous subcard model.
100005	Board type inconsistent with the preconfigured type.

16.70 TEMPERATURE_ALARM

日志内容	形式一： Temperature is greater than the high-temperature alarming threshold on sensor [STRING] [USHOT]. 形式二： Temperature is greater than the high-temperature alarming threshold on [STRING] sensor [STRING] [USHOT]. 形式三： Temperature is greater than the high-temperature alarming threshold on [STRING] [STRING] sensor [STRING] [USHOT].
日志含义	温度大于高温告警门限
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4 (Warning)
举例	DEV/4/TEMPERATURE_ALARM: Temperature is greater than the high-temperature alarming threshold on slot 1 sensor inflow 1.
对系统的影响	温度过高会影响系统正常工作
日志产生原因	温度超过严重级（Alarm）高温告警门限，或环境温度太高或者风扇异常，打印该日志
处理建议	1. 请检查机房现场环境温度是否过高，保持设备环境正常通风 2. 请使用 **display fan**命令检查风扇是否被拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 请使用 **display environment**命令查看当前温度以及生效的阈值。如果环境温度过高，改善环境温度 4. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.71 TEMPERATURE_ALARM_CLEAR

日志内容	Temperature alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	温度重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	2 (Critical)
举例	DEV/2/TEMPERATURE_ALARM_CLEAR: Temperature alarm cleared. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:Hotspot 3,slot:2,chipid:0,channel:0), ErrorCode=433004, Reason=Temperature readings from the sensor restored. ThresholdType=Shutdown, ThresholdValue=105 degrees centigrade, CurrentValue=115 degrees centigrade.)
对系统的影响	对系统无影响
日志产生原因	温度重要故障恢复
处理建议	无需处理

表16-35 TEMPERATURE_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
433004	$1 temperature out of range issue removed. $1：温度点描述 Temperature readings from the sensor restored.
433002	$1 temperature on the card in $2 restored. $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 Temperature increase above the low temperature threshold. $1 temperature on the card in $2 restored. $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 Temperature dropped below the high temperature warning threshold. $1 temperature on the card in $2 restored. $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 Temperature dropped below the high temperature alarming threshold.

16.72 TEMPERATURE_ALARM_OCCUR

日志内容	Temperature alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	温度重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	2 (Critical)
举例	DEV/2/TEMPERATURE_ALARM_OCCUR: Temperature alarm occurred. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:Hotspot 3,slot:2,chipid:0,channel:0,), ErrorCode=433004, Reason=Abnormal temperature readings from the sensor. ThresholdType=Shutdown, ThresholdValue=105 degrees centigrade, CurrentValue=115 degrees centigrade.)
对系统的影响	温度过高会影响系统正常工作
日志产生原因	温度重要故障产生，打印该日志，详情请参见故障原因描述
处理建议	1. 请检查机房现场环境温度是否过高，保持设备环境正常通风 2. 请使用**display fan**命令检查风扇是否被拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 请使用**display environment**命令查看当前温度以及生效的阈值。如果环境温度过高，改善环境温度 4. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-36 TEMPERATURE_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
433004	$1 temperature out of range. $1：温度点描述 Abnormal temperature readings from the sensor.
433002	$1 temperature on the card in $2 fell below the low temperature threshold ($3 centigrade). $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 $3：高温关断门限值，Threshold无法获取的填NA Temperature dropped below the low temperature threshold. $1 temperature on the card in $2exceeded the temperature warning threshold ($3 centigrade).

故障码	故障原因描述
	$1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 $3：高温关断门限值 Temperature exceeded the high-temperature warning threshold. $1 temperature on the card in $2 exceeded the temperature alarm threshold ($3 centigrade). $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 $3：高温关断门限值，Threshold无法获取的填NA Temperature exceeded the high temperature alarming threshold.

16.73 TEMPERATURE_FATALALARM_CLEAR

日志内容	Temperature fatal alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	温度紧急故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	1 (Alert)
举例	DEV/1/TEMPERATURE_FATALALARM_CLEAR: Temperature fatal alarm cleared. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:Hotspot 3,slot:2,chipid:0,channel:0), ErrorCode=433001, Reason=Temperature fell below the high temperature shutdown threshold. ThresholdType=Shutdown, ThresholdValue=105 degrees centigrade, CurrentValue=115 degrees centigrade.)
对系统的影响	对系统无影响
日志产生原因	温度紧急故障恢复
处理建议	无需处理

表16-37 TEMPERATURE_FATALALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
433001	$1 temperature on the card in $2 shutdown alarm restored. $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2

故障码	故障原因描述
	Temperature fell below the high temperature shutdown threshold.

16.74 TEMPERATURE_FATALALARM_OCCUR

日志内容	Temperature fatal alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	温度紧急故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	1 (Alert)
举例	DEV/1/TEMPERATURE_FATALALARM_OCCUR: Temperature fatal alarm occurred. (PhysicalIndex=9, PhysicalName=board, RelativeResource=(chiptype:Hotspot 3,slot:2,chipid:0,channel:0), ErrorCode=433001, Reason=Temperature reached the high temperature shutdown threshold. ThresholdType=Shutdown, ThresholdValue=105 degrees centigrade, CurrentValue=115 degrees centigrade。
对系统的影响	温度过高会影响系统正常工作
日志产生原因	温度紧急故障产生，打印该日志，详情请参见故障原因描述
处理建议	1. 请检查机房现场环境温度是否过高，保持设备环境正常通风 2. 请使用 **display fan**命令检查风扇是否被拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 请使用 **display environment**命令查看当前温度以及生效的阈值。如果环境温度过高，改善环境温度 4. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-38 TEMPERATURE_FATALALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
433001	$1 temperature on the card in $2 exceeded the temperature shutdown threshold ($3 centigrade) $1：温度点描述 $2：槽位号，如slot 1/2/3、slot 2/3或slot 2 $3：高温关断门限值，Threshold无法获取的填NA Temperature reached the high temperature shutdown threshold.

16.75 TEMPERATURE_LOW

日志内容	形式一： Temperature is less than the low-temperature threshold on sensor [STRING] [INT32]. 形式二： Temperature is less than the low-temperature threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is less than the low-temperature threshold on [STRING] [STRING] sensor [STRING] [INT32].
日志含义	温度低于低温告警门限
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4 (Warning)
举例	DEV/4/TEMPERATURE_LOW: Temperature is less than the low-temperature threshold on slot 1 sensor inflow 1.
对系统的影响	温度过温会影响系统正常工作
日志产生原因	温度低于低温告警门限时，打印该日志
处理建议	1. 请检查机房现场环境温度是否过低，如果环境温度过低，改善环境温度 2. 请使用**display fan**命令检查风扇是否被拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 请使用**display environment**命令查看当前温度以及生效的阈值。如果环境温度过高，改善环境温度 4. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.76 TEMPERATURE_NORMAL

日志内容	形式一： Temperature changed to normal on sensor [STRING] [INT32]. 形式二： Temperature changed to normal on [STRING] sensor [STRING] [INT32]. 形式三： Temperature changed to normal on [STRING] [STRING] sensor [STRING] [INT32].
日志含义	温度恢复正常（即大于低温告警门限，小于一般级高温告警门限）
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4 (Warning)
举例	DEV/4/TEMPERATURE_NORMAL: Temperature changed to normal on slot 1 sensor inflow 1.
对系统的影响	对系统无影响
日志产生原因	在实体的温度从异常状态中恢复正常时，打印该日志
处理建议	无需处理

16.77 TEMPERATURE_SHUTDOWN

日志内容	形式一： Temperature is greater than the high-temperature shutdown threshold on sensor [STRING] [INT32]. The slot will be powered off automatically. 形式二： Temperature is greater than the high-temperature shutdown threshold on [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically. 形式三： Temperature is greater than the high-temperature shutdown threshold on [STRING] [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically.
日志含义	温度超过关断级高温告警门限，单板将自动下电
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	2 (Critical)
举例	DEV/2/TEMPERATURE_SHUTDOWN: Temperature is greater than the high-temperature shutdown threshold on slot 1 sensor inflow 1. The slot will be powered off automatically.
对系统的影响	高温会影响系统正常工作
日志产生原因	温度超过关断级高温告警门限，或环境温度太高或者风扇异常，打印该日志
处理建议	1. 请检查机房现场环境温度是否过高，保持设备环境正常通风 2. 请使用**display fan**命令检查风扇是否被拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 请使用**display environment**命令查看当前温度以及生效的阈值。如果环境温度过高，改善环境温度 4. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.78 TEMPERATURE_WARNING

日志内容	形式一： Temperature is greater than the high-temperature warning threshold on sensor [STRING] [INT32]. 形式二： Temperature is greater than the high-temperature warning threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is greater than the high-temperature warning threshold on [STRING] [STRING] sensor [STRING] [INT32].
日志含义	温度超过一般级高温告警门限
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4 (Warning)
举例	DEV/4/TEMPERATURE_WARNING: Temperature is greater than the high-temperature warning threshold on slot 1 sensor inflow 1.
对系统的影响	高温会影响系统正常工作
日志产生原因	温度超过一般级高温告警门限，或环境温度太高或者风扇异常，打印该日志
处理建议	1. 请检查机房现场环境温度是否过高，保持设备环境正常通风 2. 请使用**display fan**命令检查风扇是否被拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 请使用**display environment**命令查看当前温度以及生效的阈值。如果环境温度过高，改善环境温度 4. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.79 TIMER_CREATE_FAILED_FIRST

日志内容	The process with PID [UINT] failed to create a timer.Reason for the failure:[STRING]
日志含义	进程创建定时器失败
参数解释	$1：创建定时器的进程的PID $2：最近一次创建定时器失败的原因，取值为： • Maximum number of timers already reached：设备允许创建的定时器个数达到最大值
日志等级	4 (Warning)
举例	DEV/4/TIMER_CREATE_FAILED_FIRST: The process with PID 70 failed to creadte a timer.Reason for the failure: Maximum number of timers already reached.
对系统的影响	可能会影响进程对应的业务模块功能
日志产生原因	进程第一次创建定时器失败以及失败的原因。为避免异常情况下，频繁打印该日志，系统对该日志采取抑制输出机制： • 进程第一次创建定时器失败时，立即打印 TIMER_CREATE_FAILED_FIRST 日志 • 超过 15 分钟后，如果该进程创建定时器再次失败，则输出日志 TIMER_CREATE_FAILED_MORE，TIMER_CREATE_FAILED_MORE 中会包含上次输出定时器创建失败日志的时间，以及上次输出定时器创建失败日志到本次输出定时器创建失败日志期间创建定时器失败的次数。15 分钟内创建失败的日志会被抑制，不会输出
处理建议	**1.** 如果进程对应的业务模块的功能受到影响，可重启设备尝试修复 **2.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.80 TIMER_CREATE_FAILED_MORE

日志内容	The process with PID [UINT] failed to create a timer:[UINT] consecutive failures since [STRING].Reason for the failure:[STRING]
日志含义	进程再次创建定时器失败
参数解释	$1：创建定时器的进程的PID $2：距离上次打印日志到当前时间内创建定时器失败的次数 $3：上次打印日志的时间 $4：最近一次创建定时器失败的原因，取值为： • Maximum number of timers already reached：设备允许创建的定时器个数达到最大值
日志等级	4 (Warning)
举例	DEV/4/TIMER_CREATE_FAILED_MORE: The process with PID 70 failed to create a timer:2 consecutive failures since 2019/11/21 16:00:00.Reason for the failure: Maximum number of timers already reached.
对系统的影响	可能会影响进程对应的业务模块功能
日志产生原因	进程第一次创建定时器失败以及失败的原因。为避免异常情况下，频繁打印该日志，系统对该日志采取抑制输出机制： • 进程第一次创建定时器失败时，立即打印 TIMER_CREATE_FAILED_FIRST 日志 • 超过 15 分钟后，如果该进程创建定时器再次失败，则输出日志 TIMER_CREATE_FAILED_MORE，TIMER_CREATE_FAILED_MORE 中会包含上次输出定时器创建失败日志的时间，以及上次输出定时器创建失败日志到本次输出定时器创建失败日志期间创建定时器失败的次数。15 分钟内创建失败的日志会被抑制，不会输出
处理建议	1. 如果进程对应的业务模块的功能受到影响，可重启设备尝试修复 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.81 VCHK_VERSION_INCOMPATIBLE

日志内容	Software version of [STRING] is incompatible with MPU.
日志含义	单板与主控板软件版本不兼容
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	1 (Alert)
举例	DEV/1/VCHK_VERSION_INCOMPATIBLE: Software version of slot 1 is incompatible with MPU.
对系统的影响	单板不可用
日志产生原因	PEX在启动过程中，检测到自己的启动软件包和父设备上运行的软件包版本不兼容，PEX会打印该信息并重启
处理建议	1. 请设置与父设备当前版本兼容的软件包作为该 PEX 的下次启动软件包/加载软件包 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

16.82 VOLTAGE_ALARM_CLEAR

日志内容	Voltage alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	电压重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	2 (Critical)
举例	DEV/2/VOLTAGE_ALARM_CLEAR: Voltage alarm cleared. (PhysicalIndex=1, PhysicalName=secondary power, RelativeResource=(voltagetype:3.3V,chasiss:1,slot:2,unitid:3), ErrorCode=421001, Reason=PoE turned on, ThresholdType=Shutdown, ThresholdValue=3.63V, CurrentValue=3.72V.)
对系统的影响	对系统无影响
日志产生原因	电压重要故障恢复
处理建议	无需处理

表16-39 VOLTAGE_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
421001	PoE turned on.
420005	Voltage on voltage chip channel $1 ($2) on the card $3 fell below the high output voltage shutdown threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage fell below the high output voltage shutdown threshold.
420003	Voltage on voltage chip channel $1 ($2) on the card $3 increased above the low output voltage shutdown threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage increased above the low output voltage shutdown threshold.

16.83 VOLTAGE_ALARM_OCCUR

日志内容	Voltage alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	电压重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	2 (Critical)
举例	DEV/2/VOLTAGE_ALARM_OCCUR: Voltage alarm occurred. (PhysicalIndex=1, PhysicalName=secondary power, RelativeResource=(voltagetype:3.3V,chasiss:1,slot:2,unitid:3), ErrorCode=421001, Reason=PoE turned off, ThresholdType=Shutdown, ThresholdValue=3.63V, CurrentValue=3.72V.)
对系统的影响	电压异常可能会影响系统正常工作
日志产生原因	电压重要故障产生，打印该日志，详情请参见故障原因描述
处理建议	1. 请使用 **display voltage**命令查看设备电源是否符合设备供电要求，如果不符合要求，需要更换电源 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-40 VOLTAGE_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
421001	PoE turned off.
420005	Voltage on voltage chip channel $1 ($2) on the card $3 exceeded the high output voltage shutdown threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage exceeded the high output voltage shutdown threshold.
420003	Voltage on voltage chip channel $1 ($2) on the card $3 lower than the low output voltage shutdown threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage lower than the low output voltage shutdown threshold.

16.84 VOLTAGE_WARNING_CLEAR

日志内容	Voltage warning alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	电压告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	4 (Warning)
举例	DEV/4/VOLTAGE_WARNING_CLEAR: Voltage warning alarm cleared. (PhysicalIndex=1, PhysicalName=secondary power, RelativeResource=(voltagetype:3.3V,chasiss:1,slot:2,unitid:3), ErrorCode=420004, Reason=Voltage fell below the high output voltage warning threshold. ThresholdType=Shutdown, ThresholdValue=3.63V, CurrentValue=3.72V.)
对系统的影响	对系统无影响
日志产生原因	电压告警恢复
处理建议	无需处理

表16-41 VOLTAGE_WARNING_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
420004	Voltage on voltage chip channel $1 ($2) on the card $3 fell below the high output voltage warning threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage fell below the high output voltage warning threshold.
420002	Voltage on voltage chip channel $1 ($2) on the card $3 increased above the low output voltage warning threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage increased above the low output voltage warning threshold.

16.85 VOLTAGE_WARNING_OCCUR

日志内容	Voltage warning alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING], ThresholdType=[STRING], ThresholdValue=[STRING], CurrentValue=[STRING])
日志含义	电压告警产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表 $6：门限类型 $7：门限值 $8：当前值
日志等级	4 (Warning)
举例	DEV/4/VOLTAGE_WARNING_OCCUR: Voltage warning alarm occurred. (PhysicalIndex=1, PhysicalName=secondary power, RelativeResource=(voltagetype:3.3V,chasiss:1,slot:2,unitid:3), ErrorCode=420004, Reason=Voltage exceeded the high output voltage warning threshold. ThresholdType=Shutdown, ThresholdValue=3.63V, CurrentValue=3.72V.)
对系统的影响	电压异常可能会影响系统正常工作
日志产生原因	电压告警产生，打印该日志，详情请参见故障原因描述
处理建议	1. 请使用 **display voltage**命令查看设备电源是否符合设备供电要求，如果不符合要求，需要更换电源 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表16-42 VOLTAGE_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
420004	Voltage on voltage chip channel $1 ($2) on the card $3 exceeded the high output voltage warning threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage exceeded the high output voltage warning threshold.
420002	Voltage on voltage chip channel $1 ($2) on the card $3 lower than the low output voltage warning threshold. $1：电压通道编号 $2：电压通道描述 $3：槽位号 Voltage lower than the low output voltage warning threshold.

17 DHCP

本节介绍 DHCP（Dynamic Host Configuration Protocol）模块输出的日志信息。

17.1 DHCP_NORESOURCES

日志内容	Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
日志含义	设备硬件资源不足，导致DHCP报文过滤规则下发失败
参数解释	无
日志等级	3 (Error)
举例	DHCP/3/DHCP_NORESOURCES: Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
对系统的影响	系统无法处理DHCP报文
日志产生原因	配置DHCP功能需要针对DHCP报文下发报文过滤规则。由于设备硬件资源不足，导致设置DHCP报文过滤规则失败
处理建议	请根据需要关闭非必要业务，释放部分硬件资源，并重新配置DHCP功能

17.2 DHCP_NOTSUPPORTED

日志内容	Failed to apply filtering rules for DHCP packets because some rules are not supported.
日志含义	下发的某些DHCP报文过滤规则设备不支持，导致DHCP报文过滤规则下发失败
参数解释	无
日志等级	3 (Error)
举例	DHCP/3/DHCP_NOTSUPPORTED: Failed to apply filtering rules for DHCP packets because some rules are not supported.
对系统的影响	系统无法处理DHCP报文
日志产生原因	配置DHCP功能需要针对DHCP报文下发DHCP报文过滤规则。由于设备不支持某些报文过滤规则，导致设置DHCP报文过滤规则失败
处理建议	请确认设备是否支持DHCP功能： • 如果设备不支持 DHCP 功能，则属于正常运行信息，无需处理 • 如果设备支持 DHCP 功能，则请重新使能 DHCP。若问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

18 DHCPR

本节介绍 DHCPR（IPv4 DHCP Relay）模块输出的日志信息。

18.1 DHCPR_SERVERCHANGE

日志内容	Switched to the DHCP server at [IPADDR] (VPN name: [STRING]) because the current DHCP server did not respond. Switched to the DHCP server at [IPADDR] because the current DHCP server did not respond.
日志含义	当前DHCP服务器未响应，DHCP中继切换到新的DHCP服务器申请地址
参数解释	$1：切换到下一个DHCP服务器的IP地址 $2：切换到下一个DHCP服务器的VPN信息 $3：切换到下一个DHCP服务器的IP地址，该服务器处于公网中
日志等级	3 (Error)
举例	• DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1; Switched to the server at *2.2.2.2* (VPN name: 1) because the current server did not respond. • DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1; Switched to the DHCP server at 2.2.2.2 because the current DHCP server did not respond.
对系统的影响	DHCP中继从新的DHCP服务器上申请地址
日志产生原因	DHCP中继无法从当前的DHCP服务器得到应答，切换到下一台DHCP服务器申请IP地址
处理建议	无需处理

18.2 DHCPR_SWITCHMASTER

日志内容	Switched to the master DHCP server at [IPADDR].
日志含义	远端服务器切换到主用DHCP服务器
参数解释	$1：主用DHCP服务器的IP地址
日志等级	3 (Error)
举例	DHCPR/3/DHCPR_SWITCHMASTER: -MDC=1; Switched to the master DHCP server at 2.2.2.2.
对系统的影响	系统将采用主用DHCP服务器上的地址网段给DHCP客户端分配地址
日志产生原因	DHCP中继配置延迟回切时间后，如果当前生效的为备用服务器，延迟时间到达后，DHCP中继会切换到主用DHCP服务器来执行申请IP地址的操作
处理建议	无需处理

19 DHCPS

本节介绍 DHCPS（DHCP server）模块输出的日志信息。

19.1 DHCPS_ALLOCATE_IP

日志内容	DHCP server received a DHCP client's request packet on interface [STRING], and allocated an IP address [IPADDR](lease [UINT32] seconds) for the DHCP client(MAC [MAC]) from [STRING] pool.
日志含义	DHCP服务器收到DHCP客户端的请求报文，并为其分配一个IPv4地址租约
参数解释	$1：DHCP服务器所在接口的接口名 $2：分配给DHCP客户端的IPv4地址 $3：分配给DHCP客户端的IPv4地址租约时长 $4：DHCP客户端的MAC地址 $5：DHCP服务器地址池名
日志等级	5 (Notification)
举例	DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server received a DHCP client's request packet on interface GigabitEthernet1/0/2, and allocated an IP address 1.0.0.91(lease 86400 seconds) for the DHCP client(MAC 0000-0000-905a) from p1 pool.
对系统的影响	对系统无影响
日志产生原因	DHCP服务器为DHCP客户端分配一个IPv4地址租约
处理建议	无需处理

19.2 DHCPS_CONFLICT_IP

日志内容	A conflict IP [IPADDR] from [STRING] pool was detected by DHCP server on interface [STRING].
日志含义	DHCP服务器的接口地址被置为冲突地址，从地址池可分配地址中删除
参数解释	$1：冲突的IPv4地址 $2：DHCP服务器地址池名 $3：DHCP服务器所在接口的接口名
日志等级	5 (Notification)
举例	DHCPS/5/DHCPS_CONFLICT_IP: A conflict IP 100.1.1.1 from p1 pool was detected by DHCP server on interface GigabitEthernet1/0/2.
对系统的影响	该冲突IP地址不可分配
日志产生原因	地址池下的地址网段内包含了DHCP服务器的接口IP地址
处理建议	无需处理

19.3 DHCPS_EXTEND_IP

日志内容	DHCP server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IP [IPADDR], MAC [MAC]).
日志含义	DHCP服务器收到DHCP客户端的DHCP请求报文，并为DHCP客户端续约
参数解释	$1：DHCP服务器所在接口的接口名 $2：DHCP服务器地址池名 $3：分配给DHCP客户端的IPv4地址 $4：DHCP客户端的MAC地址
日志等级	5 (Notification)
举例	DHCPS/5/DHCPS_EXTEND_IP: DHCP server received a DHCP client's request packet on interface GigabitEthernet1/0/2, and extended lease from p1 pool for the DHCP client (IP 1.0.0.91, MAC 0000-0000-905a).
对系统的影响	对系统无影响
日志产生原因	DHCP服务器为DHCP客户端续约
处理建议	无需处理

19.4 DHCPS_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
日志含义	因为存储空间不足导致DHCP服务器保存客户端信息到文件失败
参数解释	无
日志等级	4 (Warning)
举例	DHCPS/4/DHCPS_FILE: Failed to save DHCP client information due to lack of storage resources.
对系统的影响	DHCP客户端信息保存失败，客户端无法上线
日志产生原因	存储空间不足时，新用户上线
处理建议	请删除其它非必要文件，释放部分空间。若问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

19.5 DHCPS_RECLAIM_IP

日志内容	DHCP server reclaimed a [STRING] pool's lease(IP [IPADDR], lease [UINT32] seconds), which is allocated for the DHCP client (MAC [MAC]).
日志含义	DHCP服务器回收一个分配给DHCP客户端的地址租约
参数解释	$1：DHCP服务器地址池名 $2：分配给DHCP客户端的IPv4地址 $3：分配给DHCP客户端的IPv4地址租约时长 $4：DHCP客户端的MAC地址
日志等级	5 (Notification)
举例	DHCPS/5/DHCPS_RECLAIM_IP: DHCP server reclaimed a p1 pool's lease(IP 1.0.0.91, lease 86400 seconds), which is allocated for the DHCP client (MAC 0000-0000-905a).
对系统的影响	对系统无影响
日志产生原因	• 通过命令配置删除租约 • 客户端主动发送了 DHCP Release 报文 • 客户端没续约导致租约老化
处理建议	无需处理

19.6 DHCPS_VERIFY_CLASS

日志内容	Illegal DHCP client-PacketType=[STRING]-ClientAddress=[MAC];
日志含义	DHCP客户端请求方向报文非法
参数解释	$1：报文类型 $2：DHCP客户端的硬件地址
日志等级	5 (Notification)
举例	DHCPS/5/DHCPS_VERIFY_CLASS: Illegal DHCP client-PacketType= DHCPDISCOVER-ClientAddress=0000-5e01-0104;
对系统的影响	DHCP服务器不会处理该客户端的请求报文
日志产生原因	DHCP服务器对客户端报文白名单验证不通过
处理建议	请通过端口镜像等方法确认该请求报文来源是否合法： • 若报文来自非法用户，则忽略此请求报文 • 若报文来自合法用户，则可以将该客户端所属用户类加入用户类白名单。若问题仍未解决，则请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

20 DHCPS6

本节介绍 DHCPS6（DHCPv6 server）模块输出的 日志信息。

20.1 DHCPS6_ALLOCATE_ADDRESS

日志内容	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 address [IPADDR] (lease [UINT32] seconds) for the DHCPv6 client(DUID [HEX], IAID [HEX]) from [STRING] pool.
日志含义	DHCPv6服务器收到DHCPv6客户端的请求报文，并为其分配了一个IPv6地址租约
参数解释	$1：DHCPv6服务器所在接口的接口名 $2：分配给DHCPv6客户端的ipv6地址 $3：分配给DHCPv6客户端的ipv6地址租约时长 $4：DHCPv6客户端的DUID $5：DHCPv6客户端的IAID $6：DHCPv6服务器地址池名
日志等级	5 (Notification)
举例	DHCPS6/5/ALLOCATE ADDRESS: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 address 2000::3(lease 60 seconds) for the DHCPv6 client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
对系统的影响	对系统无影响
日志产生原因	DHCPv6服务器为DHCPv6客户端分配一个IPv6地址租约
处理建议	无需处理

20.2 DHCPS6_ALLOCATE_PREFIX

日志内容	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 prefix [IPADDR] (lease [UINT32] seconds) for the DHCPv6 client(DUID [HEX], IAID [HEX]) from [STRING] pool.
日志含义	DHCPv6服务器收到DHCPv6客户端的请求报文，并为其分配了一个IPv6前缀地址租约
参数解释	$1：DHCPv6服务器所在接口的接口名 $2：分配给DHCPv6客户端的IPv6前缀地址 $3：分配给DHCPv6客户端的IPv6前缀地址租约时长 $4：DHCPv6客户端的DUID $5：DHCPv6客户端的IAID $6：DHCPv6服务器地址池名
日志等级	5 (Notification)
举例	DHCPS6/5/ALLOCATE PREFIX: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 prefix 2000::(lease 60 seconds) for the DHCPv6 client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
对系统的影响	对系统无影响
日志产生原因	DHCPv6服务器为DHCPv6客户端分配一个IPv6前缀地址租约
处理建议	无需处理

20.3 DHCPS6_CONFLICT_ADDRESS

日志内容	A conflict IPv6 address [IPADDR] from [STRING] pool was detected by DHCPv6 server on interface [STRING].
日志含义	DHCPv6服务器的接口IPv6地址被置为冲突地址，从地址池可分配地址中删除
参数解释	$1：冲突的IPv6地址 $2：DHCPv6服务器地址池名 $3：DHCPv6服务器所在接口的接口名
日志等级	5 (Notification)
举例	DHCPS6/5/DHCPS6_CONFLICT_ADDRESS: A conflict IPv6 address 33::1 from p1 pool was detected by DHCPv6 server on interface Ethernet0/2.
对系统的影响	该冲突IPv6地址不可分配
日志产生原因	地址池下的地址网段内包含了DHCPv6服务器的接口IPv6地址
处理建议	无需处理

20.4 DHCPS6_EXTEND_ADDRESS

日志内容	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 address [IPADDR], DUID [HEX], IAID [HEX]).
日志含义	DHCPv6服务器收到DHCPv6客户端的DHCPv6请求报文，并为DHCPv6客户端续约地址
参数解释	$1：DHCPv6服务器所在接口的接口名 $2：DHCPv6服务器地址池名 $3：分配给DHCPv6客户端的IPv6地址 $4：DHCPv6客户端的DUID $5：DHCPv6客户端的IAID
日志等级	5 (Notification)
举例	DHCPS6/5/EXTEND ADDRESS: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 address 2000::3, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
对系统的影响	对系统无影响
日志产生原因	DHCPv6服务器为DHCPv6客户端地址续约
处理建议	无需处理

20.5 DHCPS6_EXTEND_PREFIX

日志内容	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 prefix [IPADDR], DUID [HEX], IAID [HEX]).
日志含义	DHCPv6服务器收到DHCPv6客户端的DHCPv6请求报文，并为DHCPv6客户端续约前缀
参数解释	$1：DHCPv6服务器所在接口的接口名 $2：DHCPv6服务器地址池名 $3：分配给DHCPv6客户端的IPv6前缀地址 $4：DHCPv6客户端的DUID $5：DHCPv6客户端的IAID
日志等级	5 (Notification)
举例	DHCPS6/5/EXTEND PREFIX: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 prefix 2000::, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
对系统的影响	对系统无影响
日志产生原因	DHCPv6服务器为DHCPv6客户端前缀地址续约
处理建议	无需处理

20.6 DHCPS6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
日志含义	因为存储空间不足导致DHCPv6服务器保存客户端信息到文件失败
参数解释	无
日志等级	4 (Warning)
举例	DHCPS6/4/DHCPS6_FILE: Failed to save DHCP client information due to lack of storage resources.
对系统的影响	DHCPv6客户端信息保存失败，客户端无法上线
日志产生原因	存储空间不足时，新用户上线
处理建议	请删除其它非必要文件，释放部分空间。若问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

20.7 DHCPS6_RECLAIM_ADDRESS

日志内容	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 address [IPADDR], lease [UINT32] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
日志含义	DHCPv6服务器回收一个分配给IPv6客户端的地址租约
参数解释	$1：DHCPv6服务器地址池名 $2：分配给DHCPv6客户端的IPv6地址 $3：分配给DHCPv6客户端的IPv6地址租约时长 $4：DHCPv6客户端的DUID $5：DHCPv6客户端的IAID
日志等级	5 (Notification)
举例	DHCPS6/5/RECLAIM ADDRESS: DHCPv6 server reclaimed a p1 pool's lease(IPv6 address 2000::3, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
对系统的影响	对系统无影响
日志产生原因	• 通过 reset 命令删除租约 • 客户端主动发送了 DHCP Release 报文 • 客户端没续约导致租约老化
处理建议	如果DHCPv6客户端仍需上线，请重新申请地址租约

20.8 DHCPS6_RECLAIM_PREFIX

日志内容	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 prefix [IPADDR], lease [INTEGER] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
日志含义	DHCPv6服务器回收一个分配给DHCPv6客户端的前缀地址租约
参数解释	$1：DHCPv6服务器所在接口的接口名 $2：分配给DHCPv6客户端的IPv6前缀地址 $3：分配给DHCPv6客户端的IPv6前缀地址租约时长 $4：DHCPv6客户端的DUID $5：DHCPv6客户端的IAID
日志等级	5 (Notification)
举例	DHCPS6/5/RECLAIM PREFIX: DHCPv6 server reclaimed a p1 pool's lease(IPv6 prefix 2000::, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
对系统的影响	对系统无影响
日志产生原因	• 通过 reset 命令删除租约 • 客户端主动发送了 DHCP Release 报文 • 客户端没续约导致租约老化
处理建议	如果DHCPv6客户端仍需上线，请重新申请前缀地址租约

21 DHCPSP4

本节介绍 DHCPSP（DHCP Snooping）模块输出的日志信息。

21.1 DHCPSP4_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
日志含义	因为存储空间不足导致DHCP Snooping保存客户端信息到文件失败
参数解释	无
日志等级	4 (Warning)
举例	DHCPSP4/4/DHCPSP4_FILE: Failed to save DHCP client information due to lack of storage resources.
对系统的影响	DHCP客户端信息保存失败，客户端无法上线
日志产生原因	存储空间不足时，存在DHCP Snooping新用户上线
处理建议	请删除其它非必要文件，释放部分空间。若问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

21.2 DHCPSP4_UNTRUSTED_SERVER

日志内容	Detected reply packet from untrusted server. Server info: IPaddress = [IPADDR], MACaddress = [MAC], Interface = [STRING].
日志含义	DHCP Snooping检测到来自非信任DHCP服务器的应答报文
参数解释	$1：非信任DHCP服务器的IP地址 $2：非信任DHCP服务器的MAC地址 $3：连接非信任DHCP服务器的接口名称
日志等级	4 (Warning)
举例	DHCPSP4/4/DHCPSP4_UNTRUSTED_SERVER: Detected reply packet from untrusted server. Server Info: IPaddress = 192.168.1.1, MACaddress = 78a0-7aa4-0307, Interface = GigabitEthernet1/0/1.
对系统的影响	系统接收不到来自非信任DHCP服务器的应答报文
日志产生原因	端口开启DHCP Snooping功能后，检测到来自非信任DHCP服务器的应答报文并丢弃时，系统输出本日志
处理建议	根据日志信息的IP地址和MAC地址等信息定位和处理非信任DHCP服务器

22 DHCPSP6

本节介绍 DHCPSP6（DHCPv6 Snooping）模块输出的 日志信息。

22.1 DHCPSP6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
日志含义	因为存储空间不足导致DHCPv6 Snooping保存客户端信息到文件失败
参数解释	无
日志等级	4 (Warning)
举例	DHCPSP6/4/DHCPSP6_FILE: Failed to save DHCP client information due to lack of storage resources.
对系统的影响	DHCPv6客户端信息保存失败，客户端无法上线
日志产生原因	存储空间不足时，存在DHCPv6 Snooping新用户上线
处理建议	请删除其它非必要文件，释放部分空间。若问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

23 DIAG

本节介绍 Diagnostic 模块输出的日志信息。

23.1 CPU_MINOR_RECOVERY

日志内容	CPU usage minor alarm removed.
日志含义	CPU利用率恢复到正常状态
参数解释	无
日志等级	5 (Notification)
举例	DIAG/5/CPU_MINOR_RECOVERY: CPU usage minor alarm removed.
对系统的影响	对系统无影响
日志产生原因	当设备处于CPU利用率低级别告警状态，并且采样值小于或等于恢复门限时，系统解除CPU低级别告警状态，CPU利用率恢复到正常状态，并打印该日志
处理建议	无需处理

23.2 CPU_MINOR_THRESHOLD

日志内容	CPU usage is in minor alarm state. CPU usage: [UINT]% in last 1 minute. CPU usage thresholds: Minor: [UINT]% Severe: [UINT]% Recovery: [UINT]% Process info: JID PID PRI State FDs HH:MM:SS CPU Name [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR] Core states: ID Idle User Kernel Interrupt Busy CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]
日志含义	CPU利用率低级别告警，显示当前CPU利用率信息

参数解释	• 整个系统中 CPU 利用率的统计信息：
	  ○ $1：过去 1 分钟内统计的 CPU 利用率
	  ○ $2：低级别告警门限
	  ○ $3：高级别告警门限
	  ○ $4：告警恢复门限
	• 整个系统中 CPU 利用率最高的前 5 个进程的信息：
	  ○ $5：进程 JID
	  ○ $6：进程 PID
	  ○ $7：进程的优先级
	  ○ $8：进程的状态
	  ○ $9：进程文件句柄
	  ○ $10：进程启动时长
	  ○ $11：进程的 CPU 占用率
	  ○ $12：进程名
	• 整个系统中 CPU 利用率最高的前 5 个核的信息：
	  ○ $13：核 ID
	  ○ $14：空闲时间
	  ○ $15：用户态进程占用的时间
	  ○ $16：内核线程占用的时间
	  ○ $17：中断占用的时间
	  ○ $18：运行时间

日志等级	4 (Warning)
举例	DIAG/4/CPU_MINOR_THRESHOLD: CPU usage is in minor alarm state. CPU usage: 3% in last 1 minute. CPU usage thresholds: Minor: 1% Severe: 2% Recovery: 0%

	Process info: JID PID PRI State FDs HH:MM:SS CPU Name 108398 108398 120 S 36 00:00:0 12.58% snmpd 52 52 102 S 0 00:01:2 2.58% [DRV_FWD] 371 371 120 S 95 00:18:5 0.17% pppd 90 90 120 R 18 00:12:0 0.34% diagd 109 109 119 S 41 00:11:1 0.00% vbrd Core states: ID Idle User Kernel Interrupt Busy CPU0 98.61% 0.24% 0.62% 0.53% 1.39% CPU1 99.88% 0.00% 0.03% 0.09% 0.12%
对系统的影响	设备运行速度会变慢，CPU处理业务能力会下降，可用CPU资源不足
日志产生原因	当CPU利用率的采样值从小于/等于变成大于低级别告警门限时，设备进入CPU利用率低级别告警状态，并定期打印该日志，直到CPU低级别告警状态解除
处理建议	**1.** 查看日志打印信息，分析占用 CPU 较高的进程是否合理 **2.** 根据分析结果，关闭暂不使用的进程 **3.** 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

23.3 CPU_SEVERE_RECOVERY

日志内容	CPU usage severe alarm removed.
日志含义	CPU利用率高级别告警解除
参数解释	无
日志等级	5 (Notification)
举例	DIAG/5/CPU_SEVERE_RECOVERY: CPU usage severe alarm removed.
对系统的影响	对系统无影响
日志产生原因	当设备处于CPU高级别告警状态，并且CPU利用率采样值小于或等于低级别告警门限时，系统解除CPU高级别告警状态，并打印该日志
处理建议	无需处理

23.4 CPU_SEVERE_THRESHOLD

日志内容	CPU usage is in severe alarm state. CPU usage: [UINT]% in last 1 minute. CPU usage thresholds: Minor: [UINT]% Severe: [UINT]% Recovery: [UINT]% Process info: JID PID PRI State FDs HH:MM:SS CPU Name [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR] Core states: ID Idle User Kernel Interrupt Busy CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]
日志含义	CPU利用率高级别告警，显示当前CPU利用率信息

参数解释	• 整个系统中 CPU 利用率的统计信息：
	  ○ $1：过去 1 分钟内统计的 CPU 利用率
	  ○ $2：低级别告警门限
	  ○ $3：高级别告警门限
	  ○ $4：告警恢复门限
	• 整个系统中 CPU 利用率最高的前 5 个进程的信息：
	  ○ $5：进程 JID
	  ○ $6：进程 PID
	  ○ $7：进程的优先级
	  ○ $8：进程的状态
	  ○ $9：进程文件句柄
	  ○ $10：进程启动时长
	  ○ $11：进程的 CPU 占用率
	  ○ $12：进程名
	• 整个系统中 CPU 利用率最高的前 5 个核的信息：
	  ○ $13：核 ID
	  ○ $14：空闲时间
	  ○ $15：用户态进程占用的时间
	  ○ $16：内核线程占用的时间
	  ○ $17：中断占用的时间
	  ○ $18：运行时间

日志等级	3 (Error)
举例	DIAG/3/CPU_SEVERE_THRESHOLD: CPU usage is in severe alarm state. CPU usage: 3% in last 1 minute. CPU usage thresholds: Minor: 1% Severe: 2% Recovery: 0%

	Process info: JID PID PRI State FDs HH:MM:SS CPU Name 108398 108398 120 S 36 00:00:0 12.58% snmpd 52 52 102 S 0 00:01:2 2.58% [DRV_FWD] 371 371 120 S 95 00:18:5 0.17% pppd 90 90 120 R 18 00:12:0 0.34% diagd 109 109 119 S 41 00:11:1 0.00% vbrd Core states: ID Idle User Kernel Interrupt Busy CPU0 98.61% 0.24% 0.62% 0.53% 1.39% CPU1 99.88% 0.00% 0.03% 0.09% 0.12%
对系统的影响	设备运行速度会变慢，CPU处理业务能力会下降，可用CPU资源不足
日志产生原因	当CPU利用率的采样值从小于/等于变成大于高级别告警门限时，设备进入CPU高级别告警状态，并定期打印该日志，直到CPU高级别告警状态解除
处理建议	1. 请使用 **display cpu-usage configuration**命令查看CPU的告警门限，如果门限设置不合适，请使用 **monitor cpu-usage**命令修改 2. 如果持续 10 分钟以上未恢复，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

23.5 CPU_USAGE_LASTMINUTE

日志内容	CPU usage was [STRING] in last minute.
日志含义	显示CPU最近1分钟的平均利用率
参数解释	$1：CPU的利用率，为百分比格式
日志等级	5 (Notification)
举例	DIAG/5/CPU_USAGE_LASTMINUTE: CPU usage was 10% in last minute.
对系统的影响	对系统无影响
日志产生原因	显示CPU最近1分钟的平均利用率
处理建议	无需处理

23.6 DIAG_DEADLOOP_DETECT

日志内容	Deadloop detected on [STRING] cpu [INT] core [INT].
日志含义	系统检测到某个内核线程发生了死循环
参数解释	$1：chassis编号+slot编号或slot编号 $2：CPU编号 $3：CPU核编号
日志等级	0 (Emergency)
举例	DIAG/0/DIAG_DEADLOOP_DETECT: Deadloop detected on slot 1 cpu 0 core 0.
对系统的影响	进程无法正常工作，对应的业务会受到影响
日志产生原因	系统检测到某个内核线程发生了死循环时，打印该日志
处理建议	1. 通过 **display process**命令查看进程运行状态，如果进程长时间持续处于R状态，一定时间后该进程会被强制重启 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

23.7 DIAG_FD_UPLIMIT_REACHED

日志内容	FD number upper limit already reached: Process name=[STRING], PID=[INTEGER].
日志含义	进程已使用的FD个数已经达到上限
参数解释	$1：进程的名称 $2：进程的ID
日志等级	4 (Warning)
举例	DIAG/4/DIAG_FD_UPLIMIT_REACHED: FD number upper limit already reached: Process name=snmpd, PID=244.
对系统的影响	进程无法打开新的文件
日志产生原因	进程已使用的FD个数已经达到上限，打印该日志
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

23.8 DIAG_FD_UPLIMIT_TO_REACH

日志内容	Number of FDs is about to reach the upper limit: Process name=[STRING], PID=[INTEGER].
日志含义	进程已使用的FD个数即将达到上限
参数解释	$1：进程的名称 $2：进程的ID
日志等级	4 (Warning)
举例	DIAG/4/DIAG_FD_UPLIMIT_TO_REACH: Number of FDs is about to reach the upper limit: Process name=snmpd, PID=244.
对系统的影响	对系统暂无影响，但需要关注进程已使用的FD个数是否持续升高
日志产生原因	进程已使用的FD个数即将达到上限，打印该日志
处理建议	无需处理

23.9 DIAG_STORAGE_BELOW_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) was below or equal to the threshold of [UINT32]%.
日志含义	存储介质磁盘空间利用率小于或等于告警阈值
参数解释	$1：存储介质的名称 $2：存储介质磁盘空间利用率 $3：存储介质利用率阈值
日志等级	4 (Warning)
举例	DIAG/4/DIAG_STORAGE_BELOW_THRESHOLD: The usage of flash (90%) was below or equal to the threshold of 95%.
对系统的影响	对系统无影响
日志产生原因	当存储介质磁盘空间利用率小于或等于告警阈值时，打印该日志
处理建议	无需处理

23.10 DIAG_STORAGE_EXCEED_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) exceeded the threshold of [UINT32]%.
日志含义	存储介质磁盘空间利用率大于告警阈值
参数解释	$1：存储介质的名称 $2：存储介质磁盘空间利用率 $3：存储介质利用率的阈值
日志等级	4 (Warning)
举例	DIAG/4/DIAG_STORAGE_EXCEED_THRESHOLD: The usage of flash (96%) exceeded the threshold of 95%.
对系统的影响	需要写磁盘的业务处理会受影响，可用存储介质磁盘空间不足
日志产生原因	当存储介质磁盘空间利用率大于告警阈值时，打印该日志
处理建议	1. 检查磁盘状态。对长期不使用的文件，例如日志文件和历史版本的软件包，请使用 **delete /unreserved**命令直接删除或者备份到PC后再使用 **delete /unreserved**命令删除 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

23.11 MEM_ALERT

日志内容	system memory info: total used free shared buffers cached Mem: ［ULONG］ ［ULONG］ ［ULONG］ ［ULONG］ ［ULONG］ ［ULONG］ -/+ buffers/cache: ［ULONG］ ［ULONG］ Swap: ［ULONG］ ［ULONG］ ［ULONG］ Lowmem: ［ULONG］ ［ULONG］ ［ULONG］
日志含义	显示整个系统的内存统计信息

参数解释	• 整个系统中内存的统计信息：
	  ○ $1：系统可分配的物理内存的大小。设备总物理内存分为不可分配物理内存和可分配物理内存。其中，不可分配物理内存用于内核代码段存储、内核管理开销以及基本功能的运行等；可分配物理内存用于支撑业务模块的运行、文件存储等操作。不可分配内存的大小由设备根据系统运行需要自动计算划分，可分配物理内存的大小等于设备总物理内存减去不可分配内存的大小
	  ○ $2：整个系统已用的物理内存大小
	  ○ $3：整个系统可用的物理内存大小
	  ○ $4：多个进程共享的物理内存总额
	  ○ $5：已使用的文件缓冲区的大小
	  ○ $6：高速缓冲寄存器已使用的内存大小
	• 应用程序对内存的使用情况：
	  ○ $7：-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached，表示应用程序已用的物理内存大小
	  ○ $8：-/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached，表示应用程序可用的物理内存大小
	• 交换分区的使用信息：
	  ○ $9：交换分区的总大小
	  ○ $10：已用的交换分区的大小
	  ○ $11：可用的交换分区的大小
	• Low memory 的使用情况：
	  ○ $12：Low memory 中内存的大小
	  ○ $13：Low memory 中已用内存的大小
	  ○ $14：Low memory 中可用内存的大小

日志等级	4 (Warning)
举例	DIAG/4/MEM_ALERT: system memory info: total used free shared buffers cached Mem: 1784424 920896 863528 0 0 35400 -/+ buffers/cache: 885496 898928 Swap: 0 0 0 Lowmem: 735848 637896 97952
对系统的影响	对系统暂无影响，但需要关注可用内存是否持续减少
日志产生原因	当已使用的内存大于或等于一级、二级或三级内存告警门限时，系统会打印该日志，告知用户内存的具体使用情况

处理建议	1. 请使用 **display memory-threshold**命令查看内存的一级、二级、三级告警门限。如果门限设置不合适，请使用 **memory-threshold**命令修改 2. 检查 ARP、路由表信息，排除设备受到非法攻击可能 3. 检查和优化组网，减少路由条目或者更换更高规格的设备

23.12 MEM_BELOW_THRESHOLD

日志内容	Memory usage has dropped below [STRING] threshold.
日志含义	内存使用率低于告警阈值
参数解释	$1：内存告警门限级别，包括： ○ minor：一级 ○ severe：二级 ○ critical：三级 ○ early-warning：预告警
日志等级	1 (Alert)
举例	DIAG/1/MEM_BELOW_THRESHOLD: Memory usage has dropped below critical threshold.
对系统的影响	对系统无影响
日志产生原因	当内存使用率低于告警阈值时，系统解除内存告警状态，并打印该日志
处理建议	无需处理

23.13 MEM_EXCEED_THRESHOLD

日志内容	Memory［STRING］threshold has been exceeded.
日志含义	内存利用率大于或等于告警阈值
参数解释	$1：内存告警门限级别，包括： ○ minor：一级 ○ severe：二级 ○ critical：三级 ○ early-warning：预告警
日志等级	1 (Alert)
举例	DIAG/1/MEM_EXCEED_THRESHOLD: Memory minor threshold has been exceeded.
对系统的影响	设备运行速度会变慢，可用内存资源不足
日志产生原因	当内存利用率大于或等于预告警、一级、二级或三级内存利用率告警阈值时，打印该日志，并通知各业务模块进行自动修复，如不再申请新的内存或者释放部分内存
处理建议	1. 请使用 **display memory-threshold**命令查看内存的一级、二级、三级告警门限。如果门限设置不合适，请使用 **memory-threshold**命令修改 2. 检查 ARP、路由表信息，排除设备受到非法攻击可能 3. 检查和优化组网，减少路由条目或者更换更高规格的设备

23.14 MEM_USAGE

日志内容	Current memory usage is [STRING].
日志含义	设备当前的内存利用率
参数解释	$1：内存的利用率，为百分比格式
日志等级	5 (Notification)
举例	DIAG/5/MEM_USAGE: Current memory usage is 10%.
对系统的影响	对系统无影响
日志产生原因	显示设备当前的内存利用率
处理建议	无需处理

24 DLDP

本节介绍 DLDP 模块输出的日志信息。

24.1 DLDP_AUTHENTICATION_FAILED

日志内容	The DLDP packet failed the authentication because of unmatched [STRING] field.
日志含义	报文验证失败
参数解释	$1：验证字段 ○ AUTHENTICATION PASSWORD：表示验证字不匹配 ○ AUTHENTICATION TYPE：表示验证类型不匹配 ○ INTERVAL：表示通告间隔不匹配
日志等级	5 (Notification)
举例	DLDP/5/DLDP_AUTHENTICATION_FAILED: The DLDP packet failed the authentication because of unmatched INTERVAL field.
对系统的影响	DLDP功能无法正常工作
日志产生原因	验证类型不匹配、验证字不匹配、通告间隔不匹配
处理建议	检查DLDP验证类型、验证字和通告间隔是否与对端一致

24.2 DLDP_LINK_BIDIRECTIONAL

日志内容	DLDP detected a bidirectional link on interface [STRING].
日志含义	DLDP在接口上检测到双向链路
参数解释	$1：接口名
日志等级	6 (Informational)
举例	DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface Ethernet1/1.
对系统的影响	无
日志产生原因	光纤正常连接
处理建议	无需处理

24.3 DLDP_LINK_SHUTMODECHG

日志内容	DLDP automatically [STRING] interface [STRING] because the port shutdown mode was changed [STRING].
日志含义	因为DLDP单通关闭模式发生变化，端口被关闭或打开
参数解释	$1：接口关闭模式指定的动作 ○ blocked：表示 DLDP 关闭了端口 ○ brought up：表示 DLDP 打开了端口 $2：接口名 $3：接口关闭模式切换指向 ○ from manual to auto：表示由手动模式切换到自动模式 ○ from manual to hybrid：表示由手动模式切换到混合模式 ○ from hybrid to auto：表示由混合模式切换到自动模式 ○ from hybrid to manual：表示由混合模式切换到手动模式
日志等级	5 (Notification)
举例	DLDP/5/DLDP_LINK_SHUTMODECHG: DLDP automatically blocked interface Ethernet1/1 because the port shutdown mode was changed from manual to auto.
对系统的影响	端口被关闭时，该接口无法转发业务流量
日志产生原因	因为DLDP单通关闭模式发生变化，端口被关闭或打开
处理建议	端口被关闭时，检查线缆是否错接、脱落或者出现其他故障

24.4 DLDP_LINK_UNIDIRECTIONAL

日志内容	DLDP detected a unidirectional link on interface [STRING]. [STRING].
日志含义	DLDP在接口上检测到单向链路
参数解释	$1：接口名 $2：接口关闭模式所指定的动作 ○ DLDP automatically blocked the interface：表示 DLDP 自动关闭了端口 ○ Please manually shut down the interface：表示需要用户手动关闭端口
日志等级	3 (Error)
举例	DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface Ethernet1/1. DLDP automatically blocked the interface.
对系统的影响	该接口无法正常转发业务流量
日志产生原因	• 端口的一条光纤未连接或断路 • 光纤交叉连接
处理建议	检查线缆是否错接、脱落或者出现其他故障

24.5 DLDP_NEIGHBOR_AGED

日志内容	A neighbor on interface [STRING] was deleted because the neighbor was aged. The neighbor's system MAC is [MAC], and the port index is [UINT16].
日志含义	接口删除了一个已老化的邻居
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	5 (Notification)
举例	DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface Ethernet1/1 was deleted because the neighbor was aged. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
对系统的影响	DLDP邻居关系无法建立，DLDP检测连接无法建立
日志产生原因	邻居老化定时器超时时间内，没有接收到Advertisement报文
处理建议	无需处理

24.6 DLDP_NEIGHBOR_CONFIRMED

日志内容	A neighbor was confirmed on interface [STRING]. The neighbor's system MAC is [MAC], and the port index is [UINT16].
日志含义	接口检测到一个处于确定状态的邻居
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	6 (Informational)
举例	DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface Ethernet1/1. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
对系统的影响	无
日志产生原因	邻居老化定时器超时时间内，接收到Advertisement报文
处理建议	无需处理

24.7 DLDP_NEIGHBOR_DELETED

日志内容	A neighbor on interface [STRING] was deleted because a [STRING] packet arrived. The neighbor's system MAC is [MAC], and the port index is [UINT16].
日志含义	由于收到了Disable报文或LinkDown报文，因此接口删除一个处于确定状态的邻居
参数解释	$1：接口名 $2：报文类型 ○ DISABLE：表示收到了 Disable 报文 ○ LINKDOWN：表示收到了 LinkDown 报文 $3：MAC地址 $4：接口索引
日志等级	5 (Notification)
举例	DLDP/5/DLDP_NEIGHBOR_DELETED: A neighbor on interface Ethernet1/1 was deleted because a DISABLE packet arrived. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
对系统的影响	DLDP邻居关系无法建立，DLDP检测连接无法建立
日志产生原因	收到了Disable报文或LinkDown报文
处理建议	无需处理

25 DOT1X

本节介绍 802.1X（DOT1X）模块输出的日志信息。

25.1 DOT1X_CLEAR_MAX_USER_THRESHOLD

日志内容	The max-user alarm trigger condition cleared when the percentage of online 802.1X users reached or dropped below the max-user alarm clear threshold on interface [STRING].
日志含义	接口上的802.1X用户接入率下降到恢复阈值或小于恢复阈值
参数解释	$1：接口名
日志等级	5 (Notification)
举例	DOT1X/5/DOT1X_CLEAR_MAX_USER_THRESHOLD: The max-user alarm trigger condition cleared when the percentage of online 802.1X users reached or dropped below the max-user alarm clear threshold on interface GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	端口上802.1X接入用户数与802.1X最大接入用户数的百分比从大于等于上限告警阈值下降到恢复阈值时，系统输出此日志信息
处理建议	无需处理

25.2 DOT1X_CONFIG_NOTSUPPORT

日志内容	802.1X is not supported on interface [STRING].
日志含义	接口不支持802.1X特性
参数解释	$1：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_CONFIG_NOTSUPPORT: 802.1X is not supported on interface GigabitEthernet1/0/1.
对系统的影响	该接口无法使用802.1X功能
日志产生原因	在不支持802.1X特性的接口使能802.1X时，系统输出此日志
处理建议	关闭该接口的802.1X功能，在支持802.1X特性的接口配置802.1X功能

25.3 DOT1X_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; User failed 802.1X authentication. Reason: [STRING].
日志含义	802.1X用户认证失败
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：错误码 $6：用户802.1X认证失败的原因： • MAC address authorization failed：授权 MAC 地址失败 • VLAN authorization failed：授权 VLAN 失败 • VSI authorization failed：授权 VSI 失败 • ACL authorization failed：授权 ACL 失败 • User profile authorization failed：授权 User Profile 失败 • URL authorization failed：授权 URL 失败 • Microsegment authorization failed：授权微分段失败 • VSI authorization failed because of insufficient resources：资源不足，授权 VSI 失败 • ACL authorization failed because of insufficient resources：资源不足，授权 ACL 失败 • MAC address authorization failed after a MAC move：MAC 迁移后授权 MAC 失败 • VLAN authorization failed because of failure in authorization VLAN selection：选择授权 VLAN 失败 • VLAN authorization failed because a free VLAN was assigned as the authorization VLAN：授权 VLAN 为 free VLAN，授权失败 • VLAN authorization failed because of failure in authorization VLAN creation：创建授权 VLAN 失败 • Tagged VLAN authorization failed in port-based access control：port-based 接入控制方式下授权 tag VLAN 失败 • Untagged VLAN authorization failed in port-based access control：port-based 接入控制方式下授权 untag VLAN 失败 • Tagged VLAN authorization failed in MAC-based access control：mac-based 接入控制方式下授权 tag VLAN 失败 • Untagged VLAN authorization failed in MAC-based access control：mac-based 接入控制方式下授权 untag VLAN 失败 • VSI authorization failed because the user belongs to a free VLAN：用户加入了 free vlan，授权 VSI 失败 • VSI authorization failed because the user's access interface does not permit the user VLAN ：接口不允许用户 VLAN 通过，授权 VSI 失败 • VSI authorization failed because of failure in AC creation：创建 AC 失败，授权 VSI 失败 • ACL authorization failed because the specified ACL does not exist：ACL 不存在，授权 ACL 失败

	• ACL authorization failed because of unsupported ACL type：ACL 类型不支持，授权 ACL 失败 • ACL authorization failed because the specified ACL conflicts with other ACLs on the user's access interface：ACL 与所在接口其他 ACL 冲突，授权 ACL 失败 • ACL authorization failed because no rule was obtained for the specified ACL：无法获取任何 ACL 规则，授权 ACL 失败 • ACL authorization failed because of ACL parameter error：ACL 的相关参数出错，授权 ACL 失败 • User profile authorization failed because an invalid user profile was assigned to the user (the authorization-fail offline feature is enabled)：配置了授权失败下线功能，User Profile 非法 • User profile authorization failed because of failure in issuing the specified user profile to driver：下驱动失败 • URL authorization failed because of insufficient resources：资源不足，授权 URL 失败 • URL authorization failed because of invalid parameter in the specified URL：URL 参数错误，授权 URL 失败 • URL authorization failed because the specified URL was not supported：不支持 URL，授权 URL 失败 • URL authorization failed because of deny rule issuing failure：下发 deny 规则失败，授权 URL 失败 • URL authorization failed because of failure in issuing the specified URL to driver：下驱动失败，授权 URL 失败 • URL authorization failed because no servers were reachable and the url-user-logoff parameter was specified：配置 Critical microsegment、Critical VSI 时指定了 url-user-logoff 参数，服务器不可达时，授权 URL 失败 • URL authorization failed because the escape critical VSI feature of port security was configured：配置了端口安全逃生到 Critical VSI 功能，授权 URL 失败
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0001-0020-VLANID=2-Username=aaa-ErrCode=5; User failed 802.1X authentication. Reason: ACL authorization failed.
对系统的影响	802.1X用户无法上线
日志产生原因	参见打印的认证失败原因
处理建议	**1.** 请确认 802.1X 认证相关配置正确 **2.** 请根据打印的认证失败原因定位问题。如果是设备或认证服务器上配置错误，请及时修改设备或服务器配置 **3.** 如果问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.4 DOT1X_LOGIN_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANID=[STRING]-AuthorizationVLANID=[STRING]-Username=[STRING]; User passed 802.1X authentication and came online.
日志含义	802.1X用户认证成功并上线
参数解释	$1：接口名 $2：MAC地址 $3：接入VLAN ID $4：授权VLAN ID $5：用户名
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-AccessVLANID=444-AuthorizationVLANID=444-Username=aaa; User passed 802.1X authentication and came online.
对系统的影响	802.1X用户成功上线
日志产生原因	当802.1X用户认证成功并上线时，系统输出此日志
处理建议	无需处理

25.5 DOT1X_LOGIN_SUCC (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; The user that failed 802.1X authentication passed open authentication and came online.
日志含义	802.1X认证失败但通过开放认证模式认证成功并上线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9; The user that failed 802.1X authentication passed open authentication and came online.
对系统的影响	802.1X用户成功上线
日志产生原因	当802.1X认证失败但通过开放认证模式认证成功并上线时，系统输出此日志
处理建议	无需处理

25.6 DOT1X_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; The 802.1X user was logged off because [STRING].
日志含义	802.1X用户正常下线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：客户端下线原因，包括如下取值： • 客户端主动发送 EAPOL-Logoff 报文下线：the client requested to log off the user • IP 电话 PC 口掉线：the PC port connection was lost
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa; The 802.1X user was logged off because the PC port connection was lost.
对系统的影响	802.1X用户下线
日志产生原因	当802.1X用户正常下线时，系统输出此日志
处理建议	无需处理

25.7 DOT1X_LOGOFF (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; The 802.1X open user was logged off because [STRING].
日志含义	802.1X open用户正常下线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：客户端下线原因，包括如下取值： • 客户端主动发送 EAPOL-Logoff 报文下线：the client requested to log off the user • IP 电话 PC 口掉线：the PC port connection was lost
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa; The 802.1X open user was logged off because the PC port connection was lost.
对系统的影响	802.1X open用户下线
日志产生原因	当802.1X open用户正常下线时，系统输出此日志
处理建议	无需处理

25.8 DOT1X_LOGOFF_ABNORMAL

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X user was logged off abnormally.
日志含义	802.1X用户异常下线

参数解释	$1：接口名
	$2：MAC地址
	$3：VLAN ID
	$4：用户名
	$5：错误码，包括如下取值：
	• 2：端口状态错误。可能原因为：
	  ◦ 设备向服务器发送授权请求或者获取授权信息失败
	  ◦ 进程重启或者主备倒换平滑在线用户时，端口 down 或者 deactive
	  ◦ 生效的授权 VLAN 不在端口允许的 VLAN 列表里
	  ◦ 接口上使能 802.1X SmartOn 功能，将未通过认证的用户踢下线
	• 3：目前不支持这种失败类型
	• 4：用户重认证失败
	• 5：设备强制去授权。可能原因为：
	  ◦ 授权处理失败
	  ◦ 上线用户数超过最大值
	  ◦ 全局关闭 OPEN 认证模式，OPEN 用户下线
	  ◦ 关闭 802.1X 功能，用户下线
	  ◦ 响应 MAC-VLAN 关闭事件，用户下线
	  ◦ 执行 **reset dot1x access-user**命令强制用户下线
	• 6：端口重启。目前不支持这种失败类型
	• 7：用户平滑过程中，执行如下操作导致用户下线：
	  ◦ 关闭 802.1X 功能
	  ◦ 执行 **dot1x port-method**命令修改端口的接入控制方式
	  ◦ 执行 **dot1x port-control**命令修改设置端口的授权状态
	• 8：用户名或密码错误，或者服务器端没有配置设备信息
	• 9：设备未收到客户端的握手报文
	• 10：闲置切断。原因可能为用户在下线检测周期内没有流量，设备强制用户下线
	• 11：限制用户在线时长（通过服务器下发的 session timeout 字段来设置）的切断。原因可能为 802.1X 会话超时导致设备强制用户下线
	• 12：服务器发起的强制用户下线。原因可能为：
	  ◦ 在服务器端强制指定的用户下线
	  ◦ 服务器通过 session control 功能强制用户下线
	• 13：实时计费失败
	• 14：缺省错误，原因可能为：
	  ◦ MAC 绑定处理失败
	  ◦ 认证成功后，清除操作 VLAN（Guest VLAN、Auth-Fail VLAN 和 Critical VLAN）失败

	◦ 计费失败 ◦ 处理 IPCIM 事件后重授权失败 • 15：用户上线的接口 DOWN • 16：PC 口掉线
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGOFF_ABNORMAL:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X user was logged off abnormally.
对系统的影响	802.1X用户异常下线
日志产生原因	参见打印的错误码信息
处理建议	1. 请根据打印的错误码定位问题，及时修改设备及服务器相关配置 2. 如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.9 DOT1X_LOGOFF_ABNORMAL (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X open user was logged off abnormally.
日志含义	802.1X open用户异常下线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：错误码
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_LOGOFF_ABNORMAL:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X open user was logged off abnormally.
对系统的影响	802.1X open用户异常下线
日志产生原因	参见打印的错误码信息
处理建议	1. 请根据打印的错误码定位问题，及时修改设备及服务器相关配置 2. 如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.10 DOT1X_MACBINDING_EXIST

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; MAC address was already bound to interface [STRING].
日志含义	用户MAC地址已绑定在其它端口
参数解释	$1：用户接入的接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：已绑定MAC地址的接口名
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_MACBINDING_EXIST: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0001-0020-VLANID=2-Username=aaa; MAC address was already bound to interface GigabitEthernet1/0/3.
对系统的影响	用户无法从该端口上线
日志产生原因	当802.1X用户MAC地址已绑定在其它端口时，系统输出此日志
处理建议	如果希望802.1X用户从新端口上线，则请在其它端口取消MAC地址绑定

25.11 DOT1X_MAX_USER_THRESHOLD

日志内容	The percentage of online 802.1X users reached or exceeded the max-user alarm trigger threshold on interface [STRING].
日志含义	接口上的802.1X用户接入率大于等于阈值
参数解释	$1：接口名
日志等级	4 (Warning)
举例	DOT1X/4/DOT1X_MAX_USER_THRESHOLD: The percentage of online 802.1X users reached or exceeded the max-user alarm trigger threshold on interface GigabitEthernet1/0/1.
对系统的影响	当802.1X接入用户达到最大接入用户数时，新802.1X用户无法上线
日志产生原因	端口上802.1X接入用户数与802.1X最大接入用户数的百分比首次达到指定的上限阈值，或者从小于等于恢复阈值增长到上限阈值时，设备输出此日志信息
处理建议	1. 通过**display dot1x interface**命令查看802.1X接入用户数的最大值，若802.1X接入用户数最大值过小，请重新配置 2. 通过**display dot1x**命令查看802.1X接入用户数上限告警阈值，若802.1X接入用户数上限告警阈值过小，请重新配置 3. 如果问题仍未解决，请收集告警信息、日志信息和配置信息，联系技术支持工程师进行处理

25.12 DOT1X_NOTENOUGH_EADFREEIP_RES

日志内容	Failed to assign a rule for Free IP [IPADDR] on interface [STRING] due to lack of ACL resources.
日志含义	由于ACL资源不足，设备在接口上下发Free IP失败
参数解释	$1：IP地址 $2：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_NOTENOUGH_EADFREEIP_RES: Failed to assign a rule for Free IP 1.1.1.0 on interface Ethernet3/1/2 due to lack of ACL resources.
对系统的影响	用户无法访问Free IP内的资源
日志产生原因	配置EAD快速部署功能后，在接口上使能802.1X特性时，由于ACL资源不足，设备在接口上下发Free IP失败
处理建议	**1.** 当前设备可能业务繁忙，暂不使能 802.1X，请稍等片刻后尝试重新使能 802.1X **2.** 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.13 DOT1X_NOTENOUGH_EADFREEMSEG_RES

日志内容	Failed to assign a rule for free microsegment [STRING] on interface [STRING] due to lack of ACL resources.
日志含义	由于ACL资源不足，设备在接口上下发免认证微分段失败
参数解释	$1：微分段ID $2：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_NOTENOUGH_EADFREEMSEG_RES: Failed to assign a rule for free microsegment 1 on interface Ethernet3/1/2 due to lack of ACL resources.
对系统的影响	用户无法访问免认证微分段内的资源
日志产生原因	配置EAD快速部署功能后，在接口上使能802.1X特性时，由于ACL资源不足，设备在接口上下发免认证微分段失败
处理建议	**1.** 当前设备可能业务繁忙，暂不使能 802.1X，请稍等片刻后尝试重新使能 802.1X **2.** 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.14 DOT1X_NOTENOUGH_EADFREERULE_RES

日志内容	Failed to assign a rule for permitting DHCP and DNS packets on interface [STRING] due to lack of ACL resources.
日志含义	由于ACL资源不足，接口上DHCP协议和DNS协议报文的过滤规则下发失败
参数解释	$1：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_NOTENOUGH_EADFREERULE_RES: Failed to assign a rule for permitting DHCP and DNS packets on interface Ethernet3/1/2 due to lack of ACL resources.
对系统的影响	无法对DHCP协议和DNS协议报文进行过滤
日志产生原因	配置EAD快速部署功能后，在接口上使能802.1X特性时，由于ACL资源不足，接口上DHCP协议和DNS协议报文的过滤规则下发失败
处理建议	**1.** 当前设备可能业务繁忙，暂不使能 802.1X，请稍等片刻后尝试重新使能 802.1X **2.** 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.15 DOT1X_NOTENOUGH_EADMACREDIR_RES

日志内容	Failed to assign a rule for redirecting HTTP packets with source MAC address [MAC] on interface [STRING].
日志含义	由于ACL资源不足，对指定接口上收到的固定源MAC地址的HTTP报文下发重定向规则失败
参数解释	$1：HTTP报文源MAC地址 $2：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_NOTENOUGH_EADMACREDIR_RES: Failed to assign a rule for redirecting HTTP packets with source MAC address 00e0-fc00-5915 on interface Ethernet3/1/2.
对系统的影响	HTTP报文无法重定向
日志产生原因	配置EAD快速部署功能后，在接口上使能802.1X特性时，由于ACL资源不足，对指定接口上收到的固定源MAC地址为HTTP报文下发重定向规则失败
处理建议	**1.** 当前设备可能业务繁忙，暂不使能 802.1X，请稍等片刻后尝试重新使能 802.1X **2.** 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.16 DOT1X_NOTENOUGH_EADPORTREDIR_RES

日志内容	Failed to assign a rule for redirecting HTTP packets on interface [STRING] due to lack of ACL resources.
日志含义	由于ACL资源不足，对指定接口收到的HTTP报文下发重定向规则失败
参数解释	$1：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_NOTENOUGH_EADPORTREDIR_RES: Failed to assign a rule for redirecting HTTP packets on interface Ethernet3/1/2 due to lack of ACL resources.
对系统的影响	HTTP报文无法重定向
日志产生原因	配置EAD快速部署功能后，在接口上使能802.1X特性时，由于ACL资源不足，对指定接口收到的HTTP报文下发重定向规则失败
处理建议	1. 当前设备可能业务繁忙，暂不使能 802.1X，请稍等片刻后尝试重新使能 802.1X 2. 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.17 DOT1X_NOTENOUGH_ENABLEDOT1X_RES

日志内容	Failed to enable 802.1X on interface [STRING] due to lack of ACL resources.
日志含义	由于ACL资源不足，无法使能802.1X功能
参数解释	$1：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_NOTENOUGH_ENABLEDOT1X_RES: Failed to enable 802.1X on interface Ethernet3/1/2 due to lack of ACL resources.
对系统的影响	无法使能802.1X功能
日志产生原因	ACL资源不足时，使能802.1X功能
处理建议	1. 当前设备可能业务繁忙，暂不使能 802.1X，请稍等片刻后尝试重新使能 802.1X 2. 如果问题无法及时解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

25.18 DOT1X_PEXAGG_NOMEMBER_RES

日志内容	Failed to enable 802.1X on interface [STRING] because the Layer 2 extended-link aggregate interface does not have member ports.
日志含义	PEX二层聚合口不存在成员口，不能在该接口使能802.1X特性
参数解释	$1：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_PEXAGG_NOMEMBER_RES: Failed to enable 802.1X on interface Bridge-Aggregation100 because the Layer 2 extended-link aggregate interface does not have member ports.
对系统的影响	该PEX二层聚合口的802.1X功能不生效
日志产生原因	PEX二层聚合口不存在成员口，不能配置接口的802.1X特性
处理建议	暂不使能802.1X，PEX二层聚合口添加成员口后重新使能802.1X

25.19 DOT1X_SMARTON_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; User failed SmartOn authentication because [STRING].
日志含义	SmartOn认证失败及其原因
参数解释	$1：接口名 $2：MAC地址 $3：失败原因，包括如下取值： • the password was wrong：密码错误 • the switch ID was wrong：Switch ID 错误
日志等级	6 (Informational)
举例	DOT1X/6/DOT1X_SMARTON_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; User failed SmartOn authentication because the password is mismatched.
对系统的影响	SmartOn认证失败
日志产生原因	由于以下原因，SmartOn认证失败： • 密码错误 • Switch ID 错误
处理建议	请确保设备和客户端上配置的密码及Switch ID一致

25.20 DOT1X_UNICAST_NOT_EFFECTIVE

日志内容	The unicast trigger feature is enabled but is not effective on interface [STRING].
日志含义	由于接口不支持单播触发特性，因此单播触发特性在接口上不生效
参数解释	$1：接口名
日志等级	3 (Error)
举例	DOT1X/3/DOT1X_UNICAST_NOT_EFFECTIVE: The unicast trigger feature is enabled but is not effective on interface Ethernet3/1/2.
对系统的影响	单播触发特性在接口上不生效
日志产生原因	在不支持单播触发特性的接口配置了单播触发功能
处理建议	切换到支持单播触发功能的接口上对用户进行802.1X认证

26 DRVPLAT

26.1 DRVPLAT

26.1.1 DrvDebug

日志内容	The temperature of hotspot [UINT32] in chassis [UINT32] slot [UINT32] reached [UINT32]. The temperature exceeded the shutdown threshold and the card is rebooting.
参数解释	$1： 热点传感器编号 $2：设备在IRF中的成员编号 $3：单板所在的槽位号 $4：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: The temperature of hotspot 1 in chassis 1 slot 1 reached 111. The temperature exceeded the shutdown threshold and the card is rebooting.
日志说明	IRF模式下，单板热点温度超过温度传感器的温度门限
处理建议	请查看风扇运行是否正常

26.1.2 DrvDebug

日志内容	The temperature of hotspot [UINT32] in slot [UINT32] reached [UINT32]. The temperature exceeded the shutdown threshold and the card is rebooting.
参数解释	$1： 热点传感器编号 $2：单板所在的槽位号 $3：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: The temperature of hotspot 1 in slot 1 read 111. The temperature exceeded the shutdown threshold and the card is rebooting.
日志说明	独立运行模式下，单板热点温度超过温度传感器的温度门限
处理建议	请查看风扇运行是否正常

26.1.3 DrvDebug

日志内容	The (undo) cut-through enable command requires a reboot to take effect.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Slot=1; The (undo) cut-through enable command requires a reboot to take effect.
日志说明	配置cut-through enable或undo cut-through enable命令后，必须保存配置并重启设备才能生效
处理建议	保存配置并重启设备

26.1.4 DrvDebug

日志内容	The device will reboot because the chip temperature is [UINT32] degrees, exceeding the overtemperature reboot threshold of [UINT32] degrees.
参数解释	$1：当前芯片温度 $2：过温重启门限
日志等级	4
举例	DRVPLAT/4/DrvDebug: The device will reboot because the chip temperature is 128 degrees, exceeding the overtemperature reboot threshold of 122 degrees.
日志说明	检测到芯片温度超过过温重启门限122度，当前芯片温度为128度，设备重启
处理建议	检查设备风扇模块是否正常

26.1.5 DrvDebug

日志内容	Port [STRING] is an IRF physical interface. You cannot activate the port basic function license for it.
参数解释	$1：本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: Port HundredGigE1/0/49 is an IRF physical interface. You cannot activate the port basic function license for it.
日志说明	IRF物理端口不支持激活端口License
处理建议	请先取消IRF物理端口配置，再激活端口License

26.1.6 DrvDebug

日志内容	Port basic function license is enabled for IRF physical interface [STRING]. For IRF to function correctly, deactivate the license for the interface.
参数解释	$1：本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: Port basic function license is enabled for IRF physical interface HundredGigE1/0/49. For IRF to function correctly, deactivate the license for the interface.
日志说明	激活了端口License的IRF物理端口，IRF功能可能会有问题
处理建议	请卸载或去激活IRF物理端口的端口License

26.1.7 DrvDebug

日志内容	Interface [STRING] is a breakout interface. A breakout interface does not support deactivating the basic port functionality license.
参数解释	$1：本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: Interface Twenty-FiveGigE 1/0/49:1 is a breakout interface. A breakout interface does not support deactivating the basic port functionality license.
日志说明	拆分接口不支持取消激活端口License
处理建议	将拆分接口合并后，再取消激活端口License

26.1.8 DRVPLAT/4/DrvDebug

日志内容	The per-packet load sharing configuration cannot take effect, because the ECMP mode is eligibility. To have the configuration take effect, first change the ECMP mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: The per-packet load sharing configuration cannot take effect, because the ECMP mode is eligibility. To have the configuration take effect, first change the ECMP mode.
日志说明	等价路由Eligibility模式与逐包负载分担功能无法同时生效，并且等价路由Eligibility模式的生效优先级高于逐包负载分担。当已经使用ecmp mode命令配置等价路由为Eligibility模式，再配置逐包负载分担功能时，提示用户该设备已经配置了Eligibility模式，逐包负载分担功能不生效。
处理建议	根据提示进行配置，若有问题，请联系技术支持。

26.1.9 DRVPLAT/4/DrvDebug

日志内容	The eligibility ECMP mode configuration succeeded, and the per-packet load sharing configuration will fail to take effect. To have the configuration take effect, first change the ECMP mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: The eligibility ECMP mode configuration succeeded, and the per-packet load sharing configuration will fail to take effect. To have the configuration take effect, first change the ECMP mode.
日志说明	等价路由Eligibility模式与逐包负载分担功能无法同时生效，并且等价路由Eligibility模式的生效优先级高于逐包负载分担。当已经配置了逐包负载分担功能时，再配置等价路由Eligibility模式，提示逐包负载分担功能将会失效，如果想要逐包负载分担功能生效，请修改等价路由模式。
处理建议	根据提示进行配置，若有问题，请联系技术支持。

26.1.10 DRVPLAT/4/DrvDebug

日志内容	Eligibility ECMP mode disabled successfully, and the per-packet load sharing configuration has taken effect.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Eligibility ECMP mode disabled successfully, and the per-packet load sharing configuration has taken effect.
日志说明	等价路由Eligibility模式与逐包负载分担功能无法同时生效，并且等价路由Eligibility模式的生效优先级高于逐包负载分担。当同时配置等价路由Eligibility模式和逐包负载分担功能，此时去使能等价路由Eligibility模式，逐包负载分担功能会恢复正常。
处理建议	根据提示进行配置，若有问题，请联系技术支持。

26.1.11 DrvDebug

日志内容	I2c read need to retry, p1= [STRING], p2 = [STRING], times: [STRING]
参数解释	$1：总线地址 $2：设备地址 $3：重试次数 其中times 参数最大为3，即如果出现3代表通过总共4次访问均失败，如果小于3，可忽略
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c read need to retry, p1=0x52, p2 = 0x20, times: 0 在读eeprom（0x52为eeprom的I2C 总线地址）的地址0x20时，出现错误，需要重试
日志说明	I2C总线读操作过程中出现错误，需要重试
处理建议	如果出现times ：3代表通过总共4次访问均失败，请联系技术支持 如果小于3，可忽略

26.1.12 DrvDebug

日志内容	I2c write need to retry, p1 = [STRING], p2 = [STRING], times: [STRING]
参数解释	$1：总线地址 $2：设备地址 $3：重试次数 其中times 参数最大为3，即如果出现3代表通过总共4次访问均失败，如果小于3，可忽略
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c write need to retry, p1=0x52, p2 = 0x20, times: 0 在写eeprom（0x52为eeprom的I2C 总线地址）的地址0x20时，出现错误，需要重试
日志说明	I2C总线写操作过程中出现错误，需要重试
处理建议	如果出现times ：3代表通过总共4次访问均失败，请联系技术支持 如果小于3，可忽略

26.1.13 DrvDebug

日志内容	I2C Stop,bus is busy!
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	提示I2C总线忙
处理建议	请联系技术支持

26.1.14 DrvDebug

日志内容	I2c Start, read state retry!
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	提示I2C总线发送Start命令后，发送完成状态寄存器一直未显示发送完成
处理建议	请忽略

26.1.15 DrvDebug

日志内容	I2c Start, write cmd retry!
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	I2C总线发送start命令后，程序判断波形未发出，进行重试操作
处理建议	请忽略

26.1.16 DrvDebug

日志内容	There is no i2c device ack!
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	提示当写数据时I2C总线中断过程错误，并给出进程号和I2C设备地址
处理建议	请联系技术支持

26.1.17 DrvDebug

日志内容	I2c Read, transmit state retry! i = [STRING].
参数解释	$1：I2C读取数据的第几个字节出现了错误。状态寄存器一直显示未完成，程序会进行重试 注：驱动代码中，一次I2C读操作可以读取多个字节
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c Read, transmit state retry! i = 2. 一次读多个字节，读取第3个（i是从0开始计数的）的时候出现了错误
日志说明	提示当读数据时，I2C总线一直处于未完成状态，并给出第几个字节出现错误
处理建议	程序会自行重试，请忽略

26.1.18 DrvDebug

日志内容	I2c Write, transmit state retry! i =[STRING].
参数解释	参数解释 $1：I2C写入数据的第几个字节出现了错误。状态寄存器一直显示未完成，程序会进行重试 注：驱动代码中，一次I2C写操作可以写入多个字节
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c Write, transmit state retry! i = 2. 一次写多个字节，写入第3个（i是从0开始计数的）的时候出现了错误
日志说明	提示当读数据时I2C总线中断过程错误，并给出进程号和I2C设备地址
处理建议	程序会自行重试，请忽略

26.1.19 DrvDebug

日志内容	I2c write no ack count = [STRING].. i = [STRING]..
参数解释	$1：本次写操作写入字节总数 $2：写入第几个出现了未收到ACK的错误
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c write no ack count = 3.. i = 2..
日志说明	提示写入总共3个字节，第3个（i是从0开始计数的）出现了错误
处理建议	程序会自行重试，请忽略

26.1.20 DrvDebug

日志内容	I2C read or write! DevAddr = [STRING], WR = [STRING], len = [STRING], num = [STRING], i = [STRING]
参数解释	$1：设备的总线地址 $2：0，指写操作；1，指读操作 $3：一次读/写字节数 $4：一次操作发送I2C start的次数 $5：读/写第几个字节的时候出现了错误
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2C read or write! DevAddr = 0x52, WR = 1, len = 3, num = 2, i = 2 eeprom（0x52为eeprom设备地址），读操作，一次读取3个字节，发送了2个start，在第3个字节出现了错误
日志说明	提示I2C总线访问失败，打印参数方便问题定位
处理建议	程序会自行重试，请忽略

26.1.21 DrvDebug

日志内容	I2C stop! DevAddr = [STRING], WR = [STRING], len = [STRING], num = [STRING], i = [STRING]
参数解释	$1：设备的总线地址 $2：0，指写操作；1，指读操作 $3：一次读/写字节数 $4：一次操作发送I2C start的次数 $5：读/写第几个字节的时候出现了错误
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2C stop! DevAddr = 0x52, WR = 1, len = 3, num = 2, i = 2 eeprom（0x52为eeprom设备地址），读操作，一次读取3个字节，发送了2个start，在第3个字节出现了错误
日志说明	提示I2C总线发送stop命令失败，打印参数方便问题定位
处理建议	程序会自行重试，请忽略

26.1.22 DrvDebug

日志内容	PCA9548 sel, write need to retry, present try times is [STRING],.
参数解释	其中times 参数最大为3，即如果出现3代表通过总共4次访问均失败，如果小于3，可忽略
日志等级	3
举例	DRVPLAT/3/DrvDebug: PCA9548 sel, write need to retry, present try times is 0,.
日志说明	提示I2C选通器件9548选通第一次访问失败，需要重试
处理建议	如果出现times ：3代表通过总共4次访问均失败，请联系技术支持 如果小于3，可忽略

26.1.23 DrvDebug

日志内容	I2c logic select is error.
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	提示通过CPLD逻辑选通I2C通道失败 注：有些元器件需要通过逻辑选通I2C通道，例如光模块
处理建议	请联系技术支持

26.1.24 DrvDebug

日志内容	The device doesn't support the subcard in subslot [UINT32].
参数解释	$1： 子卡槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: The device doesn't support the subcard in subslot 1.
日志说明	本设备不支持该槽位的子卡
处理建议	请联系技术支持

26.1.25 DrvDebug

日志内容	This device([UINT32]) does not support this kind of board([UINT32])!
参数解释	$1：设备品牌 $2：单板品牌
日志等级	2
举例	DRVPLAT/2/DrvDebug: This device(1) does not support this kind of board(2)!
日志说明	本设备不支持这种类型的单板
处理建议	请联系技术支持

26.1.26 DrvDebug

日志内容	Warning: Standby board on chassis [UINT32]slot [UINT32]is not compatible with master board, Standby board type is [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：备用主控板槽位号 $3：备用主控板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Standby board on chassis1slot 4 is not compatible with master board, Standby board type is 1.0.
日志说明	IRF模式下，备用主控板与全局主控板类型不匹配
处理建议	请联系技术支持

26.1.27 DrvDebug

日志内容	Warning: Standby board on slot [UINT32] is not compatible with master board, Standby board type is [UINT32].
参数解释	$1：备用主控板槽位号 $2：备用主控板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Standby board on slot 4 is not compatible with master board, Standby board type is 1.0.
日志说明	独立运行模式下，备用主控板和主控板的类型不匹配
处理建议	请联系技术支持

26.1.28 DrvDebug

日志内容	Warning: The LPU board on chassis [UINT32] slot [UINT32] is not compatible with MPU board, its board type is [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：业务板槽位号 $3：业务板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The LPU board on chassis 1 slot 1 is not compatible with MPU board, its board type is 3.0..
日志说明	IRF模式下，业务板和全局主控板的类型不匹配
处理建议	请联系技术支持

26.1.29 DrvDebug

日志内容	Warning: The LPU board on slot [UINT32] is not compatible with MPU board, its board type is [UINT32].
参数解释	$1：业务板槽位号 $2：业务板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: The LPU board on slot 1 is not compatible with MPU board, its board type is 3.0.
日志说明	独立运行模式下，业务板和全局主控板的类型不匹配
处理建议	请联系技术支持

26.1.30 DrvDebug

日志内容	The software version is not compatible with the hardware.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: The software version is not compatible with the hardware.
日志说明	加载的软件和硬件不匹配
处理建议	请联系技术支持

26.1.31 DrvDebug

日志内容	Board state changed to Normal on slot [UINT32], type is LSXM1CMURS2.
参数解释	$1：监控板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Board state changed to Normal on slot 1, type is LSXM1CMURS2.
日志产生原因	监控板LSXM1CMURS2状态启动正常后
处理建议	请联系技术支持

26.1.32 DrvDebug

日志内容	Board state changed to Fault on slot [UINT32].
参数解释	$1：监控板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Board state changed to Fault on slot 1.
日志说明	主控板检测监控板状态出现故障，如果两分钟后仍未恢复正常，会重启此监控板
处理建议	请联系技术支持

26.1.33 DrvDebug

日志内容	Warning: The Standby board on chassis [UINT32] slot [UINT32] is not compatible with MPU board[UINT32], its board type is [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：备用主控板槽位号 $3：主用主控板的OEM类型 $4：备用主控板的板类型+OEM类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The Standby board on chassis 1 slot 4 is not compatible with master board(0,0), its board type is 1.0.0
日志说明	IRF模式下，备用主控板与主用主控板的板类型不匹配
处理建议	请联系技术支持

26.1.34 DrvDebug

日志内容	Warning: The Standby board on slot [UINT32] is not compatible with MPU board[UINT32], its board type is [UINT32].
参数解释	$1：备用主控板槽位号 $2：主控板的oem类型 $3：备用主控板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The Standby board on slot 4 is not compatible with master board(0,0), its board type is 1.0.0
日志说明	独立运行模式下，备用主控板与主用主控板类型不匹配
处理建议	请联系技术支持

26.1.35 DrvDebug

日志内容	Board state changed to Fault on chassis [UINT32] slot [UINT32], type is unknown.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board state changed to Fault on chassis 1 slot 3, type is unknown.
日志说明	IRF模式下，单板插入时出现此日志属于正常，运行正常的单板检测到故障会打印此信息
处理建议	请联系技术支持

26.1.36 DrvDebug

日志内容	The current software version of CMU [UINT32] is incompatible with MPU. The system will upgrade the software version.
参数解释	$1：监控板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The current software version of CMU 0 is incompatible with MPU. The system will upgrade the software version.
日志说明	监控板当前版本和主控板不兼容 系统会升级当前监控板软件版本
处理建议	请联系技术支持

26.1.37 DrvDebug

日志内容	The software upgrade process of CMU [UINT32] is timed out, reboot it.
参数解释	$1：监控板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The software upgrade process of CMU 0 is timed out, reboot it.
日志说明	监控板软件升级过程超时，系统会重启监控板
处理建议	请联系技术支持

26.1.38 DrvDebug

日志内容	The software upgrade process of CMU [UINT32] is timed out.
参数解释	$1：监控板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The software upgrade process of CMU 0 is timed out.
日志说明	监控板软件升级过程超时
处理建议	请联系技术支持

26.1.39 DrvDebug

日志内容	The software upgrade process of CMU [UINT32] is completed, took [UINT32] seconds.
参数解释	$1：监控板所在的槽位号 $2：软件版本升级时间
日志等级	4
举例	DRVPLAT/4/DrvDebug: The software upgrade process of CMU 0 is completed, took 200 seconds.
日志说明	监控板软件升级过程完成并显示软件版本升级使用的时间
处理建议	请联系技术支持

26.1.40 DrvDebug

日志内容	The software upgrade process of CMU [UINT32] is continued.
参数解释	$1：监控板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The software upgrade process of CMU 0 is continued.
日志说明	监控板软件版本仍在升级，系统会重启监控板
处理建议	请联系技术支持

26.1.41 DrvDebug

日志内容	The card in [UINT32] failed to start up. Reason: Insufficient resources for chip number.
参数解释	$1：（设备在IRF中的成员编号+单板所在槽位号）/单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The card in slot 0 failed to start up. Reason: Insufficient resources for chip number.
日志说明	单板启动失败，原因是芯片内部的端口资源不够
处理建议	请联系技术支持

26.1.42 DrvDebug

日志内容	The switching fabric module in [UINT32] failed to start because the device does not support mixed installation of another boards.
参数解释	$1：（设备在IRF中的成员编号+单板所在槽位号）/单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The switching fabric module in slot 11 failed to start because the device does not support mixed installation of another boards.
日志说明	插入的业务板与当前的交换网板不匹配，请更换业务板或交换网板
处理建议	无

26.1.43 DrvDebug

日志内容	Failed to start the service module in slot [UINT32] on chassis [UINT32]. Reason: the maximum number of ECMP routes set on the switch exceeds the upper limit on the service module.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to start the service module in slot 5 on chassis 1. Reason: the maximum number of ECMP routes set on the switch exceeds the upper limit on the service module.
日志说明	IRF模式下，最大等价路由条数配置过大时，限制LSCM1GT48SC0单板启动，请重新配置最大等价路由的条数
处理建议	无

26.1.44 DrvDebug

日志内容	Failed to start the service module in slot [UINT32]. Reason: the maximum number of ECMP routes set on the switch exceeds the upper limit on the service module.
参数解释	$1：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to start the service module in slot 5. Reason: the maximum number of ECMP routes set on the switch exceeds the upper limit on the service module.
日志说明	独立运行模式下，最大等价路由条数配置过大时，限制LSCM1GT48SC0单板启动，请重新配置最大等价路由的条数
处理建议	无

26.1.45 DrvDebug

日志内容	The card in chassis [UINT32] slot [UINT32] failed to start up. Reason: Incompatibility with the expert system working mode.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The card in chassis 1 slot 5 failed to start up. Reason: Incompatibility with the expert system working mode.
日志说明	IRF模式下，设备的工作模式为专家模式时，对于S12500G-AF系列交换机，SE系列接口板无法正常运行，对于S7500X-G系列交换机，部分早期生产的带面板口的SC系列主控板、LSCM2系列SC系列接口板、LSCM1GT48SC0单板和SE系列接口板无法正常运行
处理建议	无

26.1.46 DrvDebug

日志内容	The card in slot [UINT32] failed to start up. Reason: Incompatibility with the expert system working mode.
参数解释	$1：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The card in slot 5 failed to start up. Reason: Incompatibility with the expert system working mode.
日志说明	独立运行模式下，设备的工作模式为专家模式时，对于S12500G-AF系列交换机，SE系列接口板限制启动，对于S7500X-G系列交换机，部分早期生产的带面板口的SC系列主控板、、LSCM2系列SC系列接口板、LSCM1GT48SC0单板和SE系列接口板限制启动
处理建议	无

26.1.47 DrvDebug

日志内容	The switching fabric module in slot [UINT32]/[UINT32] failed to start because it is a different model than the existing switching fabric modules.
参数解释	$1：设备在IRF中的成员编号 $2：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1 ;The switching fabric module in slot 1/10 failed to start because it is a different model than the existing switching fabric modules.
日志说明	不同类型的网板不能混插，否则设备将无法正常启动，请更换为相同类型的网板
处理建议	无

26.1.48 DrvDebug

日志内容	The board in chassis [UINT32] slot [UINT32] is in abnormal status for a long time. It will be rebooted.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1 ; The board in chassis 1 slot 5 is in abnormal status for a long time. It will be rebooted.
日志说明	IRF模式下，单板在位，但15分钟还未启动并状态未更改为Normal
处理建议	无

26.1.49 DrvDebug

日志内容	The board in slot [UINT32] is in abnormal status for a long time. It will be rebooted.
参数解释	$1：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1 ; The board in slot 5 is in abnormal status for a long time. It will be rebooted.
日志说明	独立运行模式下，单板在位，但15分钟还未启动并状态未更改为normal
处理建议	无

26.1.50 DrvDebug

日志内容	Hardware error! FMEA Voq is error!
参数解释	无
日志等级	3
举例	DRVPLAT/3/DrvDebug: Hardware error! FMEA Voq is error!
日志说明	有端口出现VOQ故障
处理建议	请联系技术支持

26.1.51 DrvDebug

日志内容	Hardware error! FMEA cpld is error!
参数解释	无
日志等级	3
举例	DRVPLAT/3/DrvDebug: Hardware error! FMEA cpld is error!
日志说明	CPLD出现故障
处理建议	请联系技术支持

26.1.52 DrvDebug

日志内容	The switch mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port %u.
参数解释	$1：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The switch mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2.
日志说明	设备在IRF模式中，各个成员设备上的工作模式必须相同，请检查各成员设备上的工作模式
处理建议	请用display switch-mode命令检查，并通过switch-mode命令修改各个成员设备上的工作模式

26.1.53 DrvDebug

日志内容	The fabric multicast-forwarding mode conf should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port %u.
参数解释	$1：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The fabric multicast-forwarding mode conf should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2.
日志说明	设备在IRF模式中，各个成员设备的组播转发模式必须相同，请检查各成员设备上的组播转发模式
处理建议	请用display fabric multicast-forwarding mode命令检查，并通过fabric multicast-forwarding mode命令修改各个成员设备的模式

26.1.54 DrvDebug

日志内容	Board state changed to Fault on slot [UINT32], type is unknown.
参数解释	$1：单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board state changed to Fault on slot 3, type is unknown.
日志说明	单板插入时出现此日志属于正常，运行正常的单板检测到故障会打印此信息
处理建议	请联系技术支持

26.1.55 DrvDebug

日志内容	Key components on the switching fabric module in slot [UINT32] are synchronizing information. Please try again later.
参数解释	$1：网板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Key components on the switching fabric module in slot 9 are synchronizing information. Please try again later.
日志说明	网板关键器件正在同步信息，请稍后再试
处理建议	请联系技术支持。

26.1.56 DrvDebug

日志内容	Key components on the switching fabric module in chassis [UINT32] slot [UINT32] are synchronizing information. Please try again later.
参数解释	$1：设备在IRF中的成员编号 $2：网板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Key components on the switching fabric module in chassis 1 slot 9 are synchronizing information. Please try again later.
日志说明	网板关键器件正在同步信息，请稍后再试
处理建议	请联系技术支持。

26.1.57 DrvDebug

日志内容	The switching fabric module in slot [UINT32] has failed to be rebooted because its status is not normal. Please try again later.
参数解释	$1：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The switching fabric module in slot 9 has failed to be rebooted because its status is not normal. Please try again later.
日志说明	网板状态normal后才能执行重启操作，请稍后再试
处理建议	请联系技术支持。

26.1.58 DrvDebug

日志内容	The switching fabric module in chassis [UINT32] slot [UINT32] has failed to be rebooted because its status is not normal. Please try again later.
参数解释	$1：设备在IRF中的成员编号 $2：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The switching fabric module in chassis 1 slot 9 has failed to be rebooted because its status is not normal. Please try again later.
日志说明	网板状态normal后才能执行重启操作，请稍后再试
处理建议	请联系技术支持。

26.1.59 DrvDebug

日志内容	The switching fabric module in slot [UINT32] has failed to be shut down because its status is not normal. Please try again later.
参数解释	$1：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The switching fabric module in slot 9 has failed to be shut down because its status is not normal. Please try again later.
日志说明	网板状态normal后才能执行断电操作，请稍后再试
处理建议	请联系技术支持。

26.1.60 DrvDebug

日志内容	The switching fabric module in chassis [UINT32] slot [UINT32] has failed to be shut down because its status is not normal. Please try again later.
参数解释	$1：设备在IRF中的成员编号 $2：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The switching fabric module in chassis 1 slot 9 has failed to be shut down because its status is not normal. Please try again later.
日志说明	网板状态normal后才能执行断电操作，请稍后再试
处理建议	请联系技术支持。

26.1.61 DrvDebug

日志内容	形式一： Please install the fabric module in slot [UINT32] or slot [UINT32]. These slots take precedence over others for fabric module installation. 形式二： Please install the fabric module in chassis [UINT32] slot [UINT32] or slot [UINT32]. These slots take precedence over others for fabric module installation.
参数解释	形式一： $1：网板槽位号 $2：网板槽位号 形式二： $1：chassis编号 $2：网板槽位号 $3：网板槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Please install the fabric module in chassis [UINT32] slot [UINT32] or slot [UINT32]. These slots take precedence over others for fabric module installation.
日志说明	请将交换网板优先安装到指定的网板槽位号
处理建议	请联系技术支持

26.1.62 DrvDebug

日志内容	形式一： Please install the fabric module in slot [UINT32], slot [UINT32], slot [UINT32], or slot [UINT32]. These slots take precedence over others for fabric module installation. 形式二： Please install the fabric module in chassis [UINT32] slot [UINT32], slot [UINT32], slot [UINT32], or slot [UINT32]. These slots take precedence over others for fabric module installation.
参数解释	形式一： $1：网板槽位号 $2：网板槽位号 $3：网板槽位号 $4：网板槽位号 形式二： $1：chassis编号 $2：网板槽位号 $3：网板槽位号 $4：网板槽位号 $5：网板槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Please install the fabric module in chassis [UINT32] slot [UINT32], slot [UINT32], slot [UINT32], or slot [UINT32]. These slots take precedence over others for fabric module installation.
日志说明	请将交换网板优先安装到指定的网板槽位号
处理建议	请联系技术支持

26.1.63 DrvDebug

日志内容	No switching fabric module is available, causing abnormal service forwarding. The device will reboot.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: No switching fabric module is available, causing abnormal service forwarding. The device will reboot.
日志说明	由于没有可用网板，将重启整框
处理建议	先检查网板是否安装，如果有的话，请联系技术支持

26.1.64 DrvDebug

日志内容	Hardware error. A severe error has occurred on IPC chips of the card in slot [UINT32]. The card will restart.
参数解释	$1：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Hardware error. A severe error has occurred on IPC chips of the card in slot 0. The card will restart.
日志说明	IPC芯片出现严重故障，单板将重启
处理建议	请联系技术支持

26.1.65 DrvDebug

日志内容	Hardware error. A severe error has occurred on IPC chips of the card in chassis [UINT32] slot [UINT32]. The card will restart.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Hardware error. A severe error has occurred on IPC chips of the card in chassis 1 slot 0. The card will restart.
日志说明	IPC芯片出现严重故障，单板将重启
处理建议	请联系技术支持

26.1.66 DrvDebug

日志内容	The card in chassis [UINT32] slot [UINT32] failed to start up. Reason: The card can start up only in expert mode.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The card in chassis 1 slot 7 failed to start up. Reason: The card can start up only in expert mode.
日志说明	单板仅支持expert模式启动
处理建议	请联系技术支持

26.1.67 DrvDebug

日志内容	The card in slot [UINT32] failed to start up. Reason: The card can start up only in expert mode.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The card in slot 7 failed to start up. Reason: The card can start up only in expert mode.
日志说明	单板仅支持expert模式启动
处理建议	请联系技术支持

26.1.68 DrvDebug

日志内容	The switching fabric module in slot [UINT32] failed to start because it is a different model than the existing switching fabric modules.
参数解释	$1：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1 ;The switching fabric module in slot 11 failed to start because it is a different model than the existing switching fabric modules.
日志说明	不同类型的网板不能混插，否则设备将无法正常启动，请更换为相同类型的网板
处理建议	无

26.1.69 DrvDebug

日志内容	The switching fabric module in chassis [UINT32] slot [UINT32] failed to start because it is a different model than the existing switching fabric modules.
参数解释	$1：设备在IRF中的成员编号 $2：网板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1 ;The switching fabric module in chassis 1 slot 11 failed to start because it is a different model than the existing switching fabric modules.
日志说明	不同类型的网板不能混插，否则设备将无法正常启动，请更换为相同类型的网板
处理建议	无

26.1.70 DrvDebug

日志内容	Global chip IDs assigned to chips on the card in slot [UINT32] are invalid. The card is to be rebooted.
参数解释	$1：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Global chip IDs assigned to chips on the card in slot 3 are invalid. The card is to be rebooted.
日志说明	由于某单板的gchip分配有误，不是本地主控板统一分配的有效值，即将重启此单板
处理建议	请联系技术支持

26.1.71 DrvDebug

日志内容	Global chip IDs assigned to chips on the card in chassis [UINT32] slot [UINT32] are invalid. The card is to be rebooted.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Global chip IDs assigned to chips on the card in chassis 1 slot 3 are invalid. The card is to be rebooted.
日志说明	由于某单板的gchip分配有误，不是本地主控板统一分配的有效值，即将重启此单板
处理建议	请联系技术支持

26.1.72 DrvDebug

日志内容	WARNING: interface [STRING] link down
参数解释	$1: 接口号
日志等级	2
举例	DRVPLAT/2/DrvDebug: WARNING: interface GigabitEthernet 1/0/1 link down
日志说明	接口链路失效
处理建议	**1.** 检查是否是网线没插好或直接重新插拔一下网线 **2.** 更换网线来检查网线是否正常 **3.** 更换本端设备端口（如果条件允许，推荐使用其它槽位的同类型单板）来检查故障是否排除 **4.** 更换对端设备端口（如果条件允许，推荐使用其它槽位的同类型单板）来检查故障是否排除 **5.** 如上述步骤故障仍未解决，请联系技术支持

26.1.73 DrvDebug

日志内容	WARNING: Local Slot [UINT32] update port info for GOLD failed, while port monitor enable!
参数解释	$1: 单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: WARNING: Local Slot 5 update port info for GOLD failed, while port monitor enable!
日志说明	端口监控使能时更新GOLD端口信息失败
处理建议	请联系技术支持

26.1.74 DrvDebug

日志内容	Chassis [UINT32] Slot [UINT32] Unit [UINT32] Port [UINT32] error frame detected!
参数解释	$1: 设备在IRF中的成员编号 $2: 单板所在的槽位号 $3: 单板上的芯片编号 $4: 单板上的端口编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Chassis=1-Slot=5; Chassis 1 Slot 5 Unit 0 Port 1 error frame detected!
日志说明	端口检测到错误帧
处理建议	请联系技术支持

26.1.75 DrvDebug

日志内容	WARNING: Unit=[UINT32],Port=[UINT32] has FCS errors, please check.
参数解释	$1: 芯片编号 $2: 端口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: WARNING: Unit=0,Port=1 has FCS errors, please check.
日志说明	端口检测到FCS（frame check sequence,帧校验）错误
处理建议	请联系技术支持

26.1.76 DrvDebug

日志内容	WARNING: interface [STRING] has FCS errors, please check.
参数解释	$1: 接口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: interface GigabitEthernet 1/0/1 has FCS errors, please check.
日志说明	接口检测到FCS（frame check sequence,帧校验）错误
处理建议	请联系技术支持

26.1.77 DrvDebug

日志内容	WARNING: Chassis [UINT32] Slot [UINT32] Unit [UINT32] Port [UINT32] has FCS errors, please check.
参数解释	$1: 设备在IRF中的成员编号 $2: 单板所在的槽位号 $3: 单板上的芯片编号 $4: 单板上的端口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=1-Slot=5;WARNING: Chassis 1 Slot 5 Unit 0 Port 1 has FCS errors, please check.
日志说明	单板端口检测到FCS（frame check sequence,帧校验）错误
处理建议	请联系技术支持

26.1.78 DrvDebug

日志内容	WARNING: Chassis [UINT32] slot [UINT32] is isolated already. Maybe caused by the hardware failure, please remove and check it.
参数解释	$1: 设备在IRF中的成员编号 $2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=1-Slot=5;WARNING: Chassis 1 slot 5 is isolated already. Maybe caused by the hardware failure, please remove and check it.
日志说明	可能由于硬件错误导致某单板被隔离，请移除该单板并检查
处理建议	请移除该单板并联系技术支持

26.1.79 DrvDebug

日志内容	WARNING: Slot [UINT32] is isolated already. Maybe caused by the hardware failure, please remove and check it.
参数解释	$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: Slot 5 is isolated already. Maybe caused by the hardware failure, please remove and check it.
日志说明	可能由于硬件错误导致某单板被隔离，请移除该单板并检查
处理建议	请移除该单板并联系技术支持

26.1.80 DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] has a hardware error, will be rebooted. Please check it.
参数解释	$1: 设备在IRF中的成员编号 $2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis 1 slot 2 has a hardware error, will be rebooted. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动重启
处理建议	• 若自动重启后单板仍然故障，且自动重启次数达到 3 次，单板将被自动隔离， • 单板被自动隔离后，请联系技术支持

26.1.81 DrvDebug

日志内容	Slot [UINT32] has a hardware error, will be rebooted. Please check it.
参数解释	$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Slot 2 has a hardware error, will be rebooted. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动重启
处理建议	• 若自动重启后单板仍然故障，且自动重启次数达到 3 次，单板将被自动隔离， • 单板被自动隔离后，请联系技术支持

26.1.82 DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] maybe have a hardware error, will be isolated. Please check it.
参数解释	$1: 设备在IRF中的成员编号 $2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis 1 slot 2 maybe have a hardware error, will be isolated. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动隔离
处理建议	请移除该单板并联系技术支持

26.1.83 DrvDebug

日志内容	Slot [UINT32] maybe have a hardware error, will be isolated. Please check it.
参数解释	$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Slot 2 maybe have a hardware error, will be isolated. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动隔离
处理建议	请移除该单板并联系技术支持

26.1.84 DrvDebug

日志内容	Priority alarm, current priority of reference [UINT32] [STRING] is [UINT32].
参数解释	$1：设备时钟源编号 $2：设备在IRF中的成员编号 $3：当前时钟源优先级
日志等级	4
举例	DRVPLAT/4/DrvDebug: Priority alarm, current priority of reference 2 of chassis 1 is 3.
日志说明	配置设备时钟源的优先级成功后产生的提示信息
处理建议	请联系技术支持

26.1.85 DrvDebug

日志内容	Priority alarm, current priority of PTP [STRING] is [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：当前PTP协议时钟源的优先级
日志等级	4
举例	DRVPLAT/4/DrvDebug: Priority alarm, current priority of PTP of chassis 1 is 3.
日志说明	配置设备PTP协议时钟源的优先级成功后产生的提示信息
处理建议	请联系技术支持

26.1.86 DrvDebug

日志内容	SSM level alarm, current SSM level of reference [UINT32] [STRING] is [STRING].
参数解释	$1：设备时钟源编号 $2：设备在IRF中的成员编号 $3：当前时钟源的SSM级别
日志等级	4
举例	DRVPLAT/4/DrvDebug: SSM level alarm, current SSM level of reference 2 of chassis 1 is SSUA.
日志说明	配置设备时钟源的SSM级别成功后产生的提示信息
处理建议	请联系技术支持

26.1.87 DrvDebug

日志内容	SSM level alarm, current SSM level of PTP [STRING] is [STRING].
参数解释	$1：设备在IRF中的成员编号 $2：当前时钟源的SSM级别
日志等级	4
举例	DRVPLAT/4/DrvDebug: SSM level alarm, current SSM level of PTP of chassis 1 is SSUA.
日志说明	配置设备时钟源的SSM级别成功后产生的提示信息
处理建议	请联系技术支持

26.1.88 DrvDebug

日志内容	Phase lock alarm, current phase lock mode [STRING] is [STRING].
参数解释	$1：设备在IRF中的成员编号 $2：当前时钟监控的锁相状态
日志等级	4
举例	DRVPLAT/4/DrvDebug: Phase lock alarm, current phase lock mode of chassis 1 is Holdover.
日志说明	当前时钟监控的锁相状态变更时出现
处理建议	请联系技术支持

26.1.89 DrvDebug

日志内容	SSM out level alarm, current SSM out level [STRING] is [STRING].
参数解释	$1：设备在IRF中的成员编号 $2：当前时钟源输出SSM级别
日志等级	4
举例	DRVPLAT/4/DrvDebug: SSM out level alarm, current SSM out level of chassis 1 is SSUA.
日志说明	当前设备上时钟源的SSM级别发生变化时出现
处理建议	请联系技术支持

26.1.90 DrvDebug

日志内容	Traced reference change alarm, current traced reference [STRING] is PTP.
参数解释	$1：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Traced reference change alarm, current traced reference of chassis 1 is PTP.
日志说明	当配置时钟监控的时钟源为PTP同步时钟时出现
处理建议	请联系技术支持

26.1.91 DrvDebug

日志内容	BFD multi-hop not support Vpn. LD[UINT]
参数解释	$1： 本端BFD鉴别值
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;BFD multi-hop not support Vpn. LD[4600].
日志说明	本设备BFD逐跳会话不支持VPN
处理建议	请删除VPN内BFD逐跳会话相关配置

26.1.92 DrvDebug

日志内容	No enough acl resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; No enough acl resources.
日志说明	使能DHCP Snooping时下发规则发现无资源
处理建议	请联系技术支持

26.1.93 DrvDebug

日志内容	Insufficient ACL resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=2; Insufficient ACL resources.
日志说明	开启DHCP Flood攻击防范功能后，若设备硬件资源不足，无法创建check状态的DHCP防Flood攻击表项，无法防范指定MAC地址的攻击
处理建议	如果设备业务占用硬件资源过多，可能会导致资源不足，需要释放一些资源，重新配置DHCP Flood攻击防范功能

26.1.94 DrvDebug

日志内容	The product can't support vrrp load-balance mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; The product can't support vrrp load-balance mode.
日志说明	不支持VRRPE模式
处理建议	不要配置VRRP负载分担模式

26.1.95 DrvDebug

日志内容	-Chassis=[INT32]-Slot=[INT32]; Tunnel[INT32] might not function properly on this device
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：Tunnel接口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=3; Tunnel1 might not function properly on this device
日志说明	创建的Tunnel接口数量超过规格数量时打印该日志
处理建议	**1.** 关闭其它多余的状态正常的 Tunnel 接口 **2.** 请联系技术支持

26.1.96 DrvDebug

日志内容	-Chassis=[INT32]-Slot=[INT32]; Tunne[INT32] recovered on this device
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：Tunnel接口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; Tunnel1 recovered on this device
日志说明	Tunnel接口恢复正常
处理建议	无

26.1.97 DrvDebug

日志内容	Failed to collect tunnel incoming traffic statistics because of insufficient ACL resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to collect tunnel incoming traffic statistics because of insufficient ACL resources.
日志说明	当前VXLAN隧道入方向流量统计失败，因为当前配置隧道统计功能所需要的设备QoS-ACL入方向资源不足
处理建议	• 删除当前没有使用但占用 QoS-ACL 入方向资源的配置 • 请联系技术支持

26.1.98 DrvDebug

日志内容	Failed to collect tunnel outgoing traffic statistics because of insufficient ACL resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to collect tunnel outgoing traffic statistics because of insufficient ACL resources.
日志说明	当前VXLAN隧道出方向流量统计失败，因为当前配置隧道统计功能所需要的设备QoS-ACL出方向资源不足
处理建议	• 删除当前没有使用但占用 QoS-ACL 出方向资源的配置 • 请联系技术支持

26.1.99 DrvDebug

日志内容	Failed to collect VSI incoming traffic statistics because of insufficient ACL resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to collect VSI incoming traffic statistics because of insufficient ACL resources.
日志说明	当前VXLAN VSI入方向流量统计失败，因为当前配置vsi统计功能所需要的设备QoS-ACL入方向资源不足
处理建议	• 删除当前没有使用但占用 QoS-ACL 入方向资源的配置 • 请联系技术支持

26.1.100 DrvDebug

日志内容	Failed to collect VSI outgoing traffic statistics because of insufficient ACL resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to collect VSI outgoing traffic statistics because of insufficient ACL resources.
日志说明	当前VXLAN VSI出方向流量统计失败，因为当前配置vsi统计功能所需要的设备QoS-ACL出方向资源不足
处理建议	• 删除当前没有使用但占用 QoS-ACL 出方向资源的配置 • 请联系技术支持

26.1.101 DrvDebug

日志内容	No enough acl resourcess.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: No enough acl resources.
日志说明	配置设备从VXLAN隧道收到指定协议类型的报文直接转发，不上送CPU功能失效。因为当前该功能所需要的QoS-ACL资源不足
处理建议	请联系技术支持

26.1.102 DrvDebug

日志内容	No enough acl resourcess.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: No enough acl resources.
日志说明	配置丢弃未知组播数据报文功能失效。因为当前配置功能所需要的设备QoS-ACL资源不足
处理建议	**1.** 请联系技术支持

26.1.103 DrvDebug

日志内容	Ringlet [STRING] [STRING] class congestion alarm is present.
参数解释	$1:环号（0环：内环；1环：外环） $2: A/B/C类业务报文
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=1; Ringlet 0 C class congestion alarm is present.
日志说明	指定子环上，数据流量过大，出现业务报文拥塞告警
处理建议	• 使用流量控制等功能减少对应类型的业务流量 • 请联系技术支持

26.1.104 DrvDebug

日志内容	Ringlet [STRING] [STRING] class congestion alarm.
参数解释	$1: 环号（0环：内环；1环：外环） $2: A/B/C类业务报文
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=1; Ringlet 0 A class congestion alarm is present.
日志说明	指定子环上，业务报文拥塞告警状态一直存在，10秒打印一次
处理建议	• 使用流量控制等功能减少对应类型的业务流量 • 请联系技术支持

26.1.105 DrvDebug

日志内容	Ringlet [STRING] [STRING] class congestion alarm is over.
参数解释	$1: 环号（0环：内环；1环：外环） $2: A/B/C类业务报文
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=1; Ringlet 0 C class congestion alarm is over
日志说明	指定子环上，业务报文拥塞告警消除时产生
处理建议	无

26.1.106 DrvDebug

日志内容	Tunnel load-sharing might not function properly.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; Tunnel load-sharing might not function properly
日志说明	不支持tunnel负载分担
处理建议	无

26.1.107 DrvDebug

日志内容	The currently configured arp rate limit exceeds the maximum arp rate limit that can be configured on this board.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; The currently configured arp rate limit exceeds the maximum arp rate limit that can be configured on this board.
日志说明	配置的ARP速率超过了可配置的最大速率限制
处理建议	降低ARP配置速率

26.1.108 DrvDebug

日志内容	Not enough resources for ARP packet rate limit.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; Not enough resources for ARP packet rate limit.
日志说明	资源不足导致配置ARP速率失效
处理建议	无

26.1.109 DrvDebug

日志内容	Tunnel operation can not be supported, [STRING].
参数解释	$1：创建隧道
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; Tunnel operation can not be supported, Tunnel1.
日志说明	不支持创建隧道操作
处理建议	无

26.1.110 DrvDebug

日志内容	[STRING] might not function properly on this device.
参数解释	$1：创建隧道
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=6; Tunnel1: might not function properly on this device
日志说明	在框式设备上创建隧道提示不支持
处理建议	无

26.1.111 DrvDebug

日志内容	Tunnel type is not support, [STRING].
参数解释	$1：创建隧道
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; Tunnel type is not support, Tunnel1.
日志说明	创建了不支持的隧道类型
处理建议	无

26.1.112 DrvDebug

日志内容	BFD detect-interface not support on this board.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; BFD detect-interface not support on this board.
日志说明	此单板上不支持配置检测接口状态的BFD会话
处理建议	无

26.1.113 DrvDebug

日志内容	[STRING]: might not function properly on this device.
参数解释	$1：创建路由口/路由子子接口
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=6; Ten-GigabitEthernet1/6/0/4.2: might not function properly on this device
日志说明	在框式设备上创建路由口/路由子接口提示不支持
处理建议	无

26.1.114 DrvDebug

日志内容	MAC address configuration is not supported.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=6; MAC address configuration is not supported.
日志说明	不支持配置接口MAC地址
处理建议	无

26.1.115 DrvDebug

日志内容	Operation failed because of insufficient resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=6; Operation failed because of insufficient resources.
日志说明	资源不足导致接口MAC地址配置失败
处理建议	无

26.1.116 DrvDebug

日志内容	Insufficient resources on the card.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug:Insufficient resources on the card.
日志说明	配置VRRP，单板3个高位地址均被使用后提示单板资源不足
处理建议	请联系技术支持

日志内容	The virtual router ID is greater than 15. The card does not support VRRP load balancing mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug:The virtual router ID is greater than 15. The card does not support VRRP load balancing mode.
日志说明	配置VRRP，单板判断vrid的高4位是否为全0，不是则说明vrid>15，单板不支持VRRP负载均衡模式
处理建议	请联系技术支持

26.1.117 DrvDebug

日志内容	The temperature of [STRING] exceeded [UINT32] Centigrade. Power supply stopped.
参数解释	$1：设备接口名称 $2：设备端口温度的最高限值
日志等级	4
举例	DRVPLAT/4/DrvDebug:The temperature of Twenty-FiveGigE exceeded 80 Centigrade. Power supply stopped.
日志说明	POE单板端口温度高于门限值，供电停止
处理建议	请联系技术支持

26.1.118 DrvDebug

日志内容	The temperature of [STRING] dropped to [UINT32] Centigrade. Power supply stopped.
参数解释	$1：设备接口名称 $2：设备端口温度的最低限值
日志等级	4
举例	DRVPLAT/4/DrvDebug:The temperature of Twenty-FiveGigE dropped to 10 Centigrade. Power supply stopped.
日志说明	POE单板端口温度低于门限值，供电停止
处理建议	请联系技术支持

26.1.119 DrvDebug

日志内容	The temperature of [STRING] dropped to [UINT32] Centigrade. Power supply recovered.
参数解释	$1：设备接口名称 $2：设备端口温度的最高限值
日志等级	4
举例	DRVPLAT/4/DrvDebug:The temperature of Twenty-FiveGigE dropped to 80 Centigrade. Power supply recovered.
日志说明	POE单板端口温度降低到高限值以下，供电恢复
处理建议	请联系技术支持

26.1.120 DrvDebug

日志内容	The temperature of [STRING] exceeded [UINT32] Centigrade. Power supply recovered.
参数解释	$1：设备接口名称 $2：设备端口温度的最低限值
日志等级	4
举例	DRVPLAT/4/DrvDebug:The temperature of Twenty-FiveGigE exceeded 10 Centigrade. Power supply recovered.
日志说明	POE单板端口温度升高至低限值以上，供电恢复
处理建议	请联系技术支持

26.1.121 DrvDebug

日志内容	WARNING: One 180W power module and one power module of higher capacity present. The total output capacity is twice that of the 180W power module.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug:WARNING: One 180W power module and one power module of higher capacity present. The total output capacity is twice that of the 180W power module.
日志说明	当设备上安装一个180W和一个更高功率的电源时，此时两块电源会总共提供360W的输出功率
处理建议	请联系技术支持

26.1.122 DrvDebug

日志内容	The link status of port [STRING] is abnormal and the port is shutdown.
参数解释	$1：本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: The link status of port Ten-GigabitEthernet1/1/4 is abnormal and the port is shutdown.
日志说明	链路异常，硬件检测到端口频繁UP/DOWN，将端口关闭
处理建议	• 检查对端设备是否发生故障。如是请解决对端设备故障问题，如否，请执行下一步 • 检查链路两端介质是否故障。如是请更换介质，如否，请联系技术支持 • 排查故障后，请对端口执行 shutdown/undo shutdown 操作

26.1.123 DrvDebug

日志内容	The port up-mode configuration exists on port [STRING]. Please remove the configuration, and then install the GE transceiver module.
参数解释	$1：本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port up-mode configuration exists on port Ten-GigabitEthernet1/1/4. Please remove the configuration, and then install the GE transceiver module.
日志说明	10G端口若有port up-mode的配置，请取消之后，再插入GE光模块
处理建议	• 检查当前端口是否存在 port up-mode 的配置；如是，请执行下一步 • 拔掉当前端口插入的 GE 光模块，然后在当前端口执行 undo port up-mode 的操作 • 再在该端口上插 GE 光模块

26.1.124 DrvDebug

日志内容	Fan Fault! Chassis [UINT32] Frame [UINT32] fan [UINT32] speed < 500(R.P.M). FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	$1：设备在IRF中的成员编号 $2：风扇框所在槽位号 $3：风扇编号 $4：风扇的状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Fault! Chassis 1 Frame 0 fan 1 speed < 500(R.P.M). FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	IRF模式下，风扇发生故障，风扇速度小于500转/每分钟
处理建议	使用**display fan**检查风扇状态 ◦ 若风扇状态为 fault，请重新拔插风扇框，如果还不能恢复，请联系技术支持 ◦ 若风扇状态为 normal，请联系技术支持

26.1.125 DrvDebug

日志内容	Fan Fault! Frame [UINT32] fan [UINT32] speed < 500(R.P.M). FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	$1：风扇框所在槽位号 $2：风扇编号 $3：风扇的状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Fault! Frame 0 fan 1 speed < 500(R.P.M). FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	独立运行模式下，风扇发生故障，风扇速度小于500转/每分钟
处理建议	使用**display fan**检查风扇状态 • 若风扇状态为 fault，请重新拔插风扇框，如果还不能恢复，请联系技术支持 • 若风扇状态为 normal，请联系技术支持

26.1.126 DrvDebug

日志内容	Fan Adjusting failed! Chassis [UINT32] Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too low! FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	$1：设备在IRF中的成员编号 $2：风扇框所在槽位号 $3：风扇编号 $4：风扇转速 $5：风扇状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Chassis 1 Frame 0 fan 1 speed is 1124(R.P.M), is too low! FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	风扇当前的转速比实际设置的风扇模式下的最小转速低

处理建议	• 当使用 **debug sysm fan** 命令，将风扇模式配置为 hign 时，提示一次，属于正常现象，无需处理
	• 其他情况，请使用 **display fan** 检查风扇状态：
	  ○ 若风扇状态为 fault，请尝试拔插风扇框
	  ○ 若风扇状态为 normal，请过 2 分钟再看日志是否一直存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持

26.1.127 DrvDebug

日志内容	Fan Adjusting failed! Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too low! FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	$1：风扇框所在槽位号 $2：风扇编号 $3：风扇转速 $4：风扇状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Frame 0 fan 1 speed is 1124(R.P.M), is too low! FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	风扇当前的转速比实际设置的风扇模式下的最小转速低

处理建议	• 当使用 **debug sysm fan** 命令，将风扇模式配置为 hign 时，提示一次，属于正常现象，无需处理
	• 其他情况，请使用 **display fan** 检查风扇状态：
	  ○ 若风扇状态为 fault，请尝试拔插风扇框
	  ○ 若风扇状态为 normal，请过 2 分钟再看日志是否一直存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持

26.1.128 DrvDebug

日志内容	Fan Adjusting failed! Chassis [UINT32] Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too high!
参数解释	$1：设备在IRF中的成员编号 $2：风扇框所在槽位号 $3：风扇编号 $4：风扇转速
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Chassis 1 Frame 0 fan 1 speed is 3524(R.P.M), is too high!
日志说明	风扇当前的转速比实际设置的风扇模式下的最大转速高

处理建议	• 当使用 **debug sysm fan *[fan-id] [section-id]***命令，将风扇模式配置为 low 或 auto 时，提示一次，属于正常现象，无需处理
	• 其他情况，请使用 **display fan** 检查风扇状态：
	  ○ 若风扇状态为 fault，请尝试拔插风扇框
	  ○ 若风扇状态为 normal，请过 2 分钟再看日志是否一直存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持

26.1.129 DrvDebug

日志内容	Fan Adjusting failed! Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too high!
参数解释	$1：风扇框所在槽位号 $2：风扇编号 $3：风扇转速
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Frame 0 fan 1 speed is 3524(R.P.M), is too high!
日志说明	风扇当前的转速比实际设置的风扇模式下的最大转速高

处理建议	• 当使用 **debug sysm fan *[fan-id] [section-id]***命令，将风扇模式配置为 low 或 auto 时，提示一次，属于正常现象，无需处理
	• 其他情况，请使用 **display fan** 检查风扇状态：
	  ○ 若风扇状态为 fault，请尝试拔插风扇框
	  ○ 若风扇状态为 normal，请过 2 分钟再看日志是否一直存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持

26.1.130 DrvDebug

日志内容	Fan Changed OK! Frame [UINT32] fan [UINT32] speed is [UINT32](R.P.M), is OK!
参数解释	$1：风扇框所在槽位号 $2：风扇编号 $3：风扇转速
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Changed OK! Frame 1 fan 1 speed is 2000(R.P.M), is OK!
日志说明	风扇当前的转速正常
处理建议	无需处理

26.1.131 DrvDebug

日志内容	Power [UINT32] is removed.
参数解释	$1：电源编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Power 2 is removed.
日志说明	电源被拔出
处理建议	无需处理

26.1.132 DrvDebug

日志内容	Warning: Not enough power to power on board chassis [UINT32] slot [UINT32]. Board power is [UINT32]w, system available power is [UINT32]w.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：单板正常运行所需功率 $4：系统可用功率
日志等级	2
举例	DRVPLAT/2/DrvDebug: Chassis=1-Slot=5;Warning: Not enough power to power on board chassis 1 slot 5. Board power is 225w, system available power is 130w.
日志说明	系统可用功率不足导致没有足够的功率给单板上电
处理建议	使用**display power**检查系统电源模块状态是否有模块状态为fault • 如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及先电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持 • 如无，请增加系统电源模块

26.1.133 DrvDebug

日志内容	Warning: Not enough power to power on board slot [UINT32]. Board power is [UINT32]w, system available power is [UINT32]w.
参数解释	$1：单板所在的槽位号 $2：单板正常运行所需功率 $3：系统可用功率（取值为0）
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power to power on board slot 5. Board power is 225w, system available power is 130w.
日志说明	系统可用功率不足导致没有足够的功率给单板上电
处理建议	使用**display power**检查系统电源模块状态是否有模块状态为fault • 如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及先电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持 • 如无，请增加系统电源模块

26.1.134 DrvDebug

日志内容	Warning: Not enough power on chassis [UINT32], system available power is [UINT32]w.
参数解释	$1：设备在IRF中的成员编号 $2：系统可用功率（取值为0）
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power on chassis 1, system available power is 0w.
日志说明	当系统可用功率为0时，每3分钟打印一次
处理建议	使用**display power**检查系统电源模块状态是否有模块状态为fault • 如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及先电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持 • 如无，请增加系统电源模块

26.1.135 DrvDebug

日志内容	Warning: Not enough power on the device, system available power is [UINT32]w.
参数解释	$1：系统可用功率
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power on the device, system available power is 0w.
日志说明	当系统可用功率为0时，每3分钟打印一次
处理建议	使用**display power**检查系统电源模块状态是否有模块状态为fault • 如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及先电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持 • 如无，请增加系统电源模块

26.1.136 DrvDebug

日志内容	Warning: Power [UINT32] differs from power [UINT32] in types! Power [UINT32] : [STRING]. Power [UINT32] : [STRING].
参数解释	$1、$2、$3、$5：电源编号 $4、$6：电源类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Power 1 differs from power 2 in types! Power 1 : PSR1400-D. Power 2 : PSR1400-12D1.
日志说明	当电源类型不一致时打印此日志
处理建议	观察打印的2个电源的类型是否一致， • 如果不一致，请更换电源类型 • 如果一致，请联系技术支持

26.1.137 DrvDebug

日志内容	Only one power module is installed in power frame [UINT32] Power [UINT32]-[UCHAR] : [STRING]
参数解释	$1、$2：电源的编号 $3：子电源在电源框内的编号 $4：电源的类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Only one power module is installed in power frame 1.
日志说明	电源框内只有一个电源正常工作
处理建议	及时插入子电源

26.1.138 DrvDebug

日志内容	Warning: Only one power [UINT32] exist ! Power [UINT32] : [STRING]
参数解释	$1、$2：电源的编号 $3：电源的类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning:Only one power 1 exist ! Power 1: PSR1400-D.
日志说明	设备只有一个电源在位
处理建议	及时插入电源

26.1.139 DrvDebug

日志内容	Hotspot [UINT32] in chassis [UINT32] slot [UINT32] read [UINT32]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	$1： 热点传感器编号 $2：设备在IRF中的成员编号 $3：单板所在的槽位号 $4：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in chassis 1 slot 1 read 111. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	IRF模式下，单板热点温度超过温度传感器的温度门限
处理建议	请查看风扇运行是否正常

26.1.140 DrvDebug

日志内容	Hotspot [UINT32] in slot [UINT32] read [UINT32]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	$1： 热点传感器编号 $2：单板所在的槽位号 $3：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in slot 1 read 111. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	独立运行模式下，单板热点温度超过温度传感器的温度门限
处理建议	请查看风扇运行是否正常

26.1.141 DrvDebug

日志内容	temp is high in power [UINT32]
参数解释	$1：电源的编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: temp is high in power 1
日志说明	电源内部温度过高
处理建议	及时检查电源，避免出现电源损坏

26.1.142 DrvDebug

日志内容	fan is faulty in power [UINT32]
参数解释	$1：电源的编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: fan is faulty in power 1.
日志说明	电源内部风扇坏掉
处理建议	及时检查电源，避免电源出现损坏

26.1.143 DrvDebug

日志内容	Chassis [UINT32]: The number of redundant PSU changed: insufficient.
参数解释	$1：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Waring: The number of redundant PSU changed: insufficient.
日志说明	设备的冗余功率减少
处理建议	及时插入电源，避免出现功率不足

26.1.144 DrvDebug

日志内容	The number of redundant PSU changed: insufficient.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: Waring: The number of redundant PSU changed: insufficient.
日志说明	设备的冗余功率减少
处理建议	及时插入电源，避免出现功率不足

26.1.145 DrvDebug

日志内容	Chassis [UINT32]: The number of redundant PSU changed: sufficient.
参数解释	$1：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Chassis 1: The number of redundant PSU changed: sufficient.
日志说明	设备的冗余功率恢复
处理建议	无需处理

26.1.146 DrvDebug

日志内容	The number of redundant PSU changed: sufficient.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The number of redundant PSU changed: sufficient.
日志说明	设备的冗余功率恢复
处理建议	无需处理

26.1.147 DrvDebug

日志内容	The power modules in power frame [UINT32] are of different models. Power[UINT32]-[UCHAR]: [STRING]. Power[UINT32]-[UCHAR]: [STRING].
参数解释	$1 、 $2、$5：电源框框号 $3 、$6：子电源的编号 $4 、$7：子电源的型号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The power modules in power frame 1 are of different models. Power1-A: PSR1200-D. Power1-B: PSR1200-A.
日志说明	电源框内出现混插
处理建议	及时更换子电源避免出现混插导致系统不稳定

26.1.148 DrvDebug

日志内容	The fan airflow directions of two power supplies in slot [INT32] are different.
参数解释	$1：设备槽位号
日志等级	2
举例	%Jan 4 00:08:45:644 2011 H3C DRVPLAT/2/DrvDebug: The fan airflow directions of two power supplies in slot 1 are different.
日志说明	两个电源的风扇风向不同，请检查
处理建议	检查电源的风扇风向是否相同

26.1.149 DrvDebug

日志内容	The power switches are not all turned on. Please turn on power switch [UINT16].
参数解释	$1：电源开关号
日志等级	5
举例	DRVPLAT/4/DrvDebug: The power switches are not all turned on. Please turn on power switch 1.
日志说明	设备电源开关未全部打开，请打开全部电源开关
处理建议	需要保证设备两个电源开关全部打开

26.1.150 DrvDebug

日志内容	Both the power switches are turned on.
参数解释	无
日志等级	5
举例	DRVPLAT/4/DrvDebug: Both the power switches are turned on.
日志说明	两个电源开关已全部打开
处理建议	无

26.1.151 DrvDebug

日志内容	Warning: Power [INT32] is not supported ! Power [INT32] : [string].
参数解释	$1：电源槽位号 $2：电源槽位号 $3：电源模块型号
日志等级	2
举例	Warning: Power 1 is not supported ! Power 1 : PSR250-12A.
日志说明	设备插入了不支持的电源模块，请检查。
处理建议	将告警电源槽位中的电源模块更换为设备支持的型号。

26.1.152 DrvDebug

日志内容	Warning: Power off all lpu boards, please check it right now.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Warning: Power off all lpu boards, please check it right now.
日志说明	由于风扇停转，所有单板都需要下电，请立即检查
处理建议	检查电源状态

26.1.153 DrvDebug

日志内容	Fan frame [UINT32] is abnormal. Please check it right now.
参数解释	$1：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Fan frame 2 is abnormal. Please check it right now.
日志说明	风扇框异常，请立即检查
处理建议	检查风扇框状态

26.1.154 DrvDebug

日志内容	At least one fabric module slot is empty.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: At least one fabric module slot is empty.
日志说明	至少有一个交换网板的槽位是空的
处理建议	请联系技术支持

26.1.155 DrvDebug

日志内容	Warning:Fans stop running in chassis [UINT32], please check it right now.
参数解释	$1：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning:Fans stop running in chassis 1, please check it right now.
日志说明	风扇框在设备上停止运行
处理建议	检查风扇框是否正常

26.1.156 DrvDebug

日志内容	Warning:Fans stop running, please check it right now,
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning:Fans stop running, please check it right now,
日志说明	风扇框在设备上停止运行
处理建议	检查风扇框是否正常

26.1.157 DrvDebug

日志内容	A fan tray was inserted into [UINT32] on chassis [UINT32].
参数解释	$1：风扇槽位号 $2：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: A fan tray was inserted into 1 on chassis 1.
日志说明	风扇框已经插入设备风扇槽位
处理建议	请联系技术支持

26.1.158 DrvDebug

日志内容	A fan tray was inserted into [UINT32].
参数解释	$1：风扇槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: A fan tray was inserted into 1.
日志说明	风扇框已经插入设备风扇槽位
处理建议	请联系技术支持

26.1.159 DrvDebug

日志内容	The fan tray in [UINT32] on chassis [UINT32] was removed.
参数解释	$1：风扇槽位号 $2：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: The fan tray in 1 on chassis 2 was removed.
日志说明	指定设备中的风扇框已经移除
处理建议	请联系技术支持

26.1.160 DrvDebug

日志内容	The fan tray in [UINT32] was removed.
参数解释	$1：风扇槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: The fan tray in 1 was removed.
日志说明	设备中的风扇框已经移除
处理建议	请联系技术支持

26.1.161 DrvDebug

日志内容	Warning: Not enough power to power on board chassis [UINT32] slot [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：单板槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power to power on board chassis 1 slot 3.
日志说明	警告：电源功率不足，无法为指定设备的单板供电
处理建议	检查电源状态

26.1.162 DrvDebug

日志内容	Only one power module is installed in power frame [UINT32]
参数解释	$1：电源槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Only one power module is installed in power frame 1
日志说明	只有一个电源模块安装在电源框中
处理建议	请联系技术支持

26.1.163 DrvDebug

日志内容	A [STRING] module was inserted into [UINT32] on chassis [UINT32].
参数解释	$1：模块名 $2：设备槽位号 $3：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: A power module was inserted into 2 on chassis 1.
日志说明	模块已经插上指定设备的某个槽位上
处理建议	请联系技术支持

26.1.164 DrvDebug

日志内容	A [STRING] module was inserted into [UINT32].
参数解释	$1：模块名 $2：设备槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: A fan module was inserted into 1.
日志说明	模块已经插到框的指定槽位上
处理建议	请联系技术支持

26.1.165 DrvDebug

日志内容	The [STRING] module in %u on chassis [UINT32] was removed.
参数解释	$1：模块名 $2：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: The power module in %u on chassis 1 was removed.
日志说明	指定成员设备上的模块已经被移除
处理建议	请联系技术支持

26.1.166 DrvDebug

日志内容	The [STRING] module in [UINT32] was removed.
参数解释	$1：模块名 $2：设备槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: The power module in 1 was removed.
日志说明	模块已经在指定槽位上被移除
处理建议	请联系技术支持

26.1.167 DrvDebug

日志内容	WARNING: This command need reboot device.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: This command need reboot device.
日志说明	因配置Cut Through功能，需要重启设备才能使之生效
处理建议	重启设备

26.1.168 DrvDebug

日志内容	WARNING: Current switch-mode is different with that being configured System, reboot board [INT] to update switch-mode.
参数解释	$1: 槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: WARNING: Current switch-mode is different with that being configured System, reboot board 5 to update switch-mode.
日志说明	检测到Switch-Mode错误，全局主配置与本地配置不一致，需要重启对应单板已保持一致
处理建议	请联系技术支持

26.1.169 DrvDebug

日志内容	Insufficient ACL resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Insufficient ACL resources.
日志说明	当前配置下发失败，因为当前配置接口的ESI功能所需要的设备QoS-ACL资源不足
处理建议	• 删除当前没有使用但占用 QoS-ACL 资源的配置 • 请联系技术支持

26.1.170 DrvDebug

日志内容	The (undo) cut-through enable command requires a reboot to take effect.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: The (undo) cut-through enable command requires a reboot to take effect
日志说明	提示配置cut-through enable命令需要重启设备后生效
处理建议	根据提示进行操作，若有问题，请联系技术支持

26.1.171 DrvDebug

日志内容	Please Set Buffer Thrd Without Burst-mode Enable. Port is [[UINT]].
参数解释	$1：接口的逻辑端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Please Set Buffer Thrd Without Burst-mode Enable. Port is 19.
日志说明	在系统视图或以太网接口视图下配置buffer queue shared命令时，配置不允许下发，因为当前已配置burst-mode enable命令，两个功能互斥。并打印涉及的端口号
处理建议	• 检查配置中是否存在 burst-mode enable 命令，若此时需要在系统视图或以太网接口视图下配置 buffer queue shared 命令，需要先保证 burst-mode enable 命令未使能 • 请联系技术支持

26.1.172 DrvDebug

日志内容	Burst-mode Conflict With Buffer Thrd. Port is [[UINT]].
参数解释	$1：接口的逻辑端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Burst-mode Conflict With Buffer Thrd. Port is 19.
日志说明	配置burst-mode enable命令时，配置不允许下发，因为已经在系统视图或以太网接口视图下配置了buffer queue shared命令，两个功能互斥。并打印涉及的端口号
处理建议	• 检查配置中是否已经在系统视图或以太网接口视图下配置了 buffer queue shared 命令，若此时需要配置 burst-mode enable 命令，请先保证系统视图或以太网接口视图下未使能 buffer queue shared 命令 • 请联系技术支持

26.1.173 DrvDebug

日志内容	Please recover PFC deadlock.Port is [[STRING]].
参数解释	$1：以太网接口名
日志等级	4
举例	DRVPLAT/4/DrvDebug: Please recover PFC deadlock.Port is WGE4/0/9.
日志说明	配置PFC死锁检测功能失败时出现（非必现），提示当前配置PFC死锁检测功能失败的原因是接口处于PFC死锁检查恢复过程中
处理建议	请联系技术支持

26.1.174 DrvDebug

日志内容	PFC Deadlock Detected. Port is [[STRING]], Cos is [[INT]].
参数解释	$1：以太网接口名 $2：Dot1p优先级的队列号
日志等级	4
举例	DRVPLAT/4/DrvDebug: PFC Deadlock Detected. Port is WGE4/0/9, Cos is 5.
日志说明	PFC死锁已经被检测到，标识对应的以太网接口和Dot1p优先级的队列号
处理建议	请联系技术支持

26.1.175 DrvDebug

日志内容	PFC Deadlock Detected. Port is [[STRING]], Cos is [[INT]].
参数解释	$1：以太网接口名 $2：Dot1p优先级的队列号
日志等级	4
举例	DRVPLAT/4/DrvDebug: PFC Deadlock Recover. Port is WGE4/0/9, Cos is 5.
日志说明	PFC死锁已执行恢复操作，标识对应的以太网接口和Dot1p优先级的队列号
处理建议	请联系技术支持

26.1.176 DrvDebug

日志内容	PFC Deadlock Limit Reached, Pfc turn-off. IfIndex:[[UINT]].
参数解释	$1：以太网接口号的十六进制
日志等级	4
举例	DRVPLAT/4/DrvDebug: PFC Deadlock Limit Reached, Pfc turn-off. IfIndex: 0x2e.
日志说明	表示对应接口PFC死锁出现的频率超过了配置门限值，执行关闭对应端口的PFC功能的动作时产生，并标识对应的以太网接口号
处理建议	• 去使能 PFC 死锁的门限 • 请联系技术支持

26.1.177 DrvDebug

日志内容	PFC deadlock limit reached! If:[[STRING]], Cos:[[UINT]], time:[[UINT]], cnt:[[UINT]].
参数解释	$1：以太网接口名 $2：Dot1p优先级的队列号

	$3：PFC死锁检测的周期（s） $4：本周期检测到的PFC死锁次数
日志等级	4
举例	DRVPLAT/4/DrvDebug: PFC deadlock limit reached! If: WGE4/0/9, Cos:5, time:20, cnt:96.
日志说明	表示当前接口队列在指定周期内发生PFC死锁的上限次数已经达到门限，执行对应的动作时产生
处理建议	若需要修改执行的动作，请通过以太网接口视图下的priority-flow-control deadlock threshold action命令配置或系统视图下的priority-flow-control deadlock threshold命令配置，优先执行以太网接口视图下的配置

26.1.178 DrvDebug

日志内容	PFC deadlock limit has been cleared, Ifname: [[STRING]].
参数解释	$1：以太网接口名
日志等级	4
举例	DRVPLAT/4/DrvDebug: PFC deadlock limit has been cleared, Ifname: WGE4/0/9.
日志说明	表示已经去使能priority-flow-control deadlock threshold命令后，不再需要执行达到门限值时端口的动作
处理建议	无需处理

26.1.179 DrvDebug

日志内容	The software version is not compatible with the hardware.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: The software version is not compatible with the hardware.
日志说明	该设备的软件版本和硬件不匹配
处理建议	检查设备的软件版本和硬件是否配套： • 若配套，则可能是硬件存在故障，请联系技术人员处理 • 若不配套，则请更换软件版本

26.1.180 DrvDebug

日志内容	Hotspot [STRING] in slot [STRING] read [STRING]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	$1：热点传感器编号 $2：单板所在的槽位号 $3：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in slot 0 read 125. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	热点温度超过温度传感器的断电门限，热点所在单板即将被断电
处理建议	1. 请使用 **display fan**命令检查所有风扇状态： • 若风扇状态为 absent，请检查风扇框是否安装到位，风扇是否插稳，风扇恢复正常后，为单板上电请执行步骤 2 • 若风扇状态为 fault，请尝试拔插风扇框或者更换新风扇，如果不能恢复请联系技术支持，若风扇恢复正常，为单板上电请执行步骤 2 • 若所有风扇状态为 normal，为单板上电请执行步骤 2 2. 更换插入新的正常单板，或者等过温的单板温度降下来，然后拔插该单板使该单板上电

26.1.181 DrvDebug

日志内容	Hotspot [STRING] in chassis [STRING] slot [STRING] read [STRING]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	$1：热点传感器编号 $2：设备在IRF中的成员编号 $3：单板所在的槽位号 $4：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in chassis 1 slot 0 read 125. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	热点温度超过温度传感器的断电门限，热点所在单板即将被断电
处理建议	1. 请使用 **display fan**命令检查所有风扇状态： • 若风扇状态为 absent，请检查风扇框是否安装到位，风扇是否插稳，风扇恢复正常后，为单板上电请执行步骤 2 • 若风扇状态为 fault，请尝试拔插风扇框或者更换新风扇，如果不能恢复请联系技术支持，若风扇恢复正常，为单板上电请执行步骤 2 • 若所有风扇状态为 normal，为单板上电请执行步骤 2 2. 更换插入新的正常单板，或者等过温的单板温度降下来，然后拔插该单板使该单板上电

26.1.182 DrvDebug

日志内容	The MPU in slot [UINT32] failed to obtain the card status in slot [UINT32].
参数解释	$1：主控板所在槽位号 $2：单板槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The MPU in slot 0 failed to obtain the card status in slot 2.
日志说明	主控板不能正确读取指定slot的单板状态信息
处理建议	请联系技术支持

26.1.183 DrvDebug

日志内容	The MPU in chassis [UINT32] slot [UINT32] failed to obtain the card status in chassis [UINT32] slot [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：主控板所在槽位号 $3：设备在IRF中的成员编号 $4：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The MPU in chassis 1 slot 0 failed to obtain the card status in chassis 1 slot 2.
日志说明	主控板不能正确读取指定slot的单板状态信息
处理建议	请联系技术支持

26.1.184 DrvDebug

日志内容	The port up-mode configuration exists on port [STRING]. Please remove the configuration, and then install the GE transceiver module.
参数解释	$1：本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port up-mode configuration exists on port Ten-GigabitEthernet3/0/49. Please remove the configuration, and then install the GE transceiver module.
日志说明	光口被强制开启后，如果10GE光口插入光电转换模块、1000M光模块，流量不能正常转发
处理建议	**1.** 如要继续使用强制开启光口功能，请拔掉当前端口上的光电转换模块、1000M 光模块 **2.** 如不继续使用强制开启光口功能，需要使用光电转换模块、1000M光模块，则请先拔掉当前 10GE光口的上述光模块，然后在端口上执行 undo port up-mode操作，再次在该端口上插入上述光模块

26.1.185 DrvDebug

日志内容	The port [STRING] has been changed to inactive status, please check.
参数解释	$1：IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 has been changed to inactive status, please check.
日志说明	提示端口状态转变为非激活状态
处理建议	**1.** 检查光模块是否插紧 **2.** 如果光模块已经插紧，请联系技术支持

26.1.186 DrvDebug

日志内容	The port [STRING] has been changed to active status.
参数解释	$1：IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 has been changed to active status.
日志说明	提示端口状态转变为激活状态
处理建议	无需处理

26.1.187 DrvDebug

日志内容	The port [STRING] can't receive irf pkt and has been changed to inactive status, please check.
参数解释	$1：IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 can't receive irf pkt and has been changed to inactive status, please check.
日志说明	指定端口不能接收IRF协议报文，并且端口已经转变成非激活状态
处理建议	**1.** 检查光模块是否插紧 **2.** 如果光模块已经插紧，请联系技术支持

26.1.188 DrvDebug

日志内容	The port [STRING] can't receive irf pkt, please check.
参数解释	$1：IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 can't receive irf pkt, please check.
日志说明	指定端口不能接收IRF协议报文
处理建议	**1.** 检查光模块是否插紧 **2.** 如果光模块已经插紧，请联系技术支持

26.1.189 DrvDebug

日志内容	Port [STRING] Connect fail, Reason: [STRING], please check.
参数解释	$1：IRF物理端口号 $2：失败原因 具体原因有： • MemberID is the same • IRF-Port is the same • LoopBack • Check timeout • Fiber Connect Error • Topo Invalid • Peer Notify • The settings for the Layer 2 and Layer 3 multicast table capacity mode are different on this card and the peer card on the neighboring member device. • Other reason
日志等级	4
举例	DRVPLAT/4/DrvDebug: Port Ten1/1/0/25 Connect fail, Reason: Check timeout, please check.
日志说明	提示端口连接失败，给出失败原因
处理建议	**1.** 如果原因为“MemberID is the same”，请修改成 IRF 成员设备的编号为不同值 **2.** 如果原因为“IRF-Port is the same”，请修改一端的 IRF 端口号，保证 IRF 链路两端一端为 IRF-Port1，另一端为 IRF-Port2 **3.** 如果原因为“LoopBack”，请取消 IRF 物理端口上的环回设置 **4.** 如果原因为“Check timeout”，请检查两端 IRF 物理端口上的配置是否正确, 一般是一侧连接 IRF 物理端口一侧连接普通业务口导致 **5.** 如果原因为“Fiber Connect Error”，请检查两端的 IRF 物理端口是否在一条 IRF 链路上，并检查 IRF 链路是否正常，IRF 物理端口上的配置是否正确 **6.** 如果原因为“Topo Invalid”，请检查设备连接 **7.** 如果原因为“Peer Notify”，请插拔对端端口的光模块尝试恢复 **8.** 如果原因为“The settings for the Layer 2 and Layer 3 multicast table capacity mode are different on this card and the peer card on the neighboring member device”，请使用 switch-mode 命令将业务板的工作模式和代理模式配置成一致。 **9.** 如果原因为“Other reason”，请联系技术支持

26.1.190 DrvDebug

日志内容	The max-ecmp-num configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [STRING]
参数解释	$1：IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The max-ecmp-num configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2
日志说明	在一个IRF中，各个成员设备的最大等价路由数配置必须相同
处理建议	请使用**display max-ecmp-num**命令检查并通过**max-ecmp-num**命令修改各个成员设备的最大等价路由数配置相同

26.1.191 DrvDebug

日志内容	The device vendor must be the same for all member devices in one IRF fabric. Please check the vendor of the neighbor device connected to IRF-port [STRING].
参数解释	$1：IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The device vendor must be the same for all member devices in one IRF fabric. Please check the vendor of the neighbor device connected to IRF-port [STRING].
日志说明	在一个IRF中，各个成员设备的公司品牌必须相同
处理建议	请使用相同公司品牌的交换机组建IRF

26.1.192 DrvDebug

日志内容	DeviceInfo must be the same in one IRF. DeviceInfo: [STRING], PeerDeviceInfo: [STRING].
参数解释	$1：本端设备类型 $2：对端设备类型
日志等级	4
举例	DRVPLAT/4/DrvDebug: DeviceInfo must be the same in one IRF. DeviceInfo: S7500XG, PeerDeviceInfo: S12500G-AF.
日志说明	本系列交换机仅能与相同系列的交换机之间建立IRF
处理建议	请使用相同系列的交换机组建IRF

26.1.193 DrvDebug

日志内容	The product can't support stack mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: The product can't support stack mode.
日志说明	本产品不支持切换成IRF模式
处理建议	请选择支持IRF模式的设备组建

26.1.194 DrvDebug

日志内容	The Systemworking mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [STRING].
参数解释	$1：IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The Systemworking mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2.
日志说明	在一个IRF中，各个成员设备的工作模式配置必须相同
处理建议	请用**display system-working-mode**命令检查并通过**system-working-mode**命令修改各个成员设备的工作模式相同

26.1.195 DrvDebug

日志内容	Failed to issue routes to hardware. The IPv6 prefix resource is insufficient.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to issue routes to hardware. The IPv6 prefix resource is insufficient.
日志说明	路由下发失败，原因是IPv6前缀资源不足。
处理建议	请联系技术支持。

日志内容	Failed to issue routes to hardware. The IPv4 prefix resource is insufficient.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Failed to issue routes to hardware. The IPv4 prefix resource is insufficient.。
日志说明	路由下发失败，原因是IPv4前缀资源不足。
处理建议	请联系技术支持。

26.1.196 DrvDebug

日志内容	Board fault: chassis [UINT32] slot [UINT32], please check it.
参数解释	$1: 设备在IRF中的成员编号。独立运行模式下，值为0 $2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board fault: chassis 1 slot 10, please check it.
日志说明	检测到单板的硬件存在故障
处理建议	**1.** 请使用 reboot 命令重启或插拔故障的单板 **2.** 请更换故障的单板 **3.** 请联系技术支持

26.1.197 DrvDebug

日志内容	Board fault: chassis [UINT32] slot [UINT32] or chassis [UINT32] slot [UINT32], please check them.
参数解释	$1、$3: 设备在IRF中的成员编号。独立运行模式下，值为0 $2、$4: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board fault: chassis 1 slot 11 or chassis 1 slot 9, please check them.
日志说明	检测到两块单板中有一块单板的硬件存在故障，但无法确认是哪一块单板
处理建议	**1.** 请使用 reboot 命令逐块重启或插拔提示有故障的单板 **2.** 请逐块更换提示有故障的单板 **3.** 请联系技术支持

26.1.198 DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] will be isolated, please check it.
参数解释	$1: 设备在IRF中的成员编号。独立运行模式下，值为0 $2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis 1 slot 2 will be isolated, please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被隔离。隔离后，单板将一直处于Fault状态
处理建议	**1.** 请重新拔插或更换提示有故障的单板 **2.** 请联系技术支持

26.1.199 DrvDebug

日志内容	The device does not support board in chassis [UINT32] slot [UINT32] ,type is unknown(0x[UINT32]), Please check.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：单板类型值
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis=1-Slot=5;The device does not support board in chassis 1 slot 5 ,type is unknown(0x108), Please check.
日志说明	IRF模式下，提示设备不支持该单板
处理建议	请联系技术支持

26.1.200 DrvDebug

日志内容	The device does not support board in slot [UINT32] ,type is unknown(0x[UINT32]), Please check.
参数解释	$1：单板所在的槽位号 $2：单板类型值
日志等级	4
举例	DRVPLAT/4/DrvDebug: The device does not support board in slot 5 ,type is unknown(0x108), Please check.
日志说明	独立运行模式下，提示设备不支持该单板
处理建议	请联系技术支持

26.1.201 DrvDebug

日志内容	The service module in slot [UINT32] failed to start up because it does not support the current multicast forwarding mode.
参数解释	$1：业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in slot 2 failed to start up because it does not support the current multicast forwarding mode.
日志说明	指定槽位上的业务板不支持当前配置的组播转发模式
处理建议	• 修改设备的组播转发模式为标准模式，并重启设备 • 更换该槽位的业务板为支持组播转发模式的业务板

26.1.202 DrvDebug

日志内容	The service module in slot [UINT32] on chassis [UINT32] failed to start up because the service module does not support the current multicast forwarding mode.
参数解释	$1：设备在IRF中的成员编号 $2：业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in slot 2 on chassis 1 failed to start up because the service module does not support the current multicast forwarding mode.
日志说明	指定槽位上的业务板不支持当前配置的组播转发模式
处理建议	• 修改设备的组播转发模式为标准模式，并重启设备 • 更换该槽位的业务板为支持组播转发模式的业务板

26.1.203 DrvDebug

日志内容	The service module in chassis [UINT32] slot [UINT32] failed to start because the current fabric-mode does not support the service module. Please change the fabric-mode.
参数解释	$1：设备在IRF中的成员编号 $2：业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in chassis 1 slot 3 failed to start because the current fabric-mode does not support the service module.Please change the fabric-mode.
日志说明	当前配置的fabric-mode不支持指定槽位上的业务板，请更换转发模式
处理建议	• 修改设备的转发模式 • 更换指定槽位的业务板为当前转发模式支持的业务板

26.1.204 DrvDebug

日志内容	The service module in chassis [UINT32] slot [UINT32] failed to start because it is not compatible with the switching fabric modules.
参数解释	$1：设备在IRF中的成员编号 $2：业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in chassis 2 slot 5 failed to start because it is not compatible with the switching fabric modules.
日志说明	插入的业务板与当前的交换网板不匹配，请更换业务板或交换网板。
处理建议	• 更换当前交换网板匹配的业务板 • 更换当前业务板匹配的交换网板

26.1.205 DrvDebug

日志内容	The service module in slot [UINT32] failed to start because it is not compatible with the switching fabric modules.
参数解释	$1：业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in slot 5 failed to start because it is not compatible with the switching fabric modules.
日志说明	插入的业务板与当前的交换网板不匹配，请更换业务板或交换网板。
处理建议	• 更换当前交换网板匹配的业务板 • 更换当前业务板匹配的交换网板

26.1.206 DrvDebug

日志内容	No switching fabric modules are present. For the system to work correctly, verify that at least one fabric module is available and operating correctly.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; No switching fabric modules are present. For the system to work correctly, verify that at least one fabric module is available and operating correctly.
日志说明	以下情况会出现此日志： • 业务板启动时，检查到网板槽位上都没有安装网板 • 网板都拔出
处理建议	**1.** 请确认设备的网板槽位上是否有网板在位。如果没有，请至少在一个网板槽位上插入交换网板；如果有，请检查交换网板是否安装到位 **2.** 请联系技术支持

26.1.207 DrvDebug

日志内容	The fabric mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [STRING].
参数解释	$1：IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; The fabric mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2.
日志说明	在一个IRF中，各个成员设备的转发配置必须相同
处理建议	请用**display fabric-mode**命令检查并通过**fabric-mode**命令修改各个成员设备的工作模式相同

26.1.208 DrvDebug

日志内容	This slot does not support global link aggregation load sharing algorithm configuration.
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug: -MDC=1-Slot=5; This slot does not support global link aggregation load sharing algorithm configuration.
日志说明	link-aggregation global load-sharing algorithm命令配置的聚合负载分担HASH算法在指定槽位的单板上不支持，当前算法可以通过display link-aggregation load-sharing mode命令查询
处理建议	• 如果需要使用当前算法进行聚合负载分担，请更换该槽位的单板 • 如果需要使用当前槽位的单板，请重新配置单板支持的聚合负载分担 HASH 算法 • 如果当前单板不需要进行聚合负载分担，则无需处理

26.1.209 DrvDebug

日志内容	[STRING]: Some VLAN interfaces might not function properly on this device.
参数解释	$1：创建的VLAN接口
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=6; Vlan-interface1000: Some VLAN interfaces might not function properly on this device.
日志说明	在框式设备上创建VLAN接口时超出最大范围提示
处理建议	在规格范围内创建，删除超规格的VLAN接口

26.1.210 DrvDebug

日志内容	OLT ports cannot recover(auto-recovery off). Reason：[STRING]
参数解释	$1：表示OLT端口无法恢复的原因，原因包括： ◦ Management tunnel down：管理通道断开 ◦ Abnormal reboot：异常重启 ◦ Executing set hardware internal epon olt resetchip：EPON OLT 芯片重启
日志等级	4
举例	DRVPLAT/4/DrvDebug: OLT ports cannot recover(auto-recovery off). Reason: Management tunnel down
日志说明	自动恢复关闭的情况下，OLT端口无法恢复的原因
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

26.1.211 DrvDebug

日志内容	OLT ports rebooted. Reason：[STRING]
参数解释	$1：表示OLT端口重启的原因，原因包括： ○ Management tunnel down：管理通道断开 ○ Abnormal reboot：异常重启 ○ Executing set hardware internal epon olt resetchip：EPON OLT 芯片重启
日志等级	4
举例	DRVPLAT/4/DrvDebug: OLT ports rebooted. Reason: Abnormal reboot
日志说明	OLT端口重启的原因
处理建议	如果OLT端口不断重启，请收集配置文件、日志信息和告警信息，并联系技术支持。

26.1.212 DrvDebug

日志内容	OLT ports recovered from：[STRING]
参数解释	$1：表示OLT端口恢复的原因，原因包括： ○ management tunnel down：管理通道断开 ○ abnormal reboot：异常重启 ○ manual reset：手动复位
日志等级	4
举例	DRVPLAT/4/DrvDebug: OLT ports recovered from manual reset
日志说明	OLT端口恢复的原因
处理建议	无

26.1.213 DrvDebug

日志内容	OLT ports cannot recover. Reason：[STRING]
参数解释	$1：表示执行OLT端口恢复操作失败的原因，原因包括： ○ Unknown：未知错误 ○ Configured with the port-type gigabitethernet command：使用了gigabitethernet 接口类型的命令行配置 ○ Assigned to a fiber backup group：指定到一个光纤备份组 ○ Assigned to an ROLT interface：指定到一个 ROLT 端口 ○ A chip of this slot is being reset. Please try again later：OLT 端口所在单板正在重启，请稍候再试
日志等级	4
举例	DRVPLAT/4/DrvDebug: OLT ports cannot recover. Reason: Unknown
日志说明	OLT端口无法执行恢复操作的原因
处理建议	**1.** 请根据日志提示信息进行操作 **2.** 若问题仍未解决，请收集配置文件、日志信息和告警信息，并联系技术支持

26.1.214 DrvDebug

日志内容	multicast CDR info：[STRING]
参数解释	$1：组播CDR的缓存信息，信息包括： ○ RecordType：记录类型（1：用户加入时记录，2：用户离开时记录） ○ MultiIp：组播组地址 ○ MultiSrcIp：组播源地址 ○ Index：接口索引 ○ SubIfIndex：UNI ID ○ MultiVlanId：组播 VlanID ○ MultiRecId：记录 ID ○ MultiJoinTime：用户上线时间 ○ JoinType：用户上线方式（1：permit 加入，2：preview 加入） ○ MultiLeaveTime：用户离线时间 ○ LeaveType：用户离线方式（1：用户自行离开，2：管理员强制断开，3：到达老化时间离开）
日志等级	4
举例	DRVPLAT/4/DrvDebug: multicast CDR info:1，244001，192168010，10，1，100，10，1150，1，1250，1
日志说明	组播CDR缓存信息记录
处理建议	无

26.1.215 DrvDebug

日志内容	Failed to issue the MAC-based VLAN entry for MAC address %02x%02x-%02x%02x-%02x%02x in VLAN %u, because resources were insufficient on the card.
参数解释	$1：MAC地址 $2：VLAN ID
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=4; Failed to issue the MAC-based VLAN entry for MAC address 0001-0001-0001 in VLAN 100, because resources were insufficient on the card.
日志说明	MAC VLAN资源不足时打印日志
处理建议	无

26.1.216 DrvDebug

日志内容	[UINT] parity and ECC errors were detected in [UINT] seconds on chip [UINT]
参数解释	$1：奇偶校验和ECC校验错误次数 $2：统计采样周期 $3：发生错误的芯片ID
日志等级	4
举例	DRVPLAT/4/DrvDebug: 10 parity and ECC errors were detected in 60 seconds on chip 1.
日志说明	芯片硬件表项在一定周期内发生的奇偶校验和ECC校验错误次数
处理建议	无

26.1.217 DrvDebug

日志内容	[UINT] inconsistency errors between hardware and software forwarding entries were detected in [UINT] seconds on chip [UINT].
参数解释	$1：软硬件表项不一致错误次数 $2：统计采样周期 $3：发生错误的芯片ID
日志等级	4
举例	DRVPLAT/4/DrvDebug: 10 inconsistency errors between hardware and software forwarding entries were detected in 60 seconds on chip 1.
日志说明	芯片在一定周期内发生软硬件表项不一致的错误
处理建议	无

26.1.218 DrvDebug

日志内容	[UINT] parity and ECC errors on chip [UINT] failed to be cleared. Please try to restart device or replace the chip.
参数解释	$1：奇偶校验和ECC校验错误恢复失败的次数 $2：发生错误的芯片ID
日志等级	4
举例	DRVPLAT/4/DrvDebug: 2 parity and ECC errors on chip 1 failed to be cleared. Please try to restart device or replace the chip.
日志说明	芯片硬件表项发生奇偶校验和ECC校验错误并且恢复失败
处理建议	重启设备或者替换芯片

26.1.219 DrvDebug

日志内容	[UINT] unrecoverable parity and ECC errors occurred in [UINT] seconds on chip [UINT]. The system will reboot automatically.
参数解释	$1：恢复失败的次数 $2：统计采样周期 $3：发生错误的芯片ID
日志等级	4
举例	DRVPLAT/4/DrvDebug: 5 unrecoverable parity and ECC errors occurred in 60 seconds on chip 1. The system will reboot automatically.
日志说明	芯片关键硬件表项在一定周期内发生的恢复失败错误次数达到阈值，设备自动重启
处理建议	无

26.1.220 DrvDebug

日志内容	[UINT] unrecoverable parity and ECC errors occurred in [UINT] seconds on chip [UINT] Please reboot the card.
参数解释	$1：恢复失败的次数 $2：统计采样周期 $3：发生错误的芯片ID
日志等级	4
举例	DRVPLAT/4/DrvDebug: 5 unrecoverable parity and ECC errors occurred in 60 seconds on chip 1. Please reboot the card.
日志说明	芯片关键硬件表项在一定周期内发生的恢复失败错误次数达到阈值，提示用户重启单板
处理建议	重启单板

26.1.221 DrvDebug

日志内容	The load sharing mode applied in aggregation group %u did not take effect on slot %u due to insufficient hardware resources.
参数解释	$1：聚合组ID $2：本地槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=4; The load sharing mode applied in aggregation group 2 did not take effect on slot 4 due to insufficient hardware resources.
日志说明	基于聚合组设置负载分担，资源不足时打印日志
处理建议	无

26.1.222 DrvDebug

日志内容	This slot does not support global link aggregation load sharing algorithm configuration
参数解释	不涉及
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=4; This slot does not support global link aggregation load sharing algorithm configuration
日志说明	配置设备不支持的HASH算法时会提示不支持
处理建议	无

26.1.223 DRVPLAT_VXLAN_WARN

日志内容	Failed to disable the tunnel resource sharing function due to resource insufficiency.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DRVPLAT_VXLAN_WARN: Failed to disable the tunnel resource sharing function due to resource insufficiency.
日志说明	由于资源不足，执行**undo vxlan flooding share-resource**命令关闭隧道资源共享功能失败
处理建议	• 维持隧道资源共享功能以节省设备资源 • 如需修改资源分配，请请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

26.1.224 PORT_ATTACK_OCCUR

日志内容	Auto port-defend started.SourceAttackInterface=[[STRING]], AttackProtocol=[[STRING]]
参数解释	$1：以太网接口号 $2：协议名称
日志等级	4
举例	DRVPLAT/4/PORT_ATTACK_OCCUR: -MDC=1-Slot=1; Auto port-defend started.SourceAttackInterface=Twenty-FiveGigE1/0/8, AttackProtocol L2_COPY_CPU
.日志说明	指定端口上受到指定协议的攻击
处理建议	请联系技术支持

26.1.225 PORT_ATTACK_OCCUR

日志内容	Auto port-defend stopped.SourceAttackInterface=[[STRING]], AttackProtocol=[[STRING]]
参数解释	$1：以太网接口号 $2：协议名称
日志等级	4
举例	DRVPLAT/4/PORT_ATTACK_OCCUR: -MDC=1-Slot=1; Auto port-defend stopped.SourceAttackInterface=Twenty-FiveGigE1/0/8, AttackProtocol=L2_COPY_CPU
.日志说明	指定端口上指定协议的攻击停止
处理建议	请联系技术支持

26.1.226 SOFTCAR DROP

日志内容	Chip=[UINT32], Cos=[UINT32], Drop at Stage=[UINT32], StageCnt=[UINT64], TotalCnt=[UINT64], possible protocol [STRING]
参数解释	$1：出现报文丢包的芯片号 $2：出现报文丢包的队列ID $3：报文丢弃的统计周期，取值为0或非0 ○ 0：表示统计周期为 10 分钟 ○ 非 0：表示统计周期为 1 小时。每 10 分钟被分为一个阶段，多个阶段均有报文丢弃时，此处显示为阶段和。例如：如果每个阶段均有报文丢弃，显示为 63(2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5)；如果只有第 1 和第 3 阶段有丢包，显示为 5(2^0 + 2^2) $4：当前计数阶段被丢弃报文数 $5：被丢弃报文总数 $6：该队列中报文的协议类型
日志等级	4
举例	DRVPLAT/4/SOFTCAR DROP: -MDC=1-Slot=2; Chip=0,Cos=15, Drop at Stage=0, StageCnt=1303, TotalCnt=1303, possible protocol ARP/ARP_DAI/VSI_ARP/SADP
日志说明	芯片上的队列报文超过队列设定的阈值后，报文被丢弃
处理建议	请联系技术支持

26.1.227 SOFTCAR DROP

日志内容	Chip=[UINT32],Cos=[UINT32]
参数解释	$1：丢包恢复的芯片号 $2：丢包恢复的队列ID
日志等级	4
举例	DRVPLAT/4/SOFTCAR RECOVER: -MDC=1-Slot=2; Chip=0,Cos=15
日志说明	检测芯片队列上没有丢包后，打印恢复日志
处理建议	无

27 EDEV

本节介绍扩展设备管理模块输出的日志信息。

27.1 ALARM_IN_REMOVED

日志内容	Alarm removed on the alarm-in port [UNIT].
日志含义	告警输入接口的告警信号已解除，恢复到正常状态
参数解释	$1：表示告警输入端口的编号
日志等级	5 (Notification)
举例	EDEV/5/ALARM_IN_REMOVED: Alarm removed on the alarm-in port 1.
对系统的影响	对系统无影响
日志产生原因	某个告警输入接口的告警信号已解除，恢复到正常状态时，打印该日志
处理建议	无需处理

27.2 ALARM_IN_REPORTED

日志内容	Alarm reported on the alarm-in port [UNIT].
日志含义	告警输入接口收到告警信号
参数解释	$1：表示告警输入端口的编号
日志等级	5 (Notification)
举例	EDEV/5/EDEV_ALARM_IN_REPORTED: Alarm reported on the alarm-in port 1.
对系统的影响	与接口相连的设备可能无法正常通信
日志产生原因	某个告警输入接口收到告警信号时，打印该日志
处理建议	检查与告警输入接口相连的设备，确认该邻居设备是否发生异常

27.3 EDEV_BOOTROM_UPDATE_FAILED

日志内容	Failed to execute the bootrom update command.
日志含义	执行bootrom update命令失败
参数解释	无
日志等级	5 (Notification)
举例	EDEV/5/EDEV_BOOTROM_UPDATE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the bootrom update command.
对系统的影响	文件系统中的BootWare程序加载到BootWare的Normal区失败
日志产生原因	用户执行**bootrom update**命令将文件系统中的BootWare程序加载到BootWare的Normal区，操作失败时，打印该日志
处理建议	请根据提示信息采取相应措施

27.4 EDEV_BOOTROM_UPDATE_SUCCESS

日志内容	Executed the bootrom update command successfully.
日志含义	执行bootrom update命令已成功
参数解释	无
日志等级	5 (Notification)
举例	EDEV/5/EDEV_BOOTROM_UPDATE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the bootrom update command successfully.
对系统的影响	对系统无影响
日志产生原因	用户执行**bootrom update**命令将文件系统中的BootWare程序加载到BootWare的Normal区，操作成功时，打印该日志
处理建议	无需处理

27.5 EDEV_FAILOVER_GROUP_STATE_CHANGE

日志内容	Status of stateful failover group [STRING] with ID [UINT32] changed to [STRING].
日志含义	备份组的状态发生了变化
参数解释	$1：备份组的名字 $2：备份组的ID $2：备份组的状态： ○ primary 表示备份组中 primary 节点处理业务 ○ secondary 表示备份组中 secondary 节点处理业务
日志等级	5 (Notification)
举例	EDEV/5/EDEV_FAILOVER_GROUP_STATE_CHANGE: -MDC=1; Status of stateful failover group 123 with ID 0 changed to primary.
对系统的影响	对系统无影响
日志产生原因	当备份组的状态发生变化时，打印该日志
处理建议	无需处理

28 eMDI

本节介绍 eMDI 模块输出的日志信息。

28.1 EMDI_INDICATOR_OVER_THRES

日志内容	[STRING] alarm for instance [USHORT] was triggered: Value=[UINT32]/100000, Threshold=[UINT32]/100000, SuppressionTimes=[UCHAR].
日志含义	eMDI实例的告警触发
参数解释	$1：监控指标类型，取值为： • RTP-LR：RTP 报文的丢包率 • RTP-SER：RTP 报文的乱序率 • DPLR：TCP 报文的下游丢包率 • UPLR：TCP 报文的上游丢包率 $2：实例ID $3：监控指标值 $4：监控指标设定的阈值 $5：监控指标设定的告警抑制次数
日志等级	5 (Notification)
举例	EMDI/5/EMDI_INDICATOR_OVER_THRES: RTP-LR alarm for instance 100 was triggered: Value=150/100000, Threshold=100/100000, SuppressionTimes=3.
对系统的影响	无
日志产生原因	eMDI监控指标连续多次达到告警阈值
处理建议	• 执行 **display emdi statistics**命令，查看实例的统计信息 • 结合多个设备的实例的统计信息，进行故障定界

28.2 EMDI_INDICATOR_OVER_THRES_RESUME

日志内容	[STRING] alarm for instance [USHORT] was removed: Value=[UINT32]/100000, Threshold=[UINT32]/100000, SuppressionTimes=[UCHAR].
日志含义	eMDI实例的告警移除
参数解释	$1：监控指标类型，取值为： • RTP-LR：RTP 报文的丢包率 • RTP-SER：RTP 报文的乱序率 • DPLR：TCP 报文的下游丢包率 • UPLR：TCP 报文的上游丢包率 $2：实例ID $3：监控指标值 $4：监控指标设定的阈值 $5：监控指标设定的告警抑制次数
日志等级	5 (Notification)
举例	EMDI/5/EMDI_INDICATOR_OVER_THRES_RESUME: RTP-LR alarm for instance 100 was removed: Value=50/100000, Threshold=100/100000, SuppressionTimes=3.
对系统的影响	无
日志产生原因	eMDI监控指标连续多次低于告警阈值，监控指标恢复
处理建议	无

28.3 EMDI_INSTANCE_CONFLICT_FLOW

日志内容	The flow (SrcIP=[STRING], SrcPort=[USHORT], DstIP=[STRING], DstPort=[USHORT], Protocol=[STRING]) to be bound to a dynamic instance overlaps with the flow bound to instance [USHORT].
日志含义	为动态实例配置的目标数据流与已存在实例中的流冲突
参数解释	$1：流的源IP地址 $2：流的源端口号 $3：流的目的IP地址 $4：流的目的端口号 $5：流的协议类型，取值包括： • tcp • udp $6：已绑定了冲突数据流的实例ID
日志等级	5 (Notification)
举例	EMDI/5/EMDI_INSTANCE_CONFLICT_FLOW: The flow (SrcIP=10.0.0.1, SrcPort=10, DstIP=20.0.0.1, DstPort=20, Protocol=tcp) to be bound to a dynamic instance overlaps with the flow bound to instance 1.
对系统的影响	无
日志产生原因	为动态实例配置的流与已存在实例中的流冲突
处理建议	请删除已存在的冲突配置

28.4 EMDI_INSTANCE_EXCEED

日志内容	Maximum number of running instances on [STRING] already reached.
日志含义	正在运行的实例数量达到了最大值
参数解释	$1：chassis编号+slot编号、slot编号或device
日志等级	5 (Notification)
举例	EMDI/5/EMDI_INSTANCE_EXCEED: Maximum number of running instances on slot 1 already reached.
对系统的影响	不支持继续启动新的实例
日志产生原因	正在运行的实例数量已经达到了单板规格最大值
处理建议	如果想继续启动一些实例，请先停止一些该板上不必要的实例

28.5 EMDI_INSTANCE_SAME_FLOW

日志内容	The flow to be bound to a dynamic instance was already bound to instance [USHORT]: SrcIP=[STRING], SrcPort=[USHORT], DstIP=[STRING], DstPort=[USHORT], Protocol=[STRING].
日志含义	为动态实例配置的目标数据流与已存在实例中的流相同
参数解释	$1：已绑定了冲突数据流的实例ID $2：流的源IP地址 $3：流的源端口号 $4：流的目的IP地址 $5：流的目的端口号 $6：流的协议类型，取值包括： • tcp • udp
日志等级	5 (Notification)
举例	EMDI/5/EMDI_INSTANCE_SAME_FLOW: The flow to be bound to a dynamic instance was already bound to instance 1: SrcIP=10.0.0.1, SrcPort=10, DstIP=20.0.0.1, DstPort=20, Protocol= tcp.
对系统的影响	无
日志产生原因	为动态实例配置的流与已存在实例中的流相同
处理建议	请删除已存在的冲突配置

29 EPA

本节介绍 EPA 模块输出的日志信息。

29.1 EPA_ENDPOINT_ONLINE

日志内容	Detected the association of an endpoint (device ID [STRING], MAC address [STRING]) on interface [STRING] in VLAN [UINT16].
日志含义	EPA监控到终端上线
参数解释	$1：连接终端的那台设备的桥MAC $2：终端的MAC地址 $3：终端上线接口 $4：终端所属的VLAN
日志等级	6 (Informational)
举例	EPA/6/EPA_ENDPOINT_ONLINE: Detected the association of an endpoint (device ID a4c2-d4ad-0200, MAC address 12c2-d4ed-0200) on interface GigabitEthernet1/0/1 in VLAN 1.
对系统的影响	对系统无影响
日志产生原因	监控到终端上线
处理建议	无需处理

29.2 EPA_ENDPOINT_OFFLINE

日志内容	Detected the disassociation of an endpoint (device ID [STRING], MAC address [STRING]) on interface [STRING] in VLAN [UINT16].
日志含义	EPA监控到终端下线
参数解释	$1：连接终端的那台设备的桥MAC $2：终端的MAC地址 $3：终端上线接口 $4：终端所属的VLAN
日志等级	6 (Informational)
举例	EPA/6/EPA_ENDPOINT_OFFLINE: Detected the disassociation of an endpoint (device ID a4c2-d4ad-0200, MAC address 12c2-d4ed-0200) on interface GigabitEthernet1/0/1 in VLAN 1.
对系统的影响	对系统无影响
日志产生原因	监控到终端下线
处理建议	无需处理

29.3 EPA_DEVICETYPE_CHANGE

日志内容	Cleared EPA monitor rule configurations. Reason: Device type changed from [STRING] to [STRING].
日志含义	因为设备类型切换，EPA监控规则被完全清除
参数解释	$1：切换前的设备类型： • TM：SmartMC 网络中的管理设备 • TC：SmartMC 网络中的成员设备 • Self-managed：非 SmartMC 网络中的设备 $2：切换后的设备类型
日志等级	6 (Informational)
举例	EPA/6/EPA_DEVICETYPE_CHANGE: Cleared EPA monitor rule configurations. Reason: Device type changed from TC to Self-managed.
对系统的影响	对系统无影响
日志产生原因	因为设备类型切换，EPA监控规则被完全清除
处理建议	如需使用规则过滤EPA终端，请重新执行**epa monitor-rule**命令来配置EPA终端静态识别规则，或者执行**epa auto-identify enable**命令开启EPA终端自动识别功能

30 ERPS

本节介绍 ERPS 模块输出的日志信息。

30.1 ERPS_PEERLINK_CHECK

日志内容	An ERPS ring member port can't be configured as a peer-link interface.
日志含义	ERPS环端口不能配置为peer-link接口
参数解释	无
日志等级	6 (Informational)
举例	ERPS/6/ERPS_PEERLINK_CHECK: An ERPS ring member port can't be configured as a peer-link interface.
对系统的影响	ERPS环无法建立
日志产生原因	ERPS环端口不支持配置为peer-link接口
处理建议	将ERPS环端口配置为非peer-link接口

30.2 ERPS_STATE_CHANGED

日志内容	Ethernet ring [UINT16] instance [UINT16] changed state to [STRING].
日志含义	ERPS环上实例状态发生改变
参数解释	$1：ERPS环号 $2：ERPS环实例编号 $3：ERPS实例状态： o Init：环端口不完整时（非互联节点的端口数量小于 2 或互联节点的端口数量小于 1），处于 Init 状态 o Idle：环初始化过后进入到稳定状态，当 Owner 节点进入 Idle 状态后，其它节点随之进入 Idle 状态 o Protection：当环网某段链路出现故障，环路经过保护倒换，最终稳定到的状态。当链路中某个节点进入 Protection 状态后，其它节点随之进入 Protection 状态 o MS：MS 状态下可以手动倒换流量转发路径。当对链路中某个节点进行 MS 操作后，其它节点随之进入 MS 状态 o FS：FS 状态下可以强制倒换流量转发路径。当对链路中某个节点进行 FS 操作后，其它节点随之进入 FS 状态 o Pending：Pending 状态是一个不稳定的状态，是各状态在进行跳转时的一个过渡状态
日志等级	4 (Warning)
举例	ERPS/4/ERPS_STATE_CHANGED: Ethernet ring 1 instance 1 changed state to Idle.
对系统的影响	网络拓扑改变，有可能引起业务流量丢失
日志产生原因	ERPS环上实例状态发生改变
处理建议	1. 请检查 ERPS 网络拓扑中是否有新的物理链路加入 o 如果有，检查新加入的物理链路是否需要，如果需要，属于正常的运行信息；如果不需要，请收集信息并联系技术支持人员 o 如果没有，请检查网络拓扑中有没有加入 ERPS 协议的端口状态变为 Up/Down，如果有，属于正常运行信息，无需处理；如果没有，请收集信息并联系技术支持人员 2. 请收集配置文件、日志信息和告警信息，并联系技术支持

31 ETH

本节介绍 ETH 模块输出的日志信息。

31.1 ETH_SET_MAC_FAILED

日志内容	Failed to set the MAC address [STRING] on [STRING].
日志含义	接口的MAC地址配置失败
参数解释	$1：MAC地址 $2：接口名称
日志等级	5 (Notification)
举例	ETH/5/ETH_SET_MAC_FAILED: Failed to set the MAC address 0001-0001-0001 on GigabitEthernet1/0/1.
对系统的影响	可能会导致该接口无法转发业务流量
日志产生原因	在配置恢复、IRF分裂、新单板插入情况下，由于接口的MAC地址和设备桥MAC地址的高36位不一致，设置接口的MAC地址失败
处理建议	重新配置合适的接口MAC地址

32 ETHMLAG

本节介绍 ETHMLAG 模块输出的日志信息。

32.1 ETHMLAG_MAC_INEFFECTIVE

日志内容	ETHMLAG failed to add the MAC address of [STRING]. Cause: [STRING].
日志含义	VLAN接口的MAC地址下发失败
参数解释	$1：接口名称 $2：出现错误的原因
日志等级	3 (Error)
举例	ETHMLAG/3/ETHMLAG_MAC_INEFFECTIVE: ETHMLAG failed to add the MAC address of Vlan-interface20. Cause: Insufficient hardware resources.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	ETHMLAG添加VLAN接口的MAC地址失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

33 ETHOAM

本节介绍 ETHOAM 模块输出的日志信息。

33.1 ETHOAM_CONNECTION_FAIL_DOWN

日志内容	The link is down on interface [string] because a remote failure occurred on peer interface.
日志含义	对端接口发生故障，链路down
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	ETHOAM/5/ETHOAM_CONNECTION_FAIL_DOWN: The link is down on interface Ethernet1/0/1 because a remote failure occurred on peer interface.
对系统的影响	链路down
日志产生原因	对端接口发生故障
处理建议	检查链路状态或对端的OAM状态

33.2 ETHOAM_CONNECTION_FAIL_TIMEOUT

日志内容	Interface [string] removed the OAM connection because it received no Information OAMPDU before the timer times out.
日志含义	接口在超时时间内没有收到信息OAMPDU，所以删除OAM连接
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	ETHOAM/5/ETHOAM_CONNECTION_FAIL_TIMEOUT: Interface Ethernet1/0/1 removed the OAM connection because it received no Information OAMPDU before the timer times out.
对系统的影响	以太网OAM连接无法建立
日志产生原因	• 链路 down • 对端的 OAM 功能没有使能
处理建议	检查链路状态或对端的OAM状态

33.3 ETHOAM_CONNECTION_FAIL_UNSATISF

日志内容	Interface [string] failed to establish an OAM connection because the peer doesn’t match the capacity of the local interface.
日志含义	对端与本端接口的OAM协议状态不匹配，建立OAM连接失败
参数解释	$1：接口名称
日志等级	3 (Error)
举例	ETHOAM/3/ETHOAM_CONNECTION_FAIL_UNSATISF: Interface Ethernet1/0/1 failed to establish an OAM connection because the peer doesn’t match the capacity of the local interface.
对系统的影响	以太网OAM连接无法建立
日志产生原因	对端与本端接口的OAM协议状态不匹配
处理建议	分析两端发出的OAM报文中的协议状态字段

33.4 ETHOAM_CONNECTION_SUCCEED

日志内容	An OAM connection is established on interface [string].
日志含义	OAM连接建立成功
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_CONNECTION_SUCCEED: An OAM connection is established on interface Ethernet1/0/1.
对系统的影响	无
日志产生原因	以太网OAM正常建立连接
处理建议	无需处理

33.5 ETHOAM_DISABLE

日志内容	Ethernet OAM is now disabled on interface [string].
日志含义	以太网OAM功能已关闭
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_DISABLE: Ethernet OAM is now disabled on interface Ethernet1/0/1.
对系统的影响	该接口的以太网OAM功能关闭
日志产生原因	用户在以太网接口下关闭了以太网OAM功能
处理建议	无需处理

33.6 ETHOAM_DISCOVERY_EXIT

日志内容	OAM interface [string] quit the OAM connection.
日志含义	本端接口退出OAM连接
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	ETHOAM/5/ ETHOAM_DISCOVERY_EXIT: OAM interface Ethernet1/0/1 quit the OAM connection.
对系统的影响	以太网OAM连接无法建立
日志产生原因	对端以太网OAM功能关闭
处理建议	无需处理

33.7 ETHOAM_ENABLE

日志内容	Ethernet OAM is now enabled on interface [string].
日志含义	以太网OAM功能已使能
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_ENABLE: Ethernet OAM is now enabled on interface Ethernet1/0/1.
对系统的影响	无
日志产生原因	用户在以太网接口下开启了以太网OAM功能
处理建议	无需处理

33.8 ETHOAM_ENTER_LOOPBACK_CTRLLED

日志内容	The local OAM entity enters remote loopback as controlled DTE on OAM interface [string].
日志含义	对端使能OAM远端环回功能后，本端OAM实体作为被控制DTE进入远端环回
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLED: The local OAM entity enters remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
对系统的影响	以太网OAM远端环回功能正常开启
日志产生原因	对端使能以太网OAM远端环回功能
处理建议	无需处理

33.9 ETHOAM_ENTER_LOOPBACK_CTRLLING

日志内容	The local OAM entity enters remote loopback as controlling DTE on OAM interface [string].
日志含义	接口使能OAM远端环回功能后，本端OAM实体作为控制DTE进入远端环回
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLING: The local OAM entity enters remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
对系统的影响	以太网OAM远端环回功能正常开启
日志产生原因	本端使能以太网OAM远端环回功能
处理建议	无需处理

33.10 ETHOAM_LOCAL_DYING_GASP

日志内容	A local Dying Gasp event occurred on interface [string].
日志含义	本端产生致命故障（Dying Gasp）事件
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_LOCAL_DYING_GASP: A local Dying Gasp event occurred on interface Ethernet1/0/1.
对系统的影响	链路down
日志产生原因	重启设备或关闭接口
处理建议	链路恢复之前不能使用

33.11 ETHOAM_LOCAL_ERROR_FRAME

日志内容	An errored frame event occurred on local interface [string].
日志含义	本地接口产生错误帧事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME: An errored frame event occurred on local interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以设定的时间为检测窗口，在窗口期内检测到的错误帧数量达到或超过了检测阈值
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

33.12 ETHOAM_LOCAL_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on local interface [string].
日志含义	本地接口产生错误帧周期事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_PERIOD: An errored frame period event occurred on local interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以收到设定数量的帧为检测窗口，在窗口期内检测到的错误帧数量达到或超过了检测阈值
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

33.13 ETHOAM_LOCAL_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on local interface [string].
日志含义	本地接口产生错误帧秒事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_SECOND: An errored frame seconds event occurred on local interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以设定的时间为检测窗口，在窗口期内检测到的错误帧秒（在某一秒内检测到至少一个错误帧，就称该秒为错误帧秒）数量达到或超过了检测阈值
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

33.14 ETHOAM_LOCAL_ERROR_SYMBOL

日志内容	An errored symbol event occurred on local interface [string].
日志含义	本端产生错误信号事件
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_LOCAL_ERROR_SYMBOL: An errored symbol event occurred on local interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以收到设定数量的信号为检测窗口，在窗口期内检测到的错误信号数量如果达到或超过了检测阈值，就产生一次错误信号事件
处理建议	本端收到错误信号，检查一下本端和对端之间的链路是否正常

33.15 ETHOAM_LOCAL_LINK_FAULT

日志内容	A local Link Fault event occurred on interface [string].
日志含义	产生本地链路故障事件
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_LOCAL_LINK_FAULT: A local Link Fault event occurred on interface Ethernet1/0/1.
对系统的影响	链路down
日志产生原因	本地接口故障
处理建议	重新连接本地接口的光纤接收端

33.16 ETHOAM_LOOPBACK_EXIT

日志内容	OAM interface [string] quit remote loopback.
日志含义	OAM接口退出远端环回
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_LOOPBACK_EXIT: OAM interface Ethernet1/0/1 quit remote loopback.
对系统的影响	远端环回连接无法建立
日志产生原因	远端环回连接建立未完成时，接口关闭远端环回或OAM连接断开
处理建议	无需处理

33.17 ETHOAM_LOOPBACK_NO_RESOURCE

日志内容	OAM interface [string] can’t enter remote loopback due to insufficient resources.
日志含义	OAM接口由于资源不足而无法进入远端环回
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_LOOPBACK_NO_RESOURCE: OAM interface Ethernet1/0/1 can’t enter remote loopback due to insufficient resources.
对系统的影响	远端环回功能无法正常使用
日志产生原因	当在本端或对端OAM实体上运行**oam remote-loopback start**命令时，OAM接口由于资源不足而无法进入远端环回
处理建议	端口上使能远端环回，需要设置端口的硬件转发资源，如果配置的端口过多，可能会导致资源不足，需要关闭一下其他端口的远端环回功能，再在本端口上重新运行**oam remote-loopback start**命令

33.18 ETHOAM_LOOPBACK_NOT_SUPPORT

日志内容	OAM interface [string] can’t enter remote loopback because the operation is not supported.
日志含义	由于设备不支持，OAM接口无法进入远端环回
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_LOOPBACK_NOT_SUPPORT: OAM interface Ethernet1/0/1 can’t enter remote loopback because the operation is not supported.
对系统的影响	远端环回功能无法正常使用
日志产生原因	设备不支持远端环回功能
处理建议	无需处理

33.19 ETHOAM_NO_ENOUGH_RESOURCE

日志内容	The configuration failed on OAM interface [string] because of insufficient resources.
日志含义	系统内存资源不足导致OAM接口上的配置失败
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ ETHOAM_NO_ENOUGH_RESOURCE: The configuration failed on OAM interface Ethernet1/0/1 because of insufficient resources.
对系统的影响	接口无法配置以太网OAM功能
日志产生原因	系统内存资源不足
处理建议	减少一下系统的无用配置，释放部分内存资源后，再重新配置

33.20 ETHOAM_NOT_CONNECTION_TIMEOUT

日志内容	Interface [string] quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
日志含义	本地端口在超时时间内没有收到信息OAMPDU，所以退出以太网OAM
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	ETHOAM/5/ ETHOAM_NOT_CONNECTION_TIMEOUT: Interface Ethernet1/0/1 quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
对系统的影响	以太网OAM连接无法建立
日志产生原因	• 链路 down • 对端的 OAM 功能没有使能
处理建议	对端发送OAM报文不及时，检查本地和对端的链路状态是否正常，以及对端的OAM功能是否使能了

33.21 ETHOAM_QUIT_LOOPBACK_CTRLLED

日志内容	The local OAM entity quit remote loopback as controlled DTE on OAM interface [string].
日志含义	当本端作为远端环回的被控端时，由于对端关闭了远端环回功能，本端也会退出远端环回
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ ETHOAM_QUIT_LOOPBACK_CTRLLED: The local OAM entity quit remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
对系统的影响	远端环回连接无法建立
日志产生原因	当本端作为远端环回的被控端时，对端关闭了远端环回功能
处理建议	无需处理

33.22 ETHOAM_QUIT_LOOPBACK_CTRLLING

日志内容	The local OAM entity quit remote loopback as controlling DTE on OAM interface [string].
日志含义	在接口上使能远端环回，当再将端口上的远端环回功能关闭后，本端会退出远端环回
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_QUIT_LOOPBACK_CONTROLLING: The local OAM entity quit remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
对系统的影响	远端环回连接无法建立
日志产生原因	在接口上使能远端环回，再将端口上的远端环回功能关闭
处理建议	无需处理

33.23 ETHOAM_REMOTE_CRITICAL

日志内容	A remote Critical event occurred on interface [string].
日志含义	发生远端紧急事件
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_REMOTE_CRITICAL: A remote Critical event occurred on interface Ethernet1/0/1.
对系统的影响	链路down
日志产生原因	发生远端紧急事件
处理建议	链路恢复之前不能使用

33.24 ETHOAM_REMOTE_DYING_GASP

日志内容	A remote Dying Gasp event occurred on interface [string].
日志含义	远端产生致命故障（Dying Gasp）事件
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_REMOTE_DYING_GASP: A remote Dying Gasp event occurred on interface Ethernet1/0/1.
对系统的影响	链路down
日志产生原因	重启远端设备或关闭接口
处理建议	链路恢复之前不能使用

33.25 ETHOAM_REMOTE_ERROR_FRAME

日志内容	An errored frame event occurred on the peer interface [string].
日志含义	对端产生错误帧事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME: An errored frame event occurred on the peer interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以设定的时间为检测窗口，在窗口期内检测到的错误帧数量达到或超过了检测阈值
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

33.26 ETHOAM_REMOTE_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on the peer interface [string].
日志含义	对端产生错误帧周期事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_PERIOD: An errored frame period event occurred on the peer interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以收到设定数量的帧为检测窗口，在窗口期内检测到的错误帧数量达到或超过了检测阈值
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

33.27 ETHOAM_REMOTE_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on the peer interface [string].
日志含义	对端产生错误帧秒事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_SECOND: An errored frame seconds event occurred on the peer interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以设定的时间为检测窗口，在窗口期内检测到的错误帧秒（在某一秒内检测到至少一个错误帧，就称该秒为错误帧秒）数量达到或超过了检测阈值
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

33.28 ETHOAM_REMOTE_ERROR_SYMBOL

日志内容	An errored symbol event occurred on the peer interface [string].
日志含义	对端产生错误信号事件
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_SYMBOL: An errored symbol event occurred on the peer interface Ethernet1/0/1.
对系统的影响	链路质量差
日志产生原因	以收到设定数量的信号为检测窗口，在窗口期内检测到的错误信号数量如果达到或超过了检测阈值
处理建议	对端收到错误信号，检查一下本端和对端之间的链路是否正常

33.29 ETHOAM_REMOTE_EXIT

日志内容	OAM interface [string] quit OAM connection because Ethernet OAM is disabled on the peer interface.
日志含义	对端接口关闭以太网OAM功能导致本端接口退出OAM连接
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	ETHOAM/5/ ETHOAM_REMOTE_EXIT: OAM interface Ethernet1/0/1 quit OAM connection because Ethernet OAM is disabled on the peer interface.
对系统的影响	以太网OAM连接无法建立
日志产生原因	对端接口关闭以太网OAM功能
处理建议	无需处理

33.30 ETHOAM_REMOTE_FAILURE_RECOVER

日志内容	Peer interface [string] recovered.
日志含义	对端接口链路故障清除，OAM连接恢复
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	ETHOAM/5/ ETHOAM_REMOTE_FAILURE_RECOVER: Peer interface Ethernet1/0/1 recovered.
对系统的影响	无
日志产生原因	对端接口链路故障清除
处理建议	无需处理

33.31 ETHOAM_REMOTE_LINK_FAULT

日志内容	A remote Link Fault event occurred on interface [string].
日志含义	产生远端链路故障事件
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ETHOAM/4/ETHOAM_REMOTE_LINK_FAULT: A remote Link Fault event occurred on interface Ethernet1/0/1.
对系统的影响	链路down
日志产生原因	远端接口故障
处理建议	重新连接远端接口的光纤接收端

34 EVB

本节介绍连接服务器的边缘交换机上 EVB 协议输出的日志信息。

34.1 EVB_AGG_FAILED

日志内容	Remove port [STRING] from aggregation group [STRING]. Otherwise, the EVB feature does not take effect.
日志含义	EVB交换机处理聚合组中物理接口失败
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	6 (Informational)
举例	EVB/6/EVB_AGG_FAILED: Remove port GigabitEthernet1/0/1 from aggregation group Bridge-Aggregation5. Otherwise, the EVB feature does not take effect.
对系统的影响	对系统无影响
日志产生原因	EVB交换机处理聚合组中物理接口失败
处理建议	将该物理接口从聚合组中删除

34.2 EVB_LICENSE_EXPIRE

日志内容	The EVB feature's license will expire in [UINT32] days.
日志含义	EVB的License将在指定天数后过期
参数解释	$1：天数
日志等级	6 (Informational)
举例	EVB/6/EVB_LICENSE_EXPIRE: The EVB feature's license will expire in 15 days.
对系统的影响	License过期后，将无法使用EVB功能
日志产生原因	EVB的License将在指定天数后失效
处理建议	安装新的EVB License

34.3 EVB_VSI_OFFLINE

日志内容	VSI [STRING] went offline.
日志含义	VSI接口/VSI聚合接口连接的终端下线
参数解释	$1：VSI接口/VSI聚合接口名称
日志等级	6 (Informational)
举例	EVB/6/EVB_VSI_OFFLINE: VSI Schannel-Aggregation1:2.0 went offline.
对系统的影响	对系统无影响
日志产生原因	设备收到服务器发送的VDP报文，或者定时器已经超时，但设备还没收到服务器的VDP回复报文，VSI接口/VSI聚合接口被删除
处理建议	无需处理

34.4 EVB_VSI_ONLINE

日志内容	VSI [STRING] came online, status is [STRING].
日志含义	VSI接口/VSI聚合接口连接的终端上线
参数解释	$1：VSI接口/VSI聚合接口名称 $2：VSI状态
日志等级	6 (Informational)
举例	EVB/6/EVB_VSI_ONLINE: VSI Schannel-Aggregation1:2.0 came online, status is association.
对系统的影响	对系统无影响
日志产生原因	EVB交换机收到VDP报文并成功创建VSI接口/VSI聚合接口
处理建议	无需处理

35 EVIISIS

本节介绍 EVI IS-IS 模块输出的日志信息。

35.1 EVIISIS_LICENSE_EXPIRED

日志内容	The EVIISIS feature is being disabled, because its license has expired.
日志含义	正在关闭EVIISIS功能，因为该功能的Licence过期
参数解释	无
日志等级	3 (Error)
举例	EVIISIS/3/EVIISIS_LICENSE_EXPIRED: The EVIISIS feature is being disabled, because its license has expired.
对系统的影响	无法使用EVIISIS功能
日志产生原因	EVIISIS的License已经过期
处理建议	请更换有效的Licence

35.2 EVIISIS_LICENSE_EXPIRED_TIME

日志内容	The EVIISIS feature will be disabled in [ULONG] days.
日志含义	距离EVIISIS的License失效的天数
参数解释	$1：功能还可使用的天数
日志等级	5 (Notification)
举例	EVIISIS/5/EVIISIS_LICENSE_EXPIRED_TIME: The EVIISIS feature will be disabled in 2 days.
对系统的影响	如果未能在License失效前准备新的License，在License失效后将无法使用EVIISIS功能。 主备倒换后新的主控板上没有可用的EVI License，会启动30天临时可用定时器。
日志产生原因	EVIISIS的License失效前产生此日志
处理建议	若要继续使用EVIISIS功能，请在有效期内安装新的License

35.3 EVIISIS_LICENSE_UNAVAILABLE

日志内容	The EVIISIS feature has no available license.
日志含义	EVIISIS无可用的License
参数解释	无
日志等级	3 (Error)
举例	EVIISIS/3/EVIISIS_LICENSE_UNAVAILABLE: The EVIISIS feature has no available license.
对系统的影响	无法使用EVIISIS功能
日志产生原因	进程启动时，没有找到EVIISIS对应的License
处理建议	请为EVIISIS安装有效的Licence

35.4 EVIISIS_NBR_CHG

日志内容	EVIISIS [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
日志含义	接口EVI IS-IS邻居状态改变
参数解释	$1：EVI IS-IS进程ID $2：邻居级别 $3：邻居的System ID $4：接口名 $5：当前邻居状态 o up：表示邻居关系已建立，可以正常工作 o initializing：表示初始状态 o down：表示邻居关系结束
日志等级	5 (Notification)
举例	EVIISIS/5/EVIISIS_NBR_CHG: EVIISIS 1, Level-1 adjacency 0011.2200.1501 (Evi-Link0), state changed to down.
对系统的影响	对系统无影响
日志产生原因	接口EVI IS-IS邻居状态改变
处理建议	当某接口邻居状态变为down或initializing时，检查EVI IS-IS配置正确性和网络连通性

36 FCLINK

本节介绍 FCLINK 模块输出的日志信息。

36.1 FCLINK_FDISC_REJECT_NORESOURCE

日志内容	VSAN [UINT16], Interface [STRING]: An FDISC was rejected because the hardware resource is not enough.
日志含义	硬件资源不足时，收到FDISC报文后，拒绝处理该报文
参数解释	$1：VSAN ID $2：接口名称
日志等级	4 (Warning)
举例	FCLINK/4/FCLINK_FDISC_REJECT_NORESOURCE: VSAN 1, Interface FC2/0/1: An FDISC was rejected because the hardware resource is not enough.
对系统的影响	节点无法登录
日志产生原因	硬件资源不足
处理建议	减少节点的数量

36.2 FCLINK_FLOGI_REJECT_NORESOURCE

日志内容	VSAN [UINT16], Interface [STRING]: An FLOGI was rejected because the hardware resource is not enough.
日志含义	硬件资源不足时，收到FLOGI报文后，拒绝处理该报文
参数解释	$1：VSAN ID $2：接口名称
日志等级	4 (Warning)
举例	FCLINK/4/FCLINK_FLOGI_REJECT_NORESOURCE: VSAN 1, Interface FC2/0/1: An FLOGI was rejected because the hardware resource is not enough.
对系统的影响	节点无法登录
日志产生原因	硬件资源不足
处理建议	减少节点的数量

37 FCOE

本节介绍 FCOE 模块输出的日志信息。

37.1 FCOE_INTERFACE_NOTSUPPORT_FCOE

日志内容	Because the aggregate interface [STRING] has been bound to a VFC interface, assigning the interface [STRING] that does not support FCoE to the aggregate interface might cause incorrect processing.
日志含义	不支持FCoE功能的接口加入到已绑定到VFC接口的聚合接口
参数解释	$1：聚合接口名称 $2：以太网接口名称
日志等级	4 (Warning)
举例	FCOE/4/FCOE_INTERFACE_NOTSUPPORT_FCOE: Because the aggregate interface Bridge-Aggregation 1 has been bound to a VFC interface, assigning the interface Ten-GigabitEthernet 2/0/1 that does not support FCoE to the aggregate interface might cause incorrect processing.
对系统的影响	如果FCoE报文被引流到此接口上，无法处理FCoE协议报文
日志产生原因	当不支持FCoE功能的接口加入到已绑定到VFC接口的聚合接口时，打印本信息
处理建议	将支持FCoE功能的接口加入到聚合接口，或者解除聚合接口与VFC接口的绑定

37.2 FCOE_LAGG_BIND_ACTIVE

日志内容	The binding between aggregate interface [STRING] and the VFC interface takes effect again, because the member port is unbound from its bound VFC interface or removed from the aggregate interface.
日志含义	因为聚合接口的成员接口解除VFC接口绑定或退出聚合组，所以聚合接口绑定的VFC接口生效
参数解释	$1：聚合接口名称
日志等级	4 (Warning)
举例	FCOE/4/FCOE_LAGG_BIND_ACTIVE: The binding between aggregate interface Bridge-Aggregation1 and the VFC interface takes effect again, because the member port is unbound from its bound VFC interface or removed from the aggregate interface.
对系统的影响	聚合接口绑定的VFC接口再次生效
日志产生原因	聚合接口的成员接口解除VFC接口绑定或退出聚合组
处理建议	*系统正常运行时产生的信息，无需处理*

37.3 FCOE_LAGG_BIND_DEACTIVE

日志内容	The binding between aggregate interface [STRING] and the VFC interface is no longer in effect, because the new member port has been bound to a VFC interface.
日志含义	因为聚合接口的成员口绑定了VFC接口，所以聚合接口绑定的VFC接口失效
参数解释	$1：聚合接口名称
日志等级	4 (Warning)
举例	FCOE/4/FCOE_LAGG_BIND_DEACTIVE: The binding between aggregate interface Bridge-Aggregation1 and the VFC interface is no longer in effect, because the new member port has been bound to a VFC interface.
对系统的影响	聚合接口绑定的VFC接口失效
日志产生原因	聚合接口的成员口绑定VFC接口
处理建议	将聚合接口的成员接口解除VFC接口绑定或退出聚合组

38 FCZONE

本节介绍 FCZONE 模块输出的日志信息。

38.1 FCZONE_DISTRIBUTE_FAILED

日志内容	-VSAN=[UINT16]; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
日志含义	扩散失败，Fabric中交换机的zone配置可能因此不一致
参数解释	$1：VSAN ID
日志等级	4 (Warning)
举例	FCZONE/4/FCZONE_DISTRIBUTE_FAILED: -VSAN=2; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
对系统的影响	会导致链路流量不通。
日志产生原因	扩散过程中报文处理异常
处理建议	不同情况下扩散失败的处理建议如下： • 如果是激活Zone set命令 **zoneset activate**触发的扩散，需要分别在Fabric中各交换机上通过 **display current-configuration**命令查看VSAN内的激活Zone set的配置，若配置不一致，则通过 **zoneset activate**命令重新激活该Zone set，以保证Fabric内所有交换机的激活Zone set的数据一致性 • 如果是完全扩散命令 **zoneset distribute**触发的扩散，需要分别在Fabric中各交换机上通过 **display current-configuration**命令查看VSAN内的激活Zone set和Zone数据库配置，若配置不一致，则通过 **zoneset distribute**命令重新激发一次完全扩散，以保证Fabric内所有交换机的Zone配置的一致性 • 如果是Zone模式切换触发的扩散，需要分别在Fabric中各交换机上通过 **display zone status**命令查看VSAN内的Zone模式，如果各交换机的Zone模式不一致，则通过 **zoneset distribute**命令来主动激发一次完全扩散，以保证Fabric内所有交换机的Zone模式的一致性

38.2 FCZONE_HARDZONE_DISABLED

日志内容	-VSAN=[UINT16]; No enough hardware resource for zone rule, switched to soft zoning.
日志含义	硬件zone资源不足，已切换成软件zone
参数解释	$1：VSAN ID
日志等级	4 (Warning)
举例	FCZONE/4/FCZONE_HARDZONE_DISABLED: -VSAN=2; No enough hardware resource for zone rule, switched to soft zoning.
对系统的影响	节点流量不能正常转发，流量不通
日志产生原因	硬件zone资源不足
处理建议	激活一个更小的zone set

38.3 FCZONE_HARDZONE_ENABLED

日志内容	-VSAN=[UINT16]; Hardware resource for zone rule is restored, switched to hard zoning.
日志含义	硬件zone资源恢复时，已切换到硬件zone
参数解释	$1：VSAN ID
日志等级	6 (Informational)
举例	FCZONE/6/FCZONE_HARDZONE_ENABLED: -VSAN=2; Hardware resource for zone rule is restored, switched to hard zoning.
对系统的影响	无
日志产生原因	硬件zone资源恢复
处理建议	系统正常运行时产生的信息，无需处理

38.4 FCZONE_ISOLATE_ALLNEIGHBOR

日志内容	-VSAN=[UINT16]; The E ports connected to all neighbors were isolated, because the length of the locally generated MR packet exceeded the limit.
日志含义	因本地生成的MR报文长度超限，隔离与所有邻居相连的E-Port
参数解释	$1：VSAN ID
日志等级	4 (Warning)
举例	FCZONE/4/FCZONE_ISOLATE_ALLNEIGHBOR: -VSAN=2; The E ports connected to all neighbors were isolated, because the length of the locally generated MR packet exceeded the limit.
对系统的影响	隔离与所有邻居相连的E-Port，E-Port状态切成down状态
日志产生原因	本地生成的MR报文长度超限
处理建议	通过**display current-configuration**命令查看本地交换机VSAN内的Zone配置，删除Zone set中不必要的配置，或重新激活一个较小的Zone set。然后，对因MR报文超大导致隔离的E-Port配置**shutdown**和**undo shutdown**命令，触发重新发起合并

38.5 FCZONE_ISOLATE_CLEAR_ALLVSAN

日志内容	-Interface=[STRING]; Isolation status was cleared in all supported VSANs.
日志含义	接口在所有支持的VSAN内去隔离
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	FCZONE/6/FCZONE_ISOLATE_CLEAR_ALLVSAN: -Interface=Fc1/0/1; Isolation status was cleared in all supported VSANs.
对系统的影响	接口在所有vsan重新协商使用
日志产生原因	接口链路层up
处理建议	系统正常运行时产生的信息，无需处理

38.6 FCZONE_ISOLATE_CLEAR_VSAN

日志内容	-Interface=[STRING]-VSAN=[UINT16]; Isolation status was cleared.
日志含义	接口在指定VSAN内去隔离
参数解释	$1：接口名称 $2：VSAN ID
日志等级	6 (Informational)
举例	FCZONE/6/FCZONE_ISOLATE_CLEAR_VSAN: -Interface=Fc1/0/1-VSAN=2; Isolation status was cleared.
对系统的影响	接口在指定vsan重新协商使用
日志产生原因	接口链路层up
处理建议	系统正常运行时产生的信息，无需处理

38.7 FCZONE_ISOLATE_NEIGHBOR

日志内容	-VSAN=[UINT16]; All the E ports connected to a neighbor were isolated because of merge failure, and the neighbor's switch WWN is [STRING].
日志含义	因与邻居交换机合并失败，隔离与该邻居相连的所有E-Port
参数解释	$1：VSAN ID $2：交换机WWN
日志等级	4 (Warning)
举例	FCZONE/4/FCZONE_ISOLATE_NEIGHBOR: -VSAN=2; All the E ports connected to a neighbor were isolated because of merge failure, and the neighbor's switch WWN is 10:00:00:11:22:00:0d:01.
对系统的影响	E-Port 链路层down
日志产生原因	与邻居交换机合并失败
处理建议	分别在本地和邻居交换机上通过**display current-configuration**命令查看VSAN内的Zone配置，并修改配置使其符合合并规则。然后，对因合并失败导致隔离的E-Port配置**shutdown**和**undo shutdown**命令触发两台交换机重新发起合并

39 FGROUP

本节介绍 Flow Group 模块输出的日志信息。

39.1 FLOWGROUP_APPLY_FAIL

日志内容	Failed to apply flow group [STRING]. Reason: [STRING]
日志含义	应用Flow Group失败
参数解释	$1：Flow Group的ID $2：失败原因 • The operation is not supported.：操作不支持 • Not enough resources to complete the operation.：资源不足
日志等级	4 (Warning)
举例	FGROUP/4/FLOWGROUP_APPLY_FAIL: Failed to apply flow group 1. Reason: The operation is not supported.
对系统的影响	应用Flow Group失败
日志产生原因	• 不支持配置，导致应用 Flow Group 失败 • 资源不足，导致应用 Flow Group 失败
处理建议	如果是资源不足的问题，建议检查并删除设备上不必要的配置，以节约资源 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

39.2 FLOWGROUP_MODIFY_FAIL

日志内容	Failed to modify flow group [STRING]. Reason: [STRING]
日志含义	修改Flow Group失败
参数解释	$1：Flow Group的ID $2：失败原因 • The operation is not supported.：操作不支持 • Not enough resources to complete the operation.：资源不足
日志等级	4 (Warning)
举例	FGROUP/4/FLOWGROUP_MODIFY_FAIL: Failed to modify flow group 1. Reason: The operation is not supported.
对系统的影响	修改Flow Group失败
日志产生原因	• 不支持配置，导致修改 Flow Group 失败 • 资源不足，导致修改 Flow Group 失败
处理建议	如果是资源不足的问题，建议检查并删除设备上不必要的配置，以节约资源 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

40 FIB

本节包含 FIB 日志消息。

40.1 FIB_FILE

日志内容	Failed to save the IP forwarding table due to lack of storage resources.
日志含义	因存储空间不足导致保存FIB失败
参数解释	无
日志等级	4 (Warning)
举例	FIB/4/FIB_FILE: -MDC=1; Failed to save the IP forwarding table due to lack of storage resources.
对系统的影响	若无法保存新生成的FIB表项，业务可能出现故障
日志产生原因	存储介质剩余空间不足，保存IP FIB信息失败
处理建议	删除存储介质中其它无用文件，释放存储介质的存储空间

40.2 FIB_PREFIX_ENOUGHRESOURCE

日志内容	Issued the software entry to the driver for IP address [STRING] and mask length

	[UINT32] on VPN instance [STRING]. Issued the software entry to the driver for IP address [STRING] and mask length [UINT32] on the public network.
日志含义	FIB软件表项与硬件表项一致
参数解释	$1：IPv4地址或者IPv6地址 $2：掩码长度或者前缀长度 $3：VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6 (Informational)
举例	FIB/6/FIB_PREFIX_ENOUGHRESOURCE: Issued the software entry to the driver for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_PREFIX_ENOUGHRESOURCE: Issued the software entry to the driver for IP address 10::2 and mask length 128 on the public network.
对系统的影响	无
日志产生原因	使用**fib consistency-check enable**命令开启IPv4 FIB表项一致性检查功能，或者使用**ipv6 fib consistency-check enable**命令开启IPv6 FIB表项一致性检查功能后，如果FIB重刷硬件表项成功，则输出此日志
处理建议	无需处理

40.3 FIB_PREFIX_INCONSISTENT

日志内容	Inconsistent software and hardware FIB entries for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Inconsistent parameters: [STRING]. Inconsistent software and hardware FIB entries for IP address [STRING] and mask length [UINT32] on the public network. Inconsistent parameters: [STRING].
日志含义	FIB软件表项与硬件表项不一致
参数解释	$1：IPv4地址或IPv6地址 $2：掩码长度或者前缀长度 $3：VPN实例名。如果该FIB属于公网，该字段不显示 $4：不一致的表项参数类型 o next hop：下一跳地址 o mpls label：MPLS 标签 o adjacent-table：邻接表 o micro-segment ID：微分段 ID
日志等级	6 (Informational)
举例	FIB/6/FIB_PREFIX_INCONSISTENT: Inconsistent software and hardware FIB entries for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. Inconsistent parameters: next hop, mpls label, adjacent-table and micro-segment ID. FIB/6/FIB_PREFIX_INCONSISTENT: Inconsistent software and hardware FIB entries for IP address 10::2 and mask length 128 on the public network. Inconsistent parameters: next hop, mpls label, adjacent-table and micro-segment ID.
对系统的影响	无
日志产生原因	使用**fib consistency-check enable**命令开启IPv4 FIB表项一致性检查功能，或者**ipv6 fib consistency-check enable**开启IPv6 FIB表项一致性检查功能后，如果设备检测到FIB软件表项与硬件表项不一致（比如FIB表项的下一跳地址），则输出本日志
处理建议	不需要处理，FIB会主动重刷硬件表项

40.4 FIB_PREFIX_NORESOURCE

日志内容	Not enough hardware resources to issue the software entry to the driver for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Not enough hardware resources to issue the software entry to the driver for IP address [STRING] and mask length [UINT32] on the public network.
日志含义	驱动没有足够的FIB硬件表项资源
参数解释	$1：IPv4地址或者IPv6地址 $2：掩码长度或者前缀长度 $3：VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6 (Informational)
举例	FIB/6/FIB_PREFIX_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_PREFIX_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IP address 10::2 and mask length 128 on the public network.
对系统的影响	无
日志产生原因	使用**fib consistency-check enable**命令开启IPv4 FIB表项一致性检查功能，或者**ipv6 fib consistency-check enable**开启IPv6 FIB表项一致性检查功能后，当FIB软件表项下发驱动时，驱动没有足够的FIB硬件表项资源，则输出此日志
处理建议	不需要处理，FIB会主动重刷硬件表项

40.5 FIB_VN_ENOUGHRESOURCE

日志内容	Issued the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Issued the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on the public network.
日志含义	FIB虚拟下一跳软件表项与硬件表项一致
参数解释	$1：FIB表项数量 $2：IPv4地址或者IPv6地址 $3：掩码长度或者前缀长度 $4：VPN实例名。如果该FIB属于公网，该字段不显示。
日志等级	6 (Informational)
举例	FIB/6/FIB_VN_ENOUGHRESOURCE: Issued the following 1 software FIB entries to the driver: Entry for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_PREFIX_ENOUGHRESOURCE: Issued the following 1 software FIB entries to the driver: Entry for IP address 10::2 and mask length 128 on the public network.
对系统的影响	无
日志产生原因	使用**fib consistency-check enable**命令开启IPv4 FIB表项一致性检查功能，或者**ipv6 fib consistency-check enable**开启IPv6 FIB表项一致性检查功能后，如果虚拟下一跳表项重刷硬件表项成功，则输出此日志，提示用户哪些FIB表项恢复
处理建议	无需处理

40.6 FIB_VN_INCONSISTENT

日志内容	Inconsistent software and hardware entries for the following [UINT32] FIB entries. Inconsistent parameters: [STRING]. Entry for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Inconsistent software and hardware entries for the following [UINT32] FIB entries. Inconsistent parameters: [STRING]. Entry for IP address [STRING] and mask length [UINT32] on the public network.
日志含义	FIB虚拟下一跳软件表项与硬件表项不一致
参数解释	$1：FIB表项个数 $2：不一致的表项参数类型 ○ next hop：下一跳地址 ○ mpls label：MPLS 标签 ○ max ECMP number：最大等价路由条数 ○ output tunnel interface：隧道出接口 $3：IPv4地址或者IPv6地址 $4：掩码长度或者前缀长度 $5：VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6 (Informational)
举例	FIB/6/FIB_VN_INCONSISTENT: Inconsistent software and hardware entries for the following 1 FIB entries. Inconsistent parameters: next hop and mpls label. Entry for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_VN_INCONSISTENT: Inconsistent software and hardware entries for the following 1 FIB entries. Inconsistent parameters: next hop and mpls label. Entry for IP address 10::2 and mask length 128 on the public network.
对系统的影响	无
日志产生原因	使用**fib consistency-check enable**命令开启IPv4 FIB表项一致性检查功能，或者**ipv6 fib consistency-check enable**开启IPv6 FIB表项一致性检查功能后，如果设备检测到FIB虚拟下一跳软件表项与硬件表项不一致（比如FIB虚拟下一跳表项的下一跳地址），则输出本日志，提示用户哪些FIB表项失效
处理建议	不需要处理，FIB会主动重刷硬件表项

40.7 FIB_VN_NORESOURCE

日志内容	Not enough hardware resources to issue the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Not enough hardware resources to issue the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on the public network.
日志含义	驱动没有足够的FIB虚拟下一跳硬件表项资源
参数解释	$1：FIB表项数量 $2：IPv4地址或者IPv6地址 $3：掩码长度或者前缀长度 $4：VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6 (Informational)
举例	FIB/6/FIB_VN_NORESOURCE: Not enough hardware resources to issue the following 1 software FIB entries to the driver: Entry for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_VN_NORESOURCE: Not enough hardware resources to issue the following 1 software FIB entries to the driver: Entry for IP address 10::2 and mask length 128 on the public network.
对系统的影响	无
日志产生原因	使用**fib consistency-check enable**命令开启IPv4 FIB表项一致性检查功能，或者**ipv6 fib consistency-check enable**开启IPv6 FIB表项一致性检查功能后，当虚拟下一跳软件表项下发驱动时，如果驱动没有足够的硬件表项资源，则输出此日志，提示用户哪些FIB表项失效
处理建议	不需要处理，FIB会主动重刷硬件表项

41 FILTER

本节介绍 FILTER 模块输出的日志信息。

41.1 FILTER_EXECUTION_ICMP

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];IcmpType(1062)=[STRING]([UINT16]);IcmpCode(1063)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
日志含义	接口上接收到ICMP报文，且ICMP报文命中报文过滤规则
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IP地址 $7：目的IP地址 $8：ICMP类型 $9：ICMP代码 $10：命中次数 $11：事件信息
日志等级	6 (Informational)
举例	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;Acl(1068)=3000;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1062)=ECHO(8);IcmpCode(1063)=0;MatchAclCount(1069)=1000;Event(1048)=Permit;
对系统的影响	对系统无影响
日志产生原因	当接口上应用了报文过滤规则，并且执行了**acl logging interval**命令配置报文过滤日志信息的生成与发送周期时，ICMP报文首次命中报文过滤规则时产生日志，之后按**acl logging interval**命令配置的日志信息的生成与发送周期发送该日志
处理建议	系统正常运行时产生的信息，无需处理

41.2 FILTER_EXECUTION_ICMPV6

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];Icmpv6Type(1064)=[STRING]([UINT16]);Icmpv6Code(1065)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
日志含义	接口上接收到ICMPv6报文，且ICMPv6报文命中报文过滤规则
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IPv6地址 $7：目的IPv6地址 $8：ICMPV6类型 $9：ICMPV6代码 $10：命中次数 $11：事件信息
日志等级	6 (Informational)
举例	FILTER/6/FILTER_EXECUTION_ICMPV6: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL6;Acl(1068)=3000;Protocol(1001)=IPv6-ICMP;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;Icmpv6Type(1064)=ECHO_REQUEST(128);Icmpv6Code(1065)=0;MatchAclCount(1069)=1000;Event(1048)=Permit;
对系统的影响	对系统无影响
日志产生原因	当接口上应用了报文过滤规则，并且执行了**acl logging interval**命令配置报文过滤日志信息的生成与发送周期时，ICMPv6报文首次命中报文过滤规则时产生日志，之后按**acl logging interval**命令配置的日志信息的生成与发送周期发送该日志
处理建议	系统正常运行时产生的信息，无需处理

41.3 FILTER_IPV4_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
日志含义	接口上接收到IPv4报文，且IPv4报文命中报文过滤规则
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：命中次数 $11：事件信息
日志等级	6 (Informational)
举例	FILTER/6/FILTER_IPV4_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;Acl(1068)=3000;Protocol(1001)=TCP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchAclCount(1069)=1000;Event(1048)=Permit;
对系统的影响	对系统无影响
日志产生原因	当接口上应用了报文过滤规则，并且执行了**acl logging interval**命令配置报文过滤日志信息的生成与发送周期时，IPv4报文首次命中报文过滤规则时产生日志，之后按**acl logging interval**命令配置的日志信息的生成与发送周期发送该日志
处理建议	系统正常运行时产生的信息，无需处理

41.4 FILTER_IPV6_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
日志含义	接口上接收到IPv6报文，且IPv6报文命中报文过滤规则
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：命中次数 $11：事件信息
日志等级	6 (Informational)
举例	FILTER/6/FILTER_IPV6_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL6;Acl(1068)=3000;Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3001::1;DstPort(1008)=1026;MatchAclCount(1069)=1000;Event(1048)=Permit;
对系统的影响	对系统无影响
日志产生原因	当接口上应用了报文过滤规则，并且执行了**acl logging interval**命令配置报文过滤日志信息的生成与发送周期时，IPv6报文首次命中报文过滤规则时产生日志，之后按**acl logging interval**命令配置的日志信息的生成与发送周期发送该日志
处理建议	系统正常运行时产生的信息，无需处理

42 FIPSNG

本节介绍 FIP Snooping 模块输出的日志信息。

42.1 FIPSNG_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for FIP snooping rule.
日志含义	Snooping规则的硬件资源不足
参数解释	N/A
日志等级	4 (Warning)
举例	FIPSNG/4/FIPSNG_HARD_RESOURCE_NOENOUGH: No enough hardware resource for FIP snooping rule.
对系统的影响	Snooping规则下发不到驱动，流量不通
日志产生原因	Snooping规则的硬件资源不足
处理建议	无需处理

42.2 FIPSNG_HARD_RESOURCE_RESTORE

日志内容	Hardware resource for FIP snooping rule is restored.
日志含义	Snooping规则的硬件资源恢复
参数解释	N/A
日志等级	6 (Informational)
举例	FIPSNG/6/FIPSNG_HARD_RESOURCE_RESTORE: Hardware resource for FIP snooping rule is restored.
对系统的影响	无
日志产生原因	Snooping规则的硬件资源恢复
处理建议	系统正常运行时产生的信息，无需处理

43 FS

本节介绍 FS（File System）模块输出的日志信息。

43.1 FS_UNFORMATTED_PARTITION

日志内容	Partition [STRING] is not formatted yet. Please format the partition first.
日志含义	未格式化分区
参数解释	$1：分区名
日志等级	4 (Warning)
举例	FS/4/FS_UNFORMATED_PARTITION: Partition usba0: is not formatted yet. Please format the partition first.
对系统的影响	可能导致存储介质读写失败
日志产生原因	分区未格式化，请先执行格式化操作
处理建议	格式化该分区

44 FTP

本节介绍 FTP（File Transfer Protocol）模块输出的日志信息。

44.1 FTP_ACL_DENY

日志内容	The FTP Connection [IPADDR]([STRING]) request was denied according to ACL rules.
日志含义	FTP ACL规则限制登录IP地址
参数解释	$1：FTP客户端IP地址 $2：FTP客户端IP地址所在VPN
日志等级	5 (Notification)
举例	FTP/5/FTP_ACL_DENY: The FTP Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
对系统的影响	系统可能受到攻击
日志产生原因	FTP ACL规则限制登录IP地址。该日志在FTP服务端检测到非法客户端尝试登录时输出
处理建议	联系技术支持工程师查看ACL规则，保证该FTP连接符合该ACL访问规则

44.2 FTPD_AUTHOR_FAILED

日志内容	Authorization failed for user [STRING]@[STRING].
日志含义	FTP登录用户授权失败
参数解释	$1：用户名 $2：用户IP地址
日志等级	4 (Warning)
举例	FTP/4/FTPD_AUTHOR_FAILED: Authorization failed for user admin@10.11.115.63.
对系统的影响	FTP登录用户无法正常访问系统
日志产生原因	该FTP用户无法获取授权
处理建议	请检查是否配置该用户支持FTP服务

44.3 FTP_REACH_SESSION_LIMIT

日志内容	FTP client [STRING] failed to log in. The current number of FTP sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
日志含义	FTP登录用户数达到上限，登录失败
参数解释	$1：FTP客户端IP地址 $2：当前的FTP会话数 $3：设备允许建立的FTP会话数
日志等级	6 (Informational)
举例	FTP/6/FTP_REACH_SESSION_LIMIT: FTP client 1.1.1.1 failed to log in. The current number of FTP sessions is 10. The maximum number allowed is (10).
对系统的影响	FTP登录用户无法正常访问系统
日志产生原因	该日志在FTP服务端检测到登录客户端数达到上限时输出
处理建议	• 请使用 **display current-configuration | include sesion-limit**命令查看设备当前允许的FTP最大登录用户数（如果执行该 **display**命令后没有显示，则表示使用的是缺省配置） • 根据需要使用 **aaa session-limit**命令配置允许的FTP最大登录用户数

45 gRPC

本节介绍 gRPC 模块输出的日志信息。

45.1 GRPC_LOGIN

日志内容	[STRING] logged in from [STRING], session id [INT32].
日志含义	用户登录成功
参数解释	$1：用户名 $2：客户端地址，包含IP协议版本、IP地址和端口号 $3：会话ID
日志等级	6 (Informational)
举例	GRPC/6/GRPC_LOGIN: user logged in from ipv4:192.168.56.99:41996, session id 1.
对系统的影响	无
日志产生原因	用户登录成功
处理建议	无需处理

45.2 GRPC_LOGIN_FAILED

日志内容	[STRING] from [STRING] login failed. 或 [STRING] from [STRING] login failed. [STRING]
日志含义	用户登录失败
参数解释	$1：用户名 $2：客户端地址，包含IP协议版本、IP地址和端口号 $3：失败原因，取值为Number of the gRPC sessions reached the limit.
日志等级	6 (Informational)
举例	GRPC/6/GRPC_LOGIN_FAILED: admin1 from ipv4:192.168.70.10:53254 login failed.
对系统的影响	如果gRPC会话数量已达到上限，则新用户（gRPC客户端）无法登录设备
日志产生原因	用户登录失败
处理建议	• 如果未显示失败原因，请检查是否已配置用户，以及用户名和密码是否正确 • 如果显示 gRPC 会话到达数量上限，请减少 gRPC 客户端连接数

45.3 GRPC_LOGOUT

日志内容	[STRING] logged out, Session id [INT32].
日志含义	用户退出登录
参数解释	$1：用户名 $2：会话ID
日志等级	6 (Informational)
举例	GRPC/6/GRPC_LOGOUT: user logged out, Session id 1.
对系统的影响	无
日志产生原因	用户正常退出登录
处理建议	无需处理

45.4 GRPC_SERVER_FAILED

日志内容	Failed to enable gRPC server.
日志含义	gRPC服务启动失败
参数解释	无
日志等级	4 (Warning)
举例	GRPC/4/GRPC_SERVER_FAILED: Failed to enable gRPC server.
对系统的影响	gRPC服务不可用
日志产生原因	gRPC服务的缺省监听端口号为50051，如果该端口号被其他服务占用，则gRPC服务启动失败
处理建议	1. 使用 **grpc port**命令修改gRPC服务的端口号 2. 若问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

45.5 GRPC_SERVICE_STOP

日志内容	gRPC service stopped. Reason: CPU usage threshold has been exceeded.
日志含义	由于gRPC的CPU占用率超过阈值，gRPC服务中止
参数解释	无
日志等级	6 (Informational)
举例	GRPC/6/GRPC_SERVICE_STOP: gRPC service stopped. Reason: CPU usage threshold has been exceeded.
对系统的影响	gRPC服务中止
日志产生原因	由于gRPC的CPU占用率超过**grpc cpu-usage max-percent**命令的配置值，采样中止
处理建议	减少配置的采样路径数量，或者增大采样周期。CPU占用率降低后，gRPC会继续采样

45.6 GRPC_SERVICE_RECOVER

日志内容	gRPC service recovered.
日志含义	gRPC服务恢复
参数解释	无
日志等级	6 (Informational)
举例	GRPC/6/GRPC_SERVICE_RECOVER: gRPC service recovered.
对系统的影响	无
日志产生原因	gRPC的CPU占用率已经等于或低于**grpc cpu-usage max-percent**命令的配置值，采样恢复
处理建议	无需处理

45.7 GRPC_SUBSCRIBE_EVENT_FAILED

日志内容	Failed to subscribe event [STRING].
日志含义	订阅事件失败
参数解释	$1：事件名
日志等级	4 (Warning)
举例	GRPC/4/GRPC_SUBSCRIBE_EVENT_FAILED: Failed to subscribe event syslog.
对系统的影响	系统不能正常推送订阅事件
日志产生原因	可能原因：订阅信息对应的业务进程未启动
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

45.8 GRPC_RECEIVE_SUBSCRIPTION

日志内容	Received a subscription of module [STRING].
日志含义	设备收到某个模块的一个订阅事件
参数解释	$1：模块名
日志等级	6 (Informational)
举例	GRPC/6/GRPC_RECEIVE_SUBSCRIPTION: Received a subscription of module syslog.
对系统的影响	无
日志产生原因	设备收到某个模块的一个订阅事件
处理建议	无需处理

46 HA

本节介绍 HA 模块输出的日志信息。

46.1 HA_BATCHBACKUP_FINISHED

日志内容	Batch backup of standby board in [STRING] has finished.
日志含义	主控板间的批量备份完成
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	5 (Notification)
举例	HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 has finished.
对系统的影响	对系统无影响
日志产生原因	全局主用主控板上的配置和运行数据批量备份到全局备用主控板完成
处理建议	无需处理

46.2 HA_BATCHBACKUP_STARTED

日志内容	Batch backup of standby board in [STRING] started.
日志含义	主控板间的批量备份开始
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	5 (Notification)
举例	HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 started.
对系统的影响	对系统无影响
日志产生原因	全局主用主控板开始将配置和运行数据批量备份到全局备用主控板
处理建议	无需处理

46.3 HA_STANDBY_NOT_READY

日志内容	Standby board in [STRING] is not ready, reboot ...
日志含义	设备进行主备倒换时，备用主控板未准备好。设备正在尝试重启备用主控板，来恢复备用主控板
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	4 (Warning)
举例	HA/4/HA_STANDBY_NOT_READY: Standby board in slot 1 is not ready, reboot ...
对系统的影响	备用slot/CPU重启，设备无法进行主用主控板和备用主控板之间的主备倒换
日志产生原因	备用主控板可能正在启动中 备用主控板可能故障
处理建议	**1.** 预防措施。在执行主备倒换之前： ○ 请执行 **display device**命令查看单板状态。如果单板状态取值为Master或者Standby，则表示单板运行正常；如果显示为Normal，单板可能正在启动中，请稍后；如果显示为其它值，请根据显示信息先处理单板故障 ○ 请执行 **display system stable state**命令查看系统的稳定状态。如果System state字段的取值不是Stable，请不要进行ISSU升级和主备倒换 **2.** 善后措施。备用主控板重启后，执行 **display device**命令查看单板状态。如果单板状态取值为Master或者Standby，则表示单板运行正常；如果显示为Normal，单板可能正在启动中，请稍后；如果显示为其它值，请联系技术支持

46.4 HA_STANDBY_TO_MASTER

日志内容	Standby board in [STRING] changed to master.
日志含义	备用主控板角色变成主用主控板
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	4 (Warning)
举例	HA/4/HA_STANDBY_TO_MASTER: Standby board in slot 1 changed to master.
对系统的影响	对系统无影响
日志产生原因	发生主备倒换，备用slot/CPU成为主用slot/CPU
处理建议	无需处理

47 HLTH

本节介绍 HLTH（Health，健康检测）模块输出的日志信息。

47.1 LIPC_COMM_FAULTY

日志内容	LIPC [STRING] between [STRING] and [STRING] might be faulty.
日志含义	指定单板之间LIPC通信异常
参数解释	$1：通信类型，取值包括： • unicast：表示单播 • broadcast：表示广播 • topo：表示拓扑 $2：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号 $3：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号
日志等级	4 (Warning)
举例	HLTH/4/LIPC_COMM_FAULTY: LIPC unicast between slot 1 and slot 2 might be faulty.
对系统的影响	单板之间的业务受影响
日志产生原因	系统检测到两个单板之间存在LIPC通信异常时，打印该日志
处理建议	执行**display system health**命令查看设备的健康状态，如果30分钟后设备仍处于故障状态，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

47.2 LIPC_COMM_RECOVER

日志内容	LIPC [STRING] between [STRING] and [STRING] recovered.
日志含义	指定单板之间LIPC通信恢复正常
参数解释	$1：通信类型，取值包括： • unicast：表示单播 • broadcast：表示广播 • topo：表示拓扑 $2：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号 $3：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号
日志等级	6 (Informational)
举例	HLTH/6/LIPC_COMM_NORMAL: LIPC unicast between slot 1 and slot 2 recovered.
对系统的影响	对系统无影响
日志产生原因	指定单板之间LIPC通信恢复正常时，打印该日志
处理建议	无需处理

48 HQOS

本节介绍 HQOS（Hierarchical QoS）模块输出的日志信息。

48.1 HQOS_DP_SET_FAIL

日志内容	Failed to set drop profile [STRING] globally.
日志含义	修改或配置丢弃策略失败
参数解释	$1：丢弃策略的名称
日志等级	4 (Warning)
举例	HQOS/4/HQOS_DP_SET_FAIL: Failed to set drop profile b globally.
对系统的影响	拥塞时该丢弃策略不生效
日志产生原因	首次应用全局丢弃策略或者修改全局丢弃策略时失败
处理建议	1. 请检查丢弃策略配置，确保支持并且策略不冲突 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

48.2 HQOS_FP_SET_FAIL

日志内容	Failed to set [STRING] in forwarding profile [STRING] globally.
日志含义	修改或配置转发策略失败
参数解释	$1：转发策略类型，取值包括： ○ gts ○ bandwidth ○ queue ○ drop profile $2：转发策略的名称
日志等级	4 (Warning)
举例	HQOS/4/HQOS_FP_SET_FAIL: Failed to set gts in forwarding profile b globally.
对系统的影响	转发策略不生效
日志产生原因	首次应用全局转发策略或者修改全局转发策略时失败
处理建议	**1.** 请检查转发策略，确保支持并且策略不冲突 **2.** 如果配置的策略不存在冲突，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

48.3 HQOS_POLICY_APPLY_FAIL

日志内容	Failed to apply some forwarding classes or forwarding groups in scheduler policy [STRING] to the [STRING] direction of interface [STRING].
日志含义	接口上应用调度策略失败
参数解释	$1：调度策略的名称 $2：调度策略应用的方向，取值包括： o inbound o outbound $3：接口名称
日志等级	4 (Warning)
举例	HQOS/4/HQOS_POLICY_APPLY_FAIL: Failed to apply some forwarding classes or forwarding groups in scheduler policy b to the inbound direction of interface Ethernet3/1/2.
对系统的影响	接口上应用的调度策略不生效
日志产生原因	接口上应用调度策略失败，或者修改接口上已应用的调度策略
处理建议	通过命令行**display qos scheduler-policy diagnosis interface**查看失败的转发节点以及失败原因，之后检查运行配置 下发未完全成功时显示下发失败的部分，接口上应用调度策略失败的原因包括： • Insufficient resources：表示硬件资源不足，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 • Conflicting match rule：match 规则类型冲突，请修改匹配规则配置 • Not support：配置不支持，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 • GTS Failed：表示转发类/转发组整形参数下发失败，请修改流量整形参数，重新配置后下发调度策略 • WRED Failed：表示转发类/转发组随机丢弃参数下发失败，请修改丢弃策略中的参数配置，重新下发调度策略 • Queue Failed：表示转发类/转发组的队列调度下发失败，请修改队列调度方式，重新下发调度策略 • Bandwidth Failed：表示转发类/转发组最小带宽保证下发失败，请修改转发策略的最小带宽保证，重新下发调度策略

48.4 HQOS_POLICY_RECOVER_FAIL

日志内容	Failed to recover scheduler policy [STRING] to the [STRING] direction of interface [STRING] due to [STRING].
日志含义	重启后接口上应用调度策略失败
参数解释	$1：调度策略的名称 $2：调度策略应用的方向，取值包括： o inbound o outbound $3：接口名称 $4：失败原因，取值包括： o conflicting with QoS configuration o conflicting with exclusive bandwidth configuration o conflicting with channel bandwidth configuration o conflicting with network slicing configuration o lack of hardware resources o not support
日志等级	4 (Warning)
举例	HQOS/4/HQOS_POLICY_RECOVER_FAIL: Failed to recover scheduler policy b to the outbound direction of interface Ethernet3/1/2 due to conflicting with QoS configuration.
对系统的影响	接口上应用的调度策略不生效
日志产生原因	接口板重启或设备重启，恢复接口上应用的调度策略失败
处理建议	请根据失败原因检查配置，失败原因包括： • conflicting with QoS configuration：调度策略与同一接口下的已存在 QoS 功能冲突，例如 WRED，CBQ 和 GTS 等功能，请删除该接口下的 QoS 配置 • conflicting with exclusive bandwidth configuration：调度策略与同一接口下的接口独占带宽功能冲突，请删除该接口下的接口独占带宽功能 • conflicting with channel bandwidth configuration：调度策略与子接口切片功能冲突，请删除该接口下的子接口切片功能 • conflicting with network slicing configuration：调度策略与 Slice ID 网络切片功能冲突，请删除该接口下的 Slice ID 网络切片功能 • lack of hardware resources：硬件资源不足，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 • not support：调度策略功能不支持，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

49 HTTPD

本节介绍 HTTPD（HTTP daemon）模块输出的日志信息。

49.1 HTTPD_CONNECT

日志内容	[STRING] client [STRING] connected to the server successfully.
日志含义	HTTP/HTTPS客户端与服务器成功建立连接
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6 (Informational)
举例	HTTPD/6/HTTPD_CONNECT: HTTP client 192.168.30.117 connected to the server successfully.
对系统的影响	无
日志产生原因	HTTP/HTTPS服务器接受了客户端的请求，HTTP/HTTPS连接成功建立
处理建议	系统正常运行时产生的信息，无需处理

49.2 HTTPD_CONNECT_TIMEOUT

日志内容	[STRING] client [STRING] connection idle timeout.
日志含义	HTTP/HTTPS连接超时
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6 (Informational)
举例	HTTPD/6/HTTPD_CONNECT_TIMEOUT: HTTP client 192.168.30.117 connection idle timeout.
对系统的影响	无
日志产生原因	HTTP/HTTPS连接因空闲时间太长而断开
处理建议	系统正常运行时产生的信息，无需处理

49.3 HTTPD_DISCONNECT

日志内容	[STRING] client [STRING] disconnected from the server.
日志含义	HTTP/HTTPS客户端与服务器断开连接
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6 (Informational)
举例	HTTPD/6/HTTPD_DISCONNECT: HTTP client 192.168.30.117 disconnected from the server.
对系统的影响	无
日志产生原因	HTTP/HTTPS 客户端断开了到服务器的连接
处理建议	系统正常运行时产生的信息，无需处理

49.4 HTTPD_FAIL_FOR_ACL

日志内容	[STRING] client [STRING] failed the ACL check and could not connect to the server.
日志含义	ACL规则限制Web用户登录
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6 (Informational)
举例	HTTPD/6/HTTPD_FAIL_FOR_ACL: HTTP client 192.168.30.117 failed the ACL check and could not connect to the server.
对系统的影响	系统可能受到攻击
日志产生原因	HTTP/HTTPS客户端没有通过ACL检查，无法建立连接
处理建议	联系技术支持工程师查看ACL规则，保证该HTTP/HTTPS连接符合该ACL访问规则

49.5 HTTPD_FAIL_FOR_ACP

日志内容	[STRING] client [STRING] was denied by the certificate access control policy and could not connect to the server.
日志含义	证书属性访问控制策略限制Web用户登录
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6 (Informational)
举例	HTTPD/6/HTTPD_FAIL_FOR_ACP: HTTP client 192.168.30.117 was denied by the certificate access control policy and could not connect to the server.
对系统的影响	系统可能受到攻击
日志产生原因	HTTP/HTTPS客户端没有通过证书接入控制策略检查，无法建立连接
处理建议	联系技术支持工程师查看证书属性访问控制策略，保证该HTTP/HTTPS连接符合该访问控制策略

49.6 HTTPD_REACH_CONNECT_LIMIT

日志内容	[STRING] client [STRING] failed to connect to the server, because the number of connections reached the upper limit.
日志含义	HTTP/HTTPS连接已达到上限，无法与服务器建立新的连接
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6 (Informational)
举例	HTTPD/6/HTTPD_REACH_CONNECT_LIMIT: HTTP client 192.168.30.117 failed to connect to the server, because the number of connections reached the upper limit.
对系统的影响	Web用户无法正常登录
日志产生原因	已达到最大连接数，无法建立新的连接
处理建议	• 请使用**display current-configuration | include sesion-limit**命令查看设备当前允许的Web最大登录用户数（如果执行该**display**命令后没有显示，则表示使用的是缺省配置） • 请根据需要使用命令**aaa session-limit**配置允许的Web最大登录用户数

50 IFMON

本节介绍接口告警模块输出的日志信息。

50.1 BGTRAFFIC_SEND_BEGIN

日志内容	Interface [STRING] began sending background traffic.
日志含义	接口开始发送背景流量
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	IFMON/6/BGTRAFFIC_SEND_BEGIN: Interface GigabitEthernet1/0/1 began sending background traffic.
对系统的影响	无
日志产生原因	接口出方向业务流量不足100Mbps时，接口开始发送背景流量
处理建议	无需处理

50.2 BGTRAFFIC_SEND_END

日志内容	Interface [STRING] stopped sending background traffic.
日志含义	接口停止发送背景流量
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	IFMON/6/BGTRAFFIC_SEND_END: Interface GigabitEthernet1/0/1 stopped sending background traffic.
对系统的影响	无
日志产生原因	接口出方向业务流量大于300Mbps时，接口停止发送背景流量
处理建议	无需处理

50.3 CRC_ERROR_RECOVERY

日志内容	Number of CRC error packets recovered to normal.
日志含义	CRC比特错误的报文数量低于下限阈值
参数解释	无
日志等级	4 (Warning)
举例	IFMON/4/CRC_ERROR_RECOVERY: Number of CRC error packets recovered to normal.
对系统的影响	无
日志产生原因	在单位统计周期中，CRC的错误报文数量低于下限阈值时会产生该日志，表示解除告警
处理建议	无需处理

50.4 CRC_ERROR_THRESHOLD

日志内容	Number of CRC error packets exceeded the high threshold: Interface Name=[STRING], High threshold=[UINT32], Number of CRC error packets=[UINT64], Interval=[UINT32]s.
日志含义	CRC比特错误的报文数量高于上限阈值
参数解释	$1：接口名称 $2：告警上限阈值或误码率高门限 $3：最近一次统计周期内的CRC错误报文数量 $4：CRC错误报文的收集和比较时间间隔，单位为秒
日志等级	4 (Warning)
举例	IFMON/4/CRC_ERROR_THRESHOLD: Number of CRC error packets exceeded the high threshold: Interface Name=HundredGigE1/0/1, High threshold=100, Number of CRC error packets=200, Interval=10s.
对系统的影响	如果物理接口下配置CRC错包率时选择配置了shutdown，接口接收到的CRC错误报文超出上限告警阈值时，关闭接口，该接口将停止转发所有报文。因CRC错误被关闭的接口不会自动恢复，需执行undo shutdown命令来恢复。未指定本参数时，表示当接口接收到的CRC错误报文超出上限告警阈值，接口将产生超上限告警，并进入告警状态
日志产生原因	在单位统计周期中，CRC的错误报文数量高于上限阈值时会产生该日志。一般产生的原因可能是设置的阈值不合理或数据在传输过程被损坏造成错误报文数量增多
处理建议	• 检查配置的上限阈值是否合理 • 检查链路环境质量是否良好

50.5 IFMON_BAD_BYTES_ERROR_RESUME

日志内容	The number of bad packet bytes on [STRING] drops below the lower threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	坏包字节数恢复到低于阈值
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_BAD_BYTES_ERROR_RESUME: The number of bad packet bytes on GigabitEthernet1/0/1 drops below the lower threshold. Threshold=99, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，坏包字节数恢复到低于阈值
处理建议	无需处理

50.6 IFMON_BAD_BYTES_ERROR_RISING

日志内容	The number of bad packet bytes on [STRING] exceeds the upper threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	坏包字节数高于阈值
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_BAD_BYTES_ERROR_RISING: The number of bad packet bytes on GigabitEthernet1/0/1 exceeds the upper threshold. Threshold=99, value=44, interval=10s.
对系统的影响	可能导致业务倒换或中断
日志产生原因	在统计周期内，坏包字节数高于阈值
处理建议	**1.** 当线路衰减过大时，请更换光纤，然后查看是否出现恢复 **2.** 在网管上查询对端站的发射光功率，如果发射光功率不正常，请更换对端站对应线路板，然后查看是否出现恢复 **3.** 更换本站上报日志的线路板，然后查看是否出现恢复 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.7 IFMON_CRC_ERROR_RESUME

日志内容	The number of CRC error packets on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	CRC错包恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_CRC_ERROR_RESUME: The number of CRC error packets on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，统计CRC错包个数从上限阈值恢复到低于下限阈值
处理建议	无需处理

50.8 IFMON_CRC_ERROR_RISING

日志内容	The number of CRC error packets on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	CRC的错包个数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_CRC_ERROR_RISING: The number of CRC error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计CRC的错包个数大于上限阈值。产出此日志的可能原因包括： • 光模块故障 • 光纤或者链路故障
处理建议	**1.** 请检查链路（包括光纤、光模块、传输设备、跳线架等部件）是否存在故障，更换故障部件，并将链路连接正常，检查是否恢复 **2.** 请检查接口下的高门限是否设置过低，可以通过 port ifmonitor crc-error命令修改门限值 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.9 IFMON_INPUT_BC_RAPID_CHANGE

日志内容	The incoming broadcast traffic of [STRING] suddenly exceeds the threshold. Threshold=[UINT64], current value=[UINT64].
日志含义	接口入方向广播流量突变超过阈值
参数解释	$1：接口名称 $2：突变阈值 $3：当前突变值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_BC_RAPID_CHANGE: The incoming broadcast traffic of GigabitEthernet1/0/1 suddenly exceeds the threshold. Threshold=99, current value=44.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	统计周期内，接口入方向广播流量突变超过阈值
处理建议	**1.** 当 CurrentInputBroadcastRate≥BaseInputBroadcastRate +InputBroadcastChangeThreshold 时，请确认是否正常的广播流量增加，如果不是请检查链路中是否存在环路 **2.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.10 IFMON_INPUT_BC_RAPID_RECOVER

日志内容	The incoming broadcast traffic of [STRING] suddenly drops below the lower threshold. Threshold=[UINT32], current value=[UINT32].
日志含义	接口入方向广播流量突变恢复正常
参数解释	$1：接口名称 $2：突变阈值 $3：当前突变值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_BC_RAPID_RECOVER: The incoming broadcast traffic of GigabitEthernet1/0/1 suddenly drops below the lower threshold. Threshold=99, current value=44.
对系统的影响	无
日志产生原因	接口入方向广播流量突变恢复到低于阈值
处理建议	无需处理

50.11 IFMON_INPUT_ERROR_RESUME

日志内容	The number of input error packets on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32].
日志含义	入方向错包个数恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_ERROR_RESUME: The number of input error packets on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44.
对系统的影响	无
日志产生原因	在统计周期内，统计入方向的错包个数从上限阈值恢复到低于下限阈值
处理建议	无需处理

50.12 IFMON_INPUT_ERROR_RISING

日志内容	The number of input error packets on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32].
日志含义	入方向错包个数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_ERROR_RISING: The number of input error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计入方向的错报个数大于上限阈值。产出此日志的可能原因包括： • 光模块故障 • 光纤或者链路故障
处理建议	1. 更换光模块，检查故障是否恢复 2. 更换光纤或者链路，检查故障是否恢复 3. 请检查接口下的上限阈值是否设置过低： 4. 若设置过低，可以通过 **port ifmonitor input-error**命令修改门限值 5. 如果设置合理，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.13 IFMON_INPUT_JAM_DISCARD

日志内容	The number of incoming packets lost due to network congestion on [STRING] exceeds the upper threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	接口入方向网络拥塞产生的丢包数超过阈值
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_JAM_DISCARD: The number of incoming packets lost due to network congestion on GigabitEthernet1/0/1 exceeds the upper threshold. Threshold=99, value=44, interval=10s.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	在统计周期内，接口入方向网络拥塞产生的丢包数超过阈值
处理建议	1. 在接口视图下执行命令 display this，查看有没有配置接口入方向限速 2. 在接口视图下执行命令 qos lr inbound cir cir-value [cbs cbs-value]修改限速配置或执行命令 undo qos lr inbound删除限速配置，查看是否恢复 3. 根据设备的具体业务情况，在接口视图下执行命令 port ifmonitor input-usage high-threshold high-value修改接口拥塞丢包告警功能的告警阈值，查看是否恢复 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.14 IFMON_INPUT_JAM_DISCARD_RESUME

日志内容	The number of incoming packets lost due to network congestion on [STRING] drops below the lower threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	接口入方向丢包恢复正常
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_JAM_DISCARD_RESUME: The number of incoming packets lost due to network congestion on GigabitEthernet1/0/1 drops below the lower threshold. Threshold=99, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，接口入方向网络拥塞产生的丢包数低于阈值
处理建议	无需处理

50.15 IFMON_INPUT_UFLOW_FALLING

日志内容	The number of incoming unknown unicast packets on [STRING] drops below threshold [UINT32]. Ratio=[UINT32].
日志含义	入接口的未知单播流量恢复到正常
参数解释	$1：接口名称 $2：阈值 $3：未知单播流量占总流量的比值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_UFLOW_FALLING : The number of incoming unknown unicast packets on GigabitEthernet1/0/1 drops below threshold =44,Ratio=20%.
对系统的影响	无
日志产生原因	入接口的未知单播流量恢复到低于阈值
处理建议	无需处理

50.16 IFMON_INPUT_UFLOW_RISING

日志内容	The number of incoming unknown unicast packets on [STRING] exceeds threshold [UINT32]. Ratio=[UINT32].
日志含义	入接口的未知单播流量超过设置的阈值
参数解释	$1：接口名称 $2：阈值 $3：未知单播流量占总流量的比值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_UFLOW_RISING: The number of incoming unknown unicast packets on GigabitEthernet1/0/1 exceeds threshold=50, Ratio=80%.
对系统的影响	可能会使正常协议报文上送带宽被抢占，导致协议中断，数据丢失
日志产生原因	设备流量异常或受到网络攻击，导致入接口的未知单播流量超过设置的阈值
处理建议	1. 在接口视图下执行命令 **display this**查看当前接口下配置的VLAN或者VSI 2. 在系统视图下进入相应的VLAN或者VSI视图，并执行命令 **display this**查看是否已开启MAC学习功能 o 如果已开启，转至步骤 3 o 如果未开启，进入步骤 4 3. 执行命令 mac-address mac-learning enable开启MAC学习功能后 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.17 IFMON_INPUT_USAGE_RESUME

日志内容	The input bandwidth usage on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], usage=[UINT32].
日志含义	入方向带宽利用率恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_USAGE_RESUME: The input bandwidth usage on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, usage=44.
对系统的影响	无
日志产生原因	入方向的带宽利用率从上限阈值限恢复到下限阈值以下
处理建议	无需处理

50.18 IFMON_INPUT_USAGE_RISING

日志内容	The input bandwidth usage on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], usage=[UINT32].
日志含义	入方向带宽利用率超过上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_INPUT_USAGE_RISING: The input bandwidth usage on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, usage=44.
对系统的影响	当接口入方向带宽利用率接近100%时，业务流量可能出现延时或丢包
日志产生原因	入方向带宽利用率超过上限阈值
处理建议	请检查接口下的上限阈值是否设置过低。 • 若设置过低，可以通过 **port ifmonitor input-usage**命令修改门限值 • 如果设置合理，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.19 IFMON_OUTPUT_ERROR_RESUME

日志内容	The number of output error packets on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32].
日志含义	出方向错包个数恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_OUTPUT_ERROR_RESUME: The number of output error packets on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44.
对系统的影响	无
日志产生原因	在统计周期内，统计出方向的错包个数从上限阈值恢复到低于下限阈值
处理建议	无需处理

50.20 IFMON_OUTPUT_ERROR_RISING

日志内容	The number of output error packets on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32].
日志含义	出方向错包个数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_OUTPUT_ERROR_RISING: The number of output error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计入方向的错包个数大于上限阈值。产出此日志的可能原因包括： • 光模块故障 • 光纤或者链路故障
处理建议	1. 请检查光纤是否插好，插好光纤后检查是否恢复 2. 检查物理链路是否正常 3. 执行命令 display interface命令查看 故障接口的光模块接收光功率（Tx Power）是否处于正常范围，查看设备两端的协商模式配置、时钟模式及扰码模式（Link protocol，clock，scramble）是否一致，如不一致请修改设备两端的协商模式配置，然后查看故障是否消除 4. 请检查接口下的上限阈值是否设置过低， o 若设置过低，可以通过 **port ifmonitor output-error**命令修改阈值 o 如果设置合理，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.21 IFMON_OUTPUT_JAM_DISCARD

日志内容	The number of outgoing packets lost due to network congestion on [STRING] exceeds the upper threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	接口出方向网络拥塞产生的丢包数超过阈值
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_OUTPUT_JAM_DISCARD: The number of outgoing packets lost due to network congestion on GigabitEthernet1/0/1 exceeds the upper threshold. Threshold=99, value=44, interval=10s.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	在统计周期内，接口出方向网络拥塞产生的丢包数超过阈值
处理建议	1. 在接口视图下执行命令 display this，查看有没有配置接口出方向限速 2. 在接口视图下执行命令 qos lr outbound cir cir-value [cbs cbs-value]修改限速配置或执行命令 undo qos lr outbound删除限速配置，查看是否恢复 3. 根据设备的具体业务情况，在接口视图下执行命令 port ifmonitor output-usage high-threshold high-value修改接口拥塞丢包告警功能的告警阈值，查看是否恢复 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.22 IFMON_OUTPUT_JAM_DISCARD_RESUME

日志内容	The number of outgoing packets lost due to network congestion on [STRING] drops below the lower threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	接口出方向丢包恢复正常
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_OUTPUT_JAM_DISCARD_RESUME: The number of outgoing packets lost due to network congestion on GigabitEthernet1/0/1 drops below the lower threshold. Threshold=99, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，接口出方向网络拥塞产生的丢包数低于阈值
处理建议	无需处理

50.23 IFMON_OUTPUT_USAGE_RESUME

日志内容	The output bandwidth usage on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], usage=[UINT32].
日志含义	出方向带宽利用率恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_OUTPUT_USAGE_RESUME: The output bandwidth usage on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, usage=44.
对系统的影响	无
日志产生原因	入方向的带宽利用率从上限阈值限恢复到下限阈值以下
处理建议	无需处理

50.24 IFMON_OUTPUT_USAGE_RISING

日志内容	The output bandwidth usage on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], usage=[UINT32].
日志含义	出方向带宽利用率超过上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值
日志等级	4 (Warning)
举例	IFMON/4/IFMON_OUTPUT_USAGE_RISING: The output bandwidth usage on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, usage=44.
对系统的影响	当接口出方向带宽利用率接近100%时，业务流量可能出现延时或丢包
日志产生原因	出方向带宽利用率超过上限阈值
处理建议	请检查接口下的上限阈值是否设置过低： • 若设置过低，可以通过 **port ifmonitor output-usage**命令修改门限值 • 如果设置合理，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.25 IFMON_PKT_DROP_RATE_RECOVER

日志内容	The packet drop rate on chassis [UINT32] slot [UINT32] drops below the lower threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s, protocol=[UINT32].
日志含义	业务板上丢弃的报文数目低于阈值
参数解释	$1：成员设备编号 $2：槽位号 $3：阈值 $4：统计值 $5：统计周期 $6：协议
日志等级	4 (Warning)
举例	IFMON/4/IFMON_PKT_DROP_RATE_RECOVER: The packet drop rate on chassis 0 slot 0 drops below the lower threshold. Threshold=99, value=44, interval=10s, protocol=1.
对系统的影响	无
日志产生原因	在统计周期内，业务板上丢弃的报文数目低于阈值
处理建议	无需处理

50.26 IFMON_PKT_DROP_RATE_RISING

日志内容	The packet drop rate on chassis [UINT32] slot [UINT32] exceeds the upper threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s, protocol=[UINT32].
日志含义	业务板上丢弃的报文数目超过阈值
参数解释	$1：成员设备编号 $2：槽位号 $3：阈值 $4：统计值 $5：统计周期 $6：协议
日志等级	4 (Warning)
举例	IFMON/4/IFMON_PKT_DROP_RATE_RISING: The packet drop rate on chassis 0 slot 0 exceeds the upper threshold. Threshold=99, value=44, interval=10s, protocol=1.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	在统计周期内，业务板上丢弃的报文数目超过阈值
处理建议	• 如果配置业务板丢失报文的告警时选择配置了 **shutdown**，当业务板接收到因丢失报文超出上限告警阈值时，关闭业务板下所有接口，该业务板将停止转发所有报文。因业务板告警被关闭的接口不会自动恢复，需执行 **undo shutdown**命令来恢复 • 如果配置业务板丢失报文的告警时选择配置了 **reboot**，当业务板接收到因丢失报文超出上限告警阈值时，重启业务板

50.27 IFMON_PORT_CRC_RATE_EXCEED

日志内容	The CRC packet error rate on [STRING] exceeds the upper threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	CRC错包速率大于等于1000个/秒
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_PORT_CRC_RATE_EXCEED: The CRC packet error rate on GigabitEthernet1/0/1 exceeds the upper threshold. Threshold=99, value=44, interval=10s.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	统计周期内，CRC错包速率大于等于1000个/秒
处理建议	**1.** 更换光模块，然后执行 display interface命令查看接口的CRC错包数是否继续增加 **2.** 更换光纤，然后执行 display interface命令查看接口的CRC错包数是否继续增加 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.28 IFMON_PORT_ERROR_RATE_EXCEED

日志内容	The number of error packets on [STRING] exceeds the upper threshold. Threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	CRC、Giants和Runts三者的平均错包速率超过1000个/秒
参数解释	$1：接口名称 $2：阈值 $3：统计值 $4：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_PORT_ERROR_RATE_EXCEED: The number of error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Threshold=99, value=44, interval=10s.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	统计周期内，CRC、Giants和Runts三者的平均错包速率超过1000个/秒
处理建议	**1.** 更换光模块，然后执行 display interface命令，查看接口的错包数是否继续增加 **2.** 更换光纤，然后执行 display interface命令，查看接口的错包数是否继续增加 **3.** 执行命令 jumboframe enable修改接口对报文长度的限制或修改报文长度，然后再执行 display interface命令查看接口的错包数是否继续增加 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.29 IFMON_RX_PAUSE_FRAME_RESUME

日志内容	The number of received pause frames on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	接收到的Rx-pause帧数恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_RX_PAUSE_FRAME_RESUME: The number of received pause frames on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，统计接收到的Rx-pause帧数从上限阈值恢复到低于下限阈值
处理建议	无需处理

50.30 IFMON_RX_PAUSE_FRAME_RISING

日志内容	The number of received pause frames on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	接收到的Rx-pause帧数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_RX_PAUSE_FRAME_RISING: The number of received pause frames on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计接收到的Rx-pause帧数大于上限阈值。产出此日志的可能原因包括： • pause 帧接收率超过上限阈值 • 连续收到 pause 帧的时间较长
处理建议	**1.** 减少对端接口接收的业务流量 **2.** 请检查接口下的上限阈值是否设置过低，相关配置命令：port ifmonitor rx-pause **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.31 IFMON_SDH_B1_ERROR_RESUME

日志内容	The number of SDH-B1 error packets on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	SdhB1错包个数恢复到低于下限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_SDH_B1_ERROR_RESUME: The number of SDH-B1 error packets on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	无
日志产生原因	统计周期内，SdhB1错包个数恢复到低于下限阈值
处理建议	无需处理

50.32 IFMON_SDH_B1_ERROR_RISING

日志内容	The number of SDH-B1 error packets on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	SdhB1错包个数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_SDH_B1_ERROR_RISING: The number of SDH-B1 error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计SdhB1的错包个数大于上限阈值
处理建议	**1.** 请检查链路（包括光纤、光模块、传输设备、跳线架等部件）是否存在故障，更换故障部件，并将链路连接正常，检查是否恢复 **2.** 请检查接口下的高门限是否设置过低，可以通过 port ifmonitor sdh-b1-error命令修改门限值 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.33 IFMON_SDH_B2_ERROR_RESUME

日志内容	The number of SDH-B2 error packets on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	SdhB2错包个数恢复到低于下限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_SDH_B2_ERROR_RESUME: The number of SDH-B2 error packets on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	无
日志产生原因	统计周期内，SdhB2错包个数恢复到低于下限阈值
处理建议	无需处理

50.34 IFMON_SDH_B2_ERROR_RISING

日志内容	The number of SDH-B2 error packets on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	SdhB2错包个数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_SDH_B2_ERROR_RISING: The number of SDH-B2 error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计SdhB2的错包个数大于上限阈值
处理建议	**1.** 请检查链路（包括光纤、光模块、传输设备、跳线架等部件）是否存在故障，更换故障部件，并将链路连接正常，检查是否恢复 **2.** 请检查接口下的高门限是否设置过低，可以通过 port ifmonitor sdh-b2-error命令修改门限值 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.35 IFMON_SDH_ERROR_RESUME

日志内容	The number of SDH error packets on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	SDH错包恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_SDH_ERROR_RESUME: The number of SDH error packets on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，统计SDH错包个数从上限阈值恢复到低于下限阈值
处理建议	无需处理

50.36 IFMON_SDH_ERROR_RISING

日志内容	The number of SDH error packets on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	Sdh错包个数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_SDH_ERROR_RISING: The number of SDH error packets on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计Sdh的错包个数大于上限阈值。产出此日志的可能原因包括： • 光模块故障 • 光纤或者链路故障
处理建议	• 更换光模块 • 更换光纤 • 请检查接口下的上限阈值是否设置过低，可以通过 **port ifmonitor sdh-error** 命令修改上限阈值 • 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.37 IFMON_TX_PAUSE_FRAME_RESUME

日志内容	The number of sent pause frames on [STRING] drops below the lower threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	发送的Rx-pause帧数恢复正常
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_TX_PAUSE_FRAME_RESUME: The number of sent pause frames on GigabitEthernet1/0/1 drops below the lower threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	无
日志产生原因	在统计周期内，统计发送的Rx-pause帧数从上限阈值恢复到低于下限阈值
处理建议	无需处理

50.38 IFMON_TX_PAUSE_FRAME_RISING

日志内容	The number of sent pause frames on [STRING] exceeds the upper threshold. Upper threshold=[UINT32], lower threshold=[UINT32], value=[UINT32], interval=[UINT32]s.
日志含义	发送的Rx-pause帧数大于上限阈值
参数解释	$1：接口名称 $2：上限阈值 $3：下限阈值 $4：统计值 $5：统计周期
日志等级	4 (Warning)
举例	IFMON/4/IFMON_TX_PAUSE_FRAME_RISING: The number of sent pause frames on GigabitEthernet1/0/1 exceeds the upper threshold. Upper threshold=99, lower threshold=22, value=44, interval=10s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在统计周期内，统计发送的Rx-pause帧数大于上限阈值。产出此日志的可能原因包括： • pause 帧发送率超过上限阈值 • 连续发送 pause 帧的时间较长
处理建议	1. 减少对端接口接收的业务流量 2. 请检查接口下的上限阈值是否设置过低，相关配置命令：port ifmonitor tx-pause 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

50.39 INPUT_ERROR_RECOVERY

日志内容	The number of input error packets dropped below the lower threshold: Interface name=[STRING].
日志含义	入方向的错误报文数量低于下限阈值
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFMON/4/INPUT_ERROR_RECOVERY: The number of input error packets dropped below the lower threshold: Interface name=GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	在单位统计周期中，入方向的错误报文数量低于下限阈值时会产生该日志，表示解除告警
处理建议	无需处理

50.40 INPUT_ERROR_THRESHOLD

日志内容	The number of input error packets exceeded the upper threshold: Interface name=[STRING], upper threshold=[UINT32], number of input error packets=[UINT64], interval=[UINT32] s.
日志含义	入方向的错误报文数量高于上限阈值
参数解释	$1：接口名称 $2：告警上限阈值或误码率高门限 $3：最近一次统计周期内的入方向错误报文数量 $4：入方向错误报文的收集和比较时间间隔，单位为秒
日志等级	4 (Warning)
举例	IFMON/4/INPUT_ERROR_THRESHOLD: The number of input error packets exceeded the upper threshold: Interface name=HundredGigE1/0/1, upper threshold=100, number of input error packets=200, interval=10 s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在单位统计周期中，入方向的错误报文数量高于上限阈值时会产生该日志。一般产生的原因可能是设置的阈值不合理或数据在传输过程被损坏造成错误报文数量增多
处理建议	• 检查配置的上限阈值是否合理 • 检查链路环境质量是否良好

50.41 OUTPUT_ERROR_RECOVERY

日志内容	The number of output error packets dropped below the lower threshold: Interface name=[STRING].
日志含义	出方向的错误报文数量低于下限阈值
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFMON/4/OUTPUT_ERROR_RECOVERY: The number of output error packets dropped below the lower threshold: Interface name=GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	在单位统计周期中，出方向的错误报文数量低于下限阈值时会产生该日志，表示解除告警
处理建议	无需处理

50.42 OUTPUT_ERROR_THRESHOLD

日志内容	The number of output error packets exceeded the upper threshold: Interface name=[STRING], upper threshold=[UINT32], number of output error packets=[UINT64], interval=[UINT32] s.
日志含义	出方向的错误报文数量高于上限阈值
参数解释	$1：接口名称 $2：告警上限阈值或误码率高门限 $3：最近一次统计周期内的出方向错误报文数量 $4：出方向错误报文的收集和比较时间间隔，单位为秒
日志等级	4 (Warning)
举例	IFMON/4/OUTPUT_ERROR_THRESHOLD: The number of output error packets exceeded the upper threshold: Interface name=HundredGigE1/0/1, upper threshold=100, number of output error packets=200, interval=10 s.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	在单位统计周期中，出方向的错误报文数量高于上限阈值时会产生该日志。一般产生的原因可能是设置的阈值不合理或数据在传输过程被损坏造成错误报文数量增多
处理建议	• 检查配置的上限阈值是否合理，若设置过低，可以通过 **port ifmonitor output-error**命令修改门限值 • 检查链路环境质量是否良好 • 执行命令 **display interface命令查看** 故障接口的光模块接收光功率（Tx Power）是否处于正常范围，查看设备两端的协商模式配置、时钟模式及扰码模式（Link protocol，clock，scramble）是否一致，如不一致请修改设备两端的协商模式配置

51 IFNET

本节介绍接口管理模块输出的日志信息。

51.1 IF_BOARD_EGRESS_DROP

日志内容	Packet loss occurs on chassis [UINT32] slot [UINT32].
日志含义	业务板出方向单播流量被丢弃
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_BOARD_EGRESS_DROP: Packet loss occurs on chassis 0 slot 0.
对系统的影响	业务板出方向单播流量被丢弃
日志产生原因	业务板出方向单播流量被丢弃
处理建议	优化网络，调整流量方案

51.2 IF_BOARD_EGRESS_DROP_RECOVER

日志内容	Packet loss recovers on chassis [UINT32] slot [UINT32].
日志含义	业务板出方向单播流量丢包情况恢复正常
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/ IF_BOARD_EGRESS_DROP_RECOVER: Packet loss recovers on chassis 0 slot 0.
对系统的影响	无
日志产生原因	业务板出方向单播流量丢包情况恢复正常
处理建议	无需处理

51.3 IF_BUFFER_CONGESTION_CLEAR

日志内容	[STRING] congestion on queue [UINT32] of [STRIING] is cleared. [UINT64] packets are discarded.
日志含义	接口队列接收数据缓冲区的拥塞解除
参数解释	$1：接收或发送数据缓冲区，ingress、egress $2：队列ID，0～7 $3：接口名称 $4：丢弃报文数
日志等级	5 (Notification)
举例	IFNET/5/IF_BUFFER_CONGESTION_CLEAR: Ingress congestion on queue 1 of GigabitEthernet1/0/1 is cleared. 1000 packets are discarded.
对系统的影响	无
日志产生原因	在接口GigabitEthernet1/0/1上队列1接收数据缓冲区的拥塞解除。共有1000个报文被丢弃
处理建议	无需处理

51.4 IF_BUFFER_CONGESTION_OCCURRENCE

日志内容	[STRING] congestion occurs on queue [INTEGER] of [STRING].
日志含义	接口队列的接收数据缓冲区发生拥塞
参数解释	$1：接收或发送数据缓冲区，ingress、egress $2：队列ID，0～7 $3：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_BUFFER_CONGESTION_OCCURRENCE: Ingress congestion occurs on queue 1 of GigabitEthernet1/0/1.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	在接口GigabitEthernet1/0/1上队列1的接收数据缓冲区发生拥塞
处理建议	检查网络状况

51.5 IF_BUFFER_IN_DISCARD

日志内容	Packets are dropped in the ingress buffer on chassis [UINT32] slot [UINT32].
日志含义	单板入方向缓存中有流量被丢弃
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_BUFFER_IN_DISCARD: Packets are dropped in the ingress buffer on chassis 0 slot 0.
对系统的影响	单板入方向缓存流量被丢弃
日志产生原因	单板入方向流量超出网板链路带宽
处理建议	优化网络，调整流量方案

51.6 IF_BUFFER_IN_DISCARD_RESUME

日志内容	Packet drop in the ingress buffer recovers on chassis [UINT32] slot [UINT32].
日志含义	单板从入方向缓存中有流量被丢弃状态中恢复
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_BUFFER_IN_DISCARD_RESUME: Packet drop in the ingress buffer recovers on chassis 0 slot 0.
对系统的影响	无
日志产生原因	在设定的时间内，网络已缓解网络拥塞
处理建议	无需处理

51.7 IF_CABLE_SNR_ABNORMAL

日志内容	The cable SNR on [STRING] is abnormal.
日志含义	接口网线上信噪比异常
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_CABLE_SNR_ABNORMAL: The cable SNR on GigabitEthernet1/0/1 is abnormal.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	网线质量不好或存在信号干扰
处理建议	1. 更换为高质量网线，如 Cat6A 网线或屏蔽网线 2. 执行 **speed**或 **auto speed**命令，降低MultiGE接口的工作速率 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.8 IF_CABLE_SNR_DETECT_NOTSUPPORT

日志内容	The cable SNR on [STRING] cannot be detected.
日志含义	网线质量无法检测
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_CABLE_SNR_DETECT_NOT_SUPPORT: The cable SNR on GigabitEthernet1/0/1 cannot be detected.
对系统的影响	可能导致基于该接口的业务流量被丢弃
日志产生原因	网线质量无法检测，MultiGE接口由Up变Down
处理建议	1. 网线质量无法检测，请更换网线 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.9 IF_CABLE_SNR_NORMAL

日志内容	The cable SNR on [STRING] is normal.
日志含义	接口网线上信噪比正常
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_CABLE_SNR_NORMAL: The cable SNR on GigabitEthernet1/0/1 is normal.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	网线质量不好或存在信号干扰
处理建议	1. 更换为高质量网线，如 Cat6A 网线或屏蔽网线 2. 执行 **speed { 100 | 1000 }**或 **auto speed { 100 | 1000 }**命令，降低MultiGE接口的工作速率 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.10 IF_COMBO_TYPE_CHANGE

日志内容	The combo type of [STRING] changes from [UINT32] to [UINT32].
日志含义	combo类型发生变化
参数解释	$1：接口名称 $2：combo类型，copper、fiber $3：combo类型，copper、fiber
日志等级	4 (Warning)
举例	IFNET/4/IF_COMBO_TYPE_CHANGE: The combo type of GigabitEthernet1/0/1 changes from copper to fiber.
对系统的影响	无
日志产生原因	**combo enable { copper | fiber }**命令行配置发生变化
处理建议	无需处理

51.11 IF_DELETE

日志内容	[STRING] is deleted.
日志含义	接口被删除
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_DELETE: GigabitEthernet1/0/1 is deleted.
对系统的影响	相关依赖接口的业务可能会受影响
日志产生原因	接口被删除
处理建议	无需处理

51.12 IF_EGRESS_DROP

日志内容	Packet loss occurs in queue [UINT32] of [STRING].
日志含义	端口存在丢包
参数解释	$1：接口名称 $2：丢包队列，0~7
日志等级	4 (Warning)
举例	IFNET/4/IF_EGRESS_DROP: Packet loss occurs in queue 0 of GigabitEthernet1/0/1.
对系统的影响	端口出方向流量被丢弃
日志产生原因	端口存在丢包
处理建议	优化网络，调整流量方案

51.13 IF_EGRESS_DROP_RECOVER

日志内容	Packet loss recovers in queue [UINT32] of [STRING].
日志含义	端口丢包情况恢复正常
参数解释	$1：接口名称 $2：丢包队列，0~7
日志等级	4 (Warning)
举例	IFNET/4/IF_EGRESS_DROP_RECOVER: Packet loss recovers in queue 0 of GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	端口丢包情况恢复正常
处理建议	无需处理

51.14 IF_ERROR_DOWN

日志内容	An error down alarm occurs on [STRING], because of [STRING].
日志含义	接口异常Down告警及其原因
参数解释	$1：接口名称 $2：接口Down的原因，取值包括： • Administratively DOWN：管理员手工关闭接口导致接口 Down • Storm-Constrain DOWN：网络风暴（如广播风暴、组播风暴等）导致接口 Down • PFC-deadlock DOWN：PFC 死锁导致接口 Down • Link-Flap DOWN：链路震荡保护导致接口 Down
日志等级	4 (Warning)
举例	IFNET/4/IF_ERROR_DOWN: An error down alarm occurs on GigabitEthernet1/0/1, because of port down.
对系统的影响	接口无法转发业务流量
日志产生原因	接口状态为Down
处理建议	请检查是否没有物理连线或者链路故障

51.15 IF_ERROR_DOWN_RECOVER

日志内容	An error down alarm recovers on [STRING].
日志含义	接口异常Down告警恢复
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	IFNET/5/IF_ERROR_DOWN_RECOVER: An error down alarm recovers on GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	接口异常Down恢复
处理建议	无需处理

51.16 IF_ETHERNET_RX_FLOW_FAILED

日志内容	The inbound traffic volume drops below the threshold on [STRING].
日志含义	以太网端口接收方向流量跌落
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_ETHERNET_RX_FLOW_FAILED: The inbound traffic volume drops below the threshold on GigabitEthernet1/0/1.
对系统的影响	存在流量突然降低问题
日志产生原因	端口UP时，以太网端口接收方向流量跌落
处理建议	无需处理

51.17 IF_FLOW_CONTROL_DEADLOCK

日志内容	Flow control deadlock occurs on [STRING].
日志含义	接口的流量控制功能处于死锁状态
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_FLOW_CONTROL_DEADLOCK: Flow control deadlock occurs on GigabitEthernet1/0/1.
对系统的影响	端口无法转发报文
日志产生原因	产生此日志的可能原因包括： • 该端口未转发报文，却从该端口接收到大量的 Pause 帧 • 端口持续发送大量 Pause 帧，但没有接收到报文
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.18 IF_FLOW_CONTROL_DEADLOCK_RESUME

日志内容	Flow control deadlock recovers on [STRING].
日志含义	接口的流量控制功能从死锁状态中恢复正常
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_FLOW_CONTROL_DEADLOCK_RESUME: Flow control deadlock recovers on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	产生此日志的可能原因包括： • 该端口发送 Pause 帧，并且有接收到报文 • 未转发报文的端口也未接收到 Pause 帧
处理建议	无需处理

51.19 IF_HALF_DUPLEX_CLEAR

日志内容	The negotiated half duplex mode on [STRING] is cleared.
日志含义	接口自协商恢复成全双工模式
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_HALF_DUPLEX_CLEAR: The negotiated half duplex mode on GigabitEthernet1/0/1 is cleared.
对系统的影响	无
日志产生原因	接口自协商恢复成全双工模式
处理建议	无需处理

51.20 IF_HALF_DUPLEX_RISING

日志内容	The half duplex mode is negotiated on [STRING].
日志含义	端口在半双工模式
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_HALF_DUPLEX_RISING: The half duplex mode is negotiated on GigabitEthernet1/0/1.
对系统的影响	端口工作在半双工模式下可能会丢包
日志产生原因	接口下半双工改变
处理建议	通过**duplex full**命令将端口设置为全双工模式

51.21 IF_INGRESS_AGING_DROP

日志内容	Traffic in the ingress buffer of chassis [UINT32] slot [UINT32] is dropped for no schedule.
日志含义	业务板上行缓存中的流量由于得不到调度而被丢弃
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_INGRESS_AGING_DROP: Traffic in the ingress buffer of chassis 0 slot 0 is dropped for no schedule.
对系统的影响	业务板的业务流量存在丢包
日志产生原因	高优先级队列的报文流量超过端口带宽，导致低优先级队列的报文得不到调度
处理建议	优化网络，调整流量方案

51.22 IF_INGRESS_AGING_DROP_RESUME

日志内容	Traffic in the ingress buffer of chassis [UINT32] slot [UINT32] recovers from drop with no schedule.
日志含义	业务板上行缓存中的流量重新得到调度
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_INGRESS_AGING_DROP_RESUME: Traffic in the ingress buffer of chassis 0 slot 0 recovers from drop with no schedule.
对系统的影响	无
日志产生原因	业务板上行缓存中的流量重新得到调度
处理建议	无需处理

51.23 IF_JUMBOFRAME_WARN

日志内容	The specified size of jumbo frames on the aggregate interface [STRING] is not supported on the member port [STRING].
日志含义	分成员端口不支持**jumboframe enable** [*size*]配置
参数解释	$1：聚合接口名称 $2：成员端口名称
日志等级	3 (Error)
举例	IFNET/3/IF_JUMBOFRAME_WARN: -MDC=1-Slot=3; The specified size of jumbo frames on the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/0/1.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	聚合接口修改**jumboframe enable** [*size*]配置，部分成员端口不支持
处理建议	确认成员端口支持配置的*size*范围，将聚合接口的*size*配置在该范围内

51.24 IF_LINKFLAP_DETECTED

日志内容	Link flapping was detected on [STRING].
日志含义	检测到接口频繁震荡
参数解释	$1：接口名称
日志等级	3 (Error)
举例	IFNET/3/IF_LINKFLAP_DETECTED: Link flapping was detected on GigabitEthernet1/0/1.
对系统的影响	该接口转发的业务流量可能被丢弃
日志产生原因	在链路震荡检查时间间隔内，接口状态从UP变为DOWN的次数大于等于链路震荡次数阈值
处理建议	1. 检查接口（本端或对端）连线是否被频繁插拔 2. 通过 **port link-flap protect enable**命令调整链路震荡检查时间间隔和链路震荡次数阈值

51.25 IF_LOCAL_FAULT

日志内容	A local fault alarm occurs on [STRING].
日志含义	远端到本端的接收链路产生故障
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LOCAL_FAULT: A local fault alarm occurs on GigabitEthernet1/0/1.
对系统的影响	可能导致业务倒换或中断
日志产生原因	远端到本端的接收链路产生故障，如接收光纤瞬断
处理建议	**1.** 检查接收光纤是否故障 **2.** 检查本端和远端的光模块是否故障 **3.** 检查本端单板是否故障 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.26 IF_LOCAL_FAULT_RESUME

日志内容	A local fault alarm recovers on [STRING].
日志含义	远端到本端的接收链路恢复正常
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LOCAL_FAULT_RESUME: A local fault alarm recovers on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	远端到本端的接收链路恢复正常
处理建议	无需处理

51.27 IF_LOOPBACK

日志内容	Loopback configuration is issued on [STRING].
日志含义	设备上配置了环回配置
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LOOPBACK: Loopback configuration is issued on GigabitEthernet1/0/1.
对系统的影响	若该端口或通道存在业务，则业务中断
日志产生原因	设备上配置了环回配置
处理建议	可以通过**undo loopback**命令用来关闭以太网接口的环回功能

51.28 IF_LOOPBACK_RESUME

日志内容	Loopback configuration is removed on [STRING].
日志含义	删除了设备上的环回配置
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LOOPBACK_RESUME: Loopback configuration is removed on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	删除了设备上的环回配置
处理建议	无需处理

51.29 IF_LOS

日志内容	A LOS alarm occurs on [STRING].
日志含义	光模块检测无光输入，接收信号丢失
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LOS: A LOS alarm occurs on GigabitEthernet1/0/1.
对系统的影响	可能导致业务倒换或中断
日志产生原因	光模块检测无光输入，接收信号丢失，产出此日志的可能原因包括： • 接收信号衰减过大 • 对端站发送信号无帧结构 • 本端接收方向故障

处理建议	**1.** 如果是光口：
	• 检查光纤是否错连（如两个速率不一致的端口连在一起），更正错误的连接后，查看是否消除
	• 在网管上查看本站接收光功率是否正常
	  ◦ 如果接收光功率过低，请清洁本站尾纤接头和线路板接收光口和检查本站的法兰盘和光衰减器是否连接正确，光衰减器的衰减值是否过大。正确使用法兰盘和光衰减器后，查看是否消除
	  ◦ 如果接收光功率过高，则增加光衰减器，调整接收光功率至正常范围，查看是否消除
	• 检查对端站的发射光功率是否正常。若发射光功率正常，则对本站线路板进行光纤环回。若此时本站故障恢复，表示对端站发送信号无帧结构
	2. 如果是电口：
	• 检查电缆是否错连（如两个速率不一致的端口连在一起），更正错误的连接后，查看故障是否消除
	• 查看对端帧格式配置是否和本端一致，确保一致后，查看故障是否消除
	3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.30 IF_LOS_RESUME

日志内容	A LOS alarm recovers on [STRING].
日志含义	光模块检测到光输入
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LOS_RESUME: A LOS alarm recovers on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	光模块检测到光输入
处理建议	无需处理

51.31 IF_LRM_STATE_ABNORMAL

日志内容	[STRING] has an unsupported LRM transceiver module inserted.
日志含义	接口插入了不支持的LRM的光模块
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_LRM_STATE_ABNORMAL: GigabitEthernet 1/0/1 has an unsupported LRM transceiver module inserted.
对系统的影响	光模块不可用，对应该接口的业务中断
日志产生原因	接口插入了不支持的LRM的光模块
处理建议	1. 执行命令 **display transceiver**查看接口当前在位的光模块类型 2. 更换在位光模块为非 LRM 光模块 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.32 IF_MULTI_CHASSIS

日志内容	A single-chassis device is changed to a multi-chassis device, and the interface information changes.
日志含义	单框设备扩容到多框设备，接口信息发生变化
参数解释	无
日志等级	4 (Warning)
举例	IFNET/4/IF_MULTI_CHASSIS: A single-chassis device is changed to a multi-chassis device, and the interface information changes.
对系统的影响	无
日志产生原因	单框设备扩容到多框设备，接口信息发生变化
处理建议	无需处理

51.33 IF_MULTI_CHASSIS_RESUME

日志内容	A multi-chassis device is rolled backed to a single-chassis device, and the interface information changes.
日志含义	多框设备回退为单框设备，接口信息发生变化
参数解释	无
日志等级	4 (Warning)
举例	IFNET/4/IF_MULTI_CHASSIS_RESUME: A multi-chassis device is rolled backed to a single-chassis device, and the interface information changes.
对系统的影响	无
日志产生原因	多框设备回退为单框设备，接口信息发生变化
处理建议	无需处理

51.34 IF_NEGO_FAILED

日志内容	Autonegotiation fails on [STRING].
日志含义	接口自协商失败
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_NEGO_FAILED: Autonegotiation fails on GigabitEthernet1/0/1.
对系统的影响	接口不能Up，链路不通
日志产生原因	接口自协商失败
处理建议	检查链路两端接口下速率和双工是否配置一致

51.35 IF_NEGO_FAILED_RESUME

日志内容	Autonegotiation succeeds on [STRING].
日志含义	接口自协商恢复成功
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_NEGO_FAILED_RESUME: Autonegotiation succeeds on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	接口自协商恢复成功
处理建议	无需处理

51.36 IF_OUTPUT_ERROR

日志内容	The number of outbound error packets exceeds the upper threshold on [STRING] with slot [UINT32] subslot [UINT32].
日志含义	接口出方向错误报文超过上限阈值
参数解释	$1：接口名称 $2：单板号 $3：子板号
日志等级	4 (Warning)
举例	IFNET/4/IF_OUTPUT_ERROR: The number of outbound error packets exceeds the upper threshold on GigabitEthernet1/0/1 with slot 0 subslot 0.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	接口出方向错误报文超过上限阈值
处理建议	1. 请检查光纤是否插好，插好光纤后检查是否恢复 2. 检查物理链路是否正常 3. 执行命令**display interface**命令查看 故障接口的光模块接收光功率（Tx Power）是否处于正常范围，查看设备两端的协商模式配置、时钟模式及扰码模式（Link protocol，clock，scramble）是否一致，如不一致请修改设备两端的协商模式配置，然后查看是否消除 4. 请检查接口下的高门限是否设置过低，若设置过低，可以通过**port ifmonitor output-error**命令修改门限值 5. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.37 IF_OUTPUT_ERROR_RESUME

日志内容	The number of outbound error packets drops below the upper threshold on [STRING] with slot [UINT32] subslot [UINT32].
日志含义	接口出方向错误报文低于上限阈值
参数解释	$1：接口名称 $2：单板号 $3：子板号
日志等级	4 (Warning)
举例	IFNET/4/IF_OUTPUT_ERROR_RESUME: The number of outbound error packets drops below the upper threshold on GigabitEthernet1/0/1 with slot 0 subslot 0.
对系统的影响	无
日志产生原因	接口出方向错误报文从高于上限阈值恢复到低于上限阈值
处理建议	无需处理

51.38 IF_PFC_DEADLOCK

日志内容	PFC deadlock occurs in queue [UINT32] on [STRING].
日志含义	PFC死锁
参数解释	$1：消息队列ID $2：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PFC_DEADLOCK: PFC deadlock occurs in queue 1 on GigabitEthernet1/0/1.
对系统的影响	可能导致网络中流量不通
日志产生原因	PFC死锁
处理建议	1. 执行 **display priority-flow-control**命令，确认网络中出现PFC死锁的原因并优化网络，若网络优化后问题未解决，请执行第 2 步； 2. 执行 **priority-flow-control deadlock cos** *cos-value* **interval** *interval*命令调整PFC死锁检测周期，以满足网络实际使用需求 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.39 IF_PFC_DEADLOCK_RESUME

日志内容	PFC deadlock recovers in queue [UINT32] on [STRING].
日志含义	PFC死锁恢复
参数解释	$1：消息队列ID $2：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PFC_DEADLOCK_RESUME: PFC deadlock occurs in queue 1 on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	PFC死锁恢复
处理建议	无需处理

51.40 IF_PFC_TURN_OFF

日志内容	PFC deadlock causes traffic interruption in queue [UINT32] on [STRING].
日志含义	PFC功能自动关闭
参数解释	$1：消息队列ID $2：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PFC_TURN_OFF: PFC deadlock causes traffic interruption in queue 1 on GigabitEthernet1/0/1.
对系统的影响	PFC功能自动关闭
日志产生原因	一个检测周期内死锁发生次数超过PFC自动关闭的阈值
处理建议	1. 执行 **display priority-flow-control**命令，确认网络中出现PFC死锁的原因并优化网络，若网络优化后问题未解决，请执行第 2 步 2. 执行 **priority-flow-control deadlock cos** *cos-value* **interval** *interval*命令调整PFC死锁检测周期，执行 **priority-flow-control deadlock threshold cos cos-value period** *period* **count** *count*命令调整自动关闭PFC功能的死锁次数，以满足网络实际使用需求； 3. 如果网络中PFC死锁已经解除，可在接口下先执行 **undo dpriority-flow-control enable**来关闭PFC功能，再使用 **priority-flow-control enable**开启PFC功能，以重新应用PFC 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.41 IF_PFC_TURN_OFF_RESUME

日志内容	Traffic interruption caused by traffic interruption recovers in queue [UINT32] on [STRING].
日志含义	PFC功能恢复正常
参数解释	$1：消息队列ID $2：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PFC_TURN_OFF_RESUME: Traffic interruption caused by traffic interruption recovers in queue 1 on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	一个检测周期内死锁发生次数低于PFC自动关闭的阈值
处理建议	无需处理

51.42 IF_PORT_DOWN

日志内容	[STRING] is down.
日志含义	物理端口的物理状态处于DOWN状态
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PORT_DOWN: GigabitEthernet1/0/1 is down.
对系统的影响	该端口无法转发业务流量
日志产生原因	物理端口的物理状态处于DOWN状态
处理建议	• 请在接口视图下执行命令**display this**，查看两端接口是否被shutdown。如被shutdown请在接口视图下执行**undo shutdown**命令 • 请查看物理链接是否正常（包括网线、光模块等硬件是否松动或脱落），请正确连接物理线路

51.43 IF_PORT_SFP_NOSUPT_SINGLEFIBER

日志内容	The transceiver module in [STRING] does not support single-mode fibers.
日志含义	接口插入的光模块不支持单纤功能
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/ IF_PORT_SFP_NOSUPT_SINGLEFIBER: The transceiver module in GigabitEthernet1/0/1 does not support single-mode fibers.
对系统的影响	接口插入的光模块导致该接口的单纤功能不可用
日志产生原因	接口插入的光模块不支持单纤功能
处理建议	请更换为支持单纤功能的光模块

51.44 IF_PORT_SFP_WORK_ONLY_NON_NEGO

日志内容	[STRING] only works in non-negotiation mode.
日志含义	XGE接口插入GE光模块导致该接口的自协商功能不可用
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PORT_SFP_WORK_ONLY_NON_NEGO: GigabitEthernet1/0/1 only works in non-negotiation mode.
对系统的影响	XGE接口插入GE光模块导致该接口的自协商功能不可用
日志产生原因	XGE接口插入的GE光模块只能工作在非自协商1000Mbit/s模式，将互联的接口速率配置未强制1000Mbit/s
处理建议	请将互联的接口配置为强制1000Mbit/s速率或更换光模块

51.45 IF_PORT_UP

日志内容	[STRING] is up.
日志含义	物理端口的物理状态处于状态
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_PORT_UP: GigabitEthernet1/0/1 is up.
对系统的影响	无
日志产生原因	物理端口的物理状态处于UP状态
处理建议	无需处理

51.46 IF_PORTRATE_DEGRADE

日志内容	The negotiated port rate degrades on [STRING], rate=[UINT32].
日志含义	接口协商速率下降
参数解释	$1：接口名称 $2：接口速率
日志等级	4 (Warning)
举例	IFNET/4/IF_PORTRATE_DEGRADE: The negotiated port rate degrades on GigabitEthernet1/0/1, rate=10.
对系统的影响	可能会导致业务流量被丢弃
日志产生原因	接口协商速率下降
处理建议	• 检查链路是否故障 • 检查对端设备电口是否存在故障

51.47 IF_PORTRATE_DEGRADE_RESUME

日志内容	The negotiated port rate recovers on [STRING], rate=[UINT32].
日志含义	接口协商速率恢复
参数解释	$1：接口名称 $2：接口速率
日志等级	4 (Warning)
举例	IFNET/4/ IF_PORTRATE_DEGRADE_RESUME: The negotiated port rate recovers on GigabitEthernet1/0/1, rate=10.
对系统的影响	无
日志产生原因	接口协商速率恢复
处理建议	无需处理

51.48 IF_QUEUE

日志内容	The usage exceeds the threshold in queue [UINT32] on [STRING], threshold=[UINT32], current value=[UINT32].
日志含义	接口上队列的队列深度使用率超过接口上的使用率阈值
参数解释	$1：消息队列ID $2：接口名称 $3：使用率阈值 $4：当前使用率
日志等级	4 (Warning)
举例	IFNET/4/IF_QUEUE: The usage exceeds the threshold in queue 1 on GigabitEthernet1/0/1, threshold=22, current value=10.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	接口上队列的队列深度使用率超过接口上的使用率阈值
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.49 IF_QUEUE_RESUME

日志内容	The usage drops below the threshold in queue [UINT32] on [STRING], threshold=[UINT32], current value=[UINT32].
日志含义	接口上队列的队列深度使用率恢复到正常状态
参数解释	$1：消息队列ID $2：接口名称 $3：使用率阈值 $4：当前使用率
日志等级	4 (Warning)
举例	IFNET/4/IF_QUEUE_RESUME: The usage drops below the threshold in queue 1 on GigabitEthernet1/0/1, threshold=22, current value=10.
对系统的影响	无
日志产生原因	接口上队列的队列深度使用率恢复到正常状态
处理建议	无需处理

51.50 IF_QUEUE_STAT_DISCARD

日志内容	The number of dropped objects exceeds the threshold in queue [UINT32] on [STRING], discardType=[STRING], threshold=[UINT32].
日志含义	端口队列丢包数/丢弃字节数/丢包率超过阈值
参数解释	$1：消息队列ID $2：接口名称 $3：丢包类型，丢包数、丢包字节数、丢包率 $4：当前阈值
日志等级	4 (Warning)
举例	IFNET/4/IF_STAT_DISCARD: The number of dropped objects exceeds the threshold in queue 1 on GigabitEthernet1/0/1, discardType=discardbyte, threshold=100.
对系统的影响	存在丢包问题，可能影响接口业务
日志产生原因	端口队列丢包数/丢弃字节数/丢包率超过阈值
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.51 IF_QUEUE_STAT_DISCARD_RESUME

日志内容	The number of dropped objects drops below the threshold in queue [UINT32] on [STRING], discardType=[STRING], threshold=[UINT32].
日志含义	端口队列丢包数/丢弃字节数/丢包率恢复到正常状态
参数解释	$1：消息队列ID $2：接口名称 $3：丢包类型，丢包数、丢包字节数、丢包率 $4：当前阈值
日志等级	4 (Warning)
举例	IFNET/4/IF_QUEUE_STAT_DISCARD_RESUME: The number of dropped objects drops below the threshold in queue 1 on GigabitEthernet1/0/1, discardType=discardbyte, threshold=100.
对系统的影响	无
日志产生原因	端口队列丢包数/丢弃字节数/丢包率恢复到正常状态
处理建议	无需处理

51.52 IF_RECOVER_OVER_SLOT

日志内容	The card in chassis [UINT32] slot [UINT32] starts.
日志含义	业务板进入可使用状态
参数解释	$1：成员设备编号 $2：槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_RECOVER_OVER_SLOT: The card in chassis 0 slot 0 starts.
对系统的影响	该业务板可以使用
日志产生原因	业务板进入可使用状态
处理建议	无需处理

51.53 IF_RECOVER_OVER_SUBSLOT

日志内容	The subcard in chassis [UINT32] slot [UINT32] subslot [UINT32] starts.
日志含义	接口子卡进入可使用状态
参数解释	$1：成员设备编号 $2：槽位号 $2：子槽位号
日志等级	4 (Warning)
举例	IFNET/4/IF_RECOVER_OVER_SUBSLOT: The subcard in chassis 0 slot 0 subslot 0 starts.
对系统的影响	该接口子卡可以使用
日志产生原因	接口子卡进入可使用状态
处理建议	无需处理

51.54 IF_REMOTE_FAULT

日志内容	A remote fault alarm occurs on [STRING].
日志含义	本端到远端的发送链路产生故障
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_REMOTE_FAULT: A remote fault alarm occurs on GigabitEthernet1/0/1.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	本端到远端的发送链路产生故障
处理建议	**1.** 检查发送光纤是否故障 **2.** 检查本端和远端的光模块是否故障 **3.** 检查远端单板是否故障 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

51.55 IF_REMOTE_FAULT_RESUME

日志内容	A remote fault alarm recovers on [STRING].
日志含义	本端到远端的接收链路恢复正常
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_REMOTE_FAULT_RESUME: A remote fault alarm recovers on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	本端到远端的发送链路恢复正常
处理建议	无需处理

51.56 IF_RX_FLOW_FAILED_RESUME

日志内容	The inbound traffic volume increases to the normal range on [STRING].
日志含义	以太网端口接收方向流量回升
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_RX_FLOW_FAILED_RESUME: The inbound traffic volume increases to the normal range on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	以太网端口接收方向流量回升
处理建议	无需处理

51.57 IF_TX_FLOW_FAILED

日志内容	The outbound traffic volume drops below the threshold on [STRING].
日志含义	以太网端口发送方向流量跌落
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_TX_FLOW_FAILED: The outbound traffic volume drops below the threshold on GigabitEthernet1/0/1.
对系统的影响	存在流量突然降低问题
日志产生原因	端口UP时，以太网端口发送方向流量跌落
处理建议	无需处理

51.58 IF_TX_FLOW_FAILED_RESUME

日志内容	The outbound traffic volume increases to the normal range on [STRING].
日志含义	以太网端口发送方向流量回升
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IFNET/4/IF_TX_FLOW_FAILED_RESUME: The outbound traffic volume increases to the normal range on GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	以太网端口发送方向流量回升
处理建议	无需处理

51.59 INTERFACE_NOTSUPPRESSED

日志内容	Interface [STRING] is not suppressed.
日志含义	接口由抑制状态变为非抑制状态
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	IFNET/6/INTERFACE_NOTSUPPRESSED: Interface Ethernet0/0/0 is not suppressed.
对系统的影响	无
日志产生原因	接口由抑制状态变为非抑制状态，此时上层业务可以感知接口UP/DOWN状态变化
处理建议	无需处理

51.60 INTERFACE_SUPPRESSED

日志内容	Interface [STRING] was suppressed.
日志含义	接口状态频繁变化导致接口被抑制
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	IFNET/5/INTERFACE_SUPPRESSED: Interface Ethernet0/0/0 was suppressed.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	当接口状态频繁变化时，接口被抑制。抑制期间，上层业务不能感知端口UP/DOWN状态变化
处理建议	**1.** 检查接口（本端或对端）连线是否被频繁插拔 **2.** 通过配置以太网接口物理连接状态抑制功能调整抑制参数

51.61 LINK_UPDOWN

日志内容	Line protocol state on the interface [STRING] changed to [STRING].
日志含义	接口的链路层协议状态发生变化
参数解释	$1：接口名称 $2：协议状态，up、down
日志等级	5 (Notification)
举例	IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ethernet0/0 changed to down.
对系统的影响	如果接口物理链路状态变为down，则无法转发业务流量；如果接口物理链路状态变为up，则无影响
日志产生原因	接口的链路层协议状态发生变化
处理建议	链路层状态为down时，请使用**display interface**命令查看链路层状态，进一步定位链路层状态为down的原因

51.62 PFC_WARNING

日志内容	On interface [STRING], the rate of [STRING] PFC packets of 802.1p priority [INTEGER] exceeded the PFC early-warning threshold [INTEGER] pps. The current rate is [INTEGER].
日志含义	接口接收或者发送PFC报文的速率达到预警门限
参数解释	$1：接口名称 $2：告警方向，input、output $3：指定的802.1p优先级 $4：指定接口每秒接收的PFC帧数量，单位为pps $5：当前接口接收PFC报文的速率，单位为pps
日志等级	4 (Warning)
举例	IFNET/4/PFC_WARNING: On interface GigabitEthernet1/0/1, the rate of input PFC packets of 802.1p priority 1 exceeded the PFC early-warning threshold 50 pps. The current rate is 60.
对系统的影响	可能导致PFC报文被丢弃
日志产生原因	接口接收或者发送PFC报文的速率达到预警门限
处理建议	无需处理

51.63 PHY_UPDOWN

日志内容	Physical state on the interface [STRING] changed to [STRING].
日志含义	接口的链路状态发生变化
参数解释	$1：接口名称 $2：链路状态，up、down
日志等级	3 (Error)
举例	IFNET/3/PHY_UPDOWN: Physical state on the interface Ethernet0/0 changed to down.
对系统的影响	如果接口物理状态变为down，则无法转发业务流量；如果接口物理状态变为up，则无影响
日志产生原因	接口的链路状态发生变化
处理建议	物理层状态为down时，请检查是否没有物理连线或者链路故障。.

51.64 PROTOCOL_UPDOWN

日志内容	Protocol [STRING] state on the interface [STRING] changed to [STRING].
日志含义	接口上协议的状态发生变化
参数解释	$1：协议名称 $2：接口名称 $3：协议状态，up、down
日志等级	5 (Notification)
举例	IFNET/5/PROTOCOL_UPDOWN: Protocol IPX state on the interface Ethernet6/4/1 changed to up.
对系统的影响	如果接口协议状态变为down，则无法转发业务流量；如果接口协议状态变为up，则无影响
日志产生原因	接口上一个协议的状态发生变化
处理建议	网络层状态为down时，请检查网络层协议配置

51.65 STORM_CONSTRAIN_BELOW

日志内容	[STRING] is in controlled status, [STRING] flux falls below its lower threshold [STRING].
日志含义	该端口下任意类型的流量从超上限回落到小于下限阈值
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制下限 • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
日志等级	1 (Alert)
举例	IFNET/1/STORM_CONSTRAIN_BELOW: GigabitEthernet1/0/1 is in controlled status, BC flux falls below its lower threshold 90%.
对系统的影响	无
日志产生原因	端口处于受控状态，该端口下任意类型的流量从超上限回落到小于下限阈值
处理建议	无需处理

51.66 STORM_CONSTRAIN_CONTROLLED

日志内容	[STRING] turned into controlled status, port status is controlled, packet type is [STRING], upper threshold is [STRING].
日志含义	端口处于受控状态
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制上限 • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
日志等级	1 (Alert)
举例	IFNET/1/STORM_CONSTRAIN_CONTROLLED: GigabitEthernet1/0/1 turned into controlled status, port status is controlled, packet type is BC, upper threshold is 90%.
对系统的影响	可能会导致该类型的流量出现丢包或该端口被关闭
日志产生原因	端口处于受控状态，该端口下任意类型的流量超过配置的上限阈值
处理建议	无需处理

51.67 STORM_CONSTRAIN_EXCEED

日志内容	[STRING] is in controlled status, [STRING] flux exceeds its upper threshold [STRING].
日志含义	该端口下任意类型的流量超过配置的上限阈值
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制上限 • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
日志等级	1 (Alert)
举例	IFNET/1/STORM_CONSTRAIN_EXCEED: GigabitEthernet1/0/1 is in controlled status, BC flux exceeds its upper threshold 90%.
对系统的影响	可能会导致该类型的流量出现丢包或该端口被关闭
日志产生原因	端口处于受控状态，该端口下任意类型的流量超过配置的上限阈值
处理建议	无需处理

51.68 STORM_CONSTRAIN_NORMAL

日志内容	[STRING] returned to normal status, port status is [STRING], packet type is [STRING], lower threshold is [STRING].
日志含义	该端口下任意类型的流量从超上限回落到小于下限阈值
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制下限 • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
日志等级	1 (Alert)
举例	IFNET/1/STORM_CONSTRAIN_NORMAL: GigabitEthernet1/0/1 returned to normal status, port status is normal, packet type is BC, lower threshold is 10%.
对系统的影响	无
日志产生原因	端口处于正常状态，该端口下任意类型的流量从超上限回落到小于下限阈值
处理建议	无需处理

51.69 TUNNEL_LINK_UPDOWN

日志内容	Line protocol state on the interface [STRING] changed to [STRING].
日志含义	Tunnel接口的链路层协议状态发生变化
参数解释	$1：接口名称 $2：协议状态，up、down
日志等级	5 (Notification)
举例	IFNET/5/TUNNEL_LINK_UPDOWN: Line protocol state on the interface Tunnel1 changed to down.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	Tunnel接口的链路层协议状态发生变化
处理建议	链路层状态为down时，请使用**display interface**命令查看链路层状态，进一步定位链路层状态为down的原因

51.70 TUNNEL_PHY_UPDOWN

日志内容	Physical state on the interface [STRING] changed to [STRING].
日志含义	Tunnel接口的链路状态发生变化
参数解释	$1：接口名称 $2：链路状态，up、down
日志等级	3 (Error)
举例	IFNET/3/TUNNEL_PHY_UPDOWN: Physical state on the interface Tunnel1 changed to down.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	Tunnel接口的链路状态发生变化
处理建议	物理层状态为down时，请检查是否没有物理连线或者链路故障

51.71 VLAN_MODE_CHANGE

日志内容	Dynamic VLAN [INT32] has changed to a static VLAN.
日志含义	创建VLAN导致动态VLAN转换成静态VLAN
参数解释	$1：VLANID
日志等级	5 (Notification)
举例	IFNET/5/VLAN_MODE_CHANGE: Dynamic VLAN 20 has changed to a static VLAN.
对系统的影响	无
日志产生原因	创建VLAN接口导致动态VLAN转换成静态VLAN
处理建议	无需处理

52 IGMP

本节介绍 IGMP 模块输出的日志信息。

52.1 IGMP_GROUP_JOIN

日志内容	Interface receives an IGMP Join message. (IfName=[STRING], IfIndex=[UINT32], Version=[STRING], SrcAddr=[STRING], GrpAddr=[STRING], HostAddr=[STRING], VPNName=[STRING])
日志含义	接收到组播IGMPv1、IGMPv2加入报文
参数解释	$1：接口名称 $2：接口索引 $3：IGMP版本：IGMPv1、IGMPv2 $4：组播源地址 $5：组播组地址 $6：发送报文的主机地址 $7：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6(Notification)
举例	IGMP/6/IGMP_GROUP_JOIN: Interface receives an IGMP Join message. (IfName=GigabitEthernet 1/0/1, IfIndex=257, Version=IGMPv2, SrcAddr=192.168.1.3, GrpAddr=236.1.1.1, HostAddr=10.1.2.1, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	设备接收到组播IGMPv1、IGMPv2加入报文
处理建议	无需处理

52.2 IGMP_GROUP_LEAVE

日志内容	Interface receives an IGMP Leave message or corresponding group timer on this interface expires. (IfName=[STRING], IfIndex=[UINT32], SrcAddr=[STRING], GrpAddr=[STRING], VPNName=[STRING])
日志含义	设备接收到组播IGMPv1、IGMPv2离开报文
参数解释	$1：接口名称 $2：接口索引 $3：组播源地址 $4：组播组地址 $5：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6 (Notification)
举例	IGMP/6/IGMP_GROUP_LEAVE: Interface receives an IGMP Leave message or corresponding group timer on this interface expires. (IfName=GigabitEthernet 1/0/1, IfIndex=257, SrcAddr=192.168.1.3, GrpAddr=236.1.1.1, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	设备接收到组播IGMPv1、IGMPv2成员离开报文
处理建议	无需处理

53 IKE

本节介绍 IKE 模块输出的日志信息。

53.1 IKE_P1_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 1 SA in [STRING] mode [STRING] state. Reason: [STRING]. SA information: • Role: [STRING] • Local IP: [STRING] • Local ID type: [STRING] • Local ID: [STRING] • Local port: [UINT32] • Retransmissions: [UINT32] • Remote IP: [STRING] • Remote ID type: [STRING] • Remote ID: [STRING] • Remote port: [UINT32] • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32] • IKE profile name: [STRING]
日志含义	IKE建立第一阶段SA协商失败
参数解释	$1：协商模式，主模式或者野蛮模式 $2：协商状态机状态 $3：失败原因： • 认证对端签名失败，显示为：Failed to verify the peer signature • 缺少 HASH 载荷，显示为：HASH payload is missing • 认证对端 HASH 失败，显示为：Failed to verify the peer HASH. Local HASH is %s. Peer HASH is %s • 缺少签名载荷，显示为：Signature payload is missing • 从证书中获取摘要名称失败，显示为：Failed to get subject name from certificate • 获取证书失败，显示为：Failed to get certificate • 获取本地证书失败，显示为：Failed to get local certificate • 获取私钥失败，显示为：Failed to get private key • 认证对端证书失败，显示为：Failed to verify the peer certificate (%s) • 从 ID 载荷中获取 ID 数据失败，显示为：Failed to get ID data for constructing ID payload • 无效的 ID 载荷长度，显示为：Invalid ID payload length: %d • 无效的 ID 载荷协议和端口号，显示为：Invalid ID payload with protocol %u and port %u

	• 无效的 ID 类型，显示为：Invalid ID type (%u) • 不支持的属性，显示为：Unsupported attribute %u • 属性重复，显示为：Attribute %s is repeated • 不支持的 DOI，显示为：Unsupported DOI %s • 不支持的 DOI 场景，显示为：Unsupported IPsec DOI situation (%u) • KE（KEY EXCHANGE）载荷不存在，显示为：KE payload is missing • 无效的 KE 载荷长度，显示为：Invalid KE payload length (%lu) • 无效的 Nonce 载荷长度，显示为：Invalid nonce payload length (%lu) • 无可用的提议，显示为：No available proposal • 解析证书请求载荷失败，显示为：Failed to parse the Cert Request payload • 提议载荷必须为 SA 载荷中的最后一个载荷，但提议载荷后有载荷，显示为：The proposal payload must be the last payload in the SA payload, but it is found followed by the %s payload • 提议载荷中出现非预期的协议 ID，显示为：Unexpected protocol ID (%u) found in proposal payload • 提议载荷中缺少变换载荷，显示为：No transform payload in proposal payload • 变换载荷编号非递增，显示为：Transform number is not monotonically increasing • 无效的变换载荷 ID，显示为：Invalid transform ID (%s) • 没有找到匹配的变换载荷，显示为：No acceptable transform • 提议载荷中出现非预期的载荷，显示为：Unexpected %s payload in proposal • 提议载荷中存在无效的 SPI 长度，显示为：Invalid SPI length (%d) in proposal payload • 一个提议载荷中只能存在一个变换载荷，当前存在多个变换载荷，显示为：Only one transform is permitted in one proposal, but %u transforms are found • 在 profile 下未找到匹配的提议，显示为：Failed to find matching proposal in profile %s • 在 profile 下没有找到提议，显示为：Failed to find proposal %u in profile %s • 在 profile 下没有找到 keychain，显示为：Failed to find keychain %s in profile %s • 重传超时，显示为：Retransmission timeout • 配置错误，显示为：Incorrect configuration • 构造证书请求载荷失败，显示为：Failed to construct certificate request payload • 收到错误通知，显示为：An error notification is received • 添加 Tunnel 失败，显示为：Failed to add tunnel $4：建立IPsec SA的角色，发起者或者响应者 $5-$9：本端信息 $10-$14: 远端信息 $15: 内部VPN实例 $16: 外部VPN实例 $17-$18: 发起者Cookie和响应者Cookie $19: 连接号 $20: IKE Tunnel编号，默认值为4294967295 $21: IKE profile名称

日志等级	6 (Informational)
举例	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA in main mode IKE_P1_STATE_SEND1 state. Reason: Failed to get certificate. SA information: • Role: Initiator • Local IP: 4.4.4.4 • Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR • Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance : bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Connection ID: 1 • Tunnel ID: 1 • IKE profile name: abc
对系统的影响	无法建立IKE SA
日志产生原因	• 两端的 IKE 安全提议参数、IKE 认证算法不一致 • 两端的预共享密钥不一致 • 证书不可用或证书无效 • 物理链路状态不佳或对等体网络不可达
处理建议	• 检查两端的 IKE 安全提议参数、IKE 认证算法是否一致，若不一致请修改为一致 • 检查两端的预共享密钥是否一致，若不一致请修改为一致 • 检查是否已获取证书，若已获取证书则检查证书是否在有效期内，若未获取证书或证书已失效请重新获取证书 • 检查物理链路状态和对等体网络是否可达，若物理链路状态不佳或对等体网络不可达请排查网络故障 执行以上检查后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

53.2 IKE_P2_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 2 SA in [STRING] state. Reason: [STRING]. SA information: • Role: [STRING]. • Local address: [STRING]. • Remote address: [STRING]. • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: Protocol:[STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING]. • Outside VPN instance: [STRING]. • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING]. • Message ID: [STRING]. • Connection ID: [UINT32]. • Tunnel ID: [UINT32].
日志含义	IKE建立第二阶段SA失败
参数解释	$1：协商状态机状态 $2：失败原因： • 构造 ID 载荷失败，显示为：Failed to construct ID payload • 计算 HASH 算法失败，显示为：Failed to calculate %s • 验证 HASH 算法失败，显示为：Failed to validate %s • 计算密钥材料失败，显示为：Failed to compute key material • 配置错误，显示为：Incorrect configuration • 转换 IPsec SA 失败，显示为：Failed to switch IPsec SA • Nonce 载荷不存在，显示为：The nonce payload doesn't exist • 无效的 Nonce 载荷长度，显示为：Invalid nonce payload length (%lu) • SA 载荷中没有有效的 DH group 描述，显示为：No valid DH group description in SA payload • KE 载荷不存在，显示为：The KE payload doesn't exist • 存在多个 KE 载荷，显示为：Too many KE payloads • KE 载荷长度与 DH group 描述不匹配，显示为：The length of the KE payload doesn't match the DH group description • 获取 SP 时与 IPsec 通信失败，显示为：Failed to send message to IPsec when getting SP • 获取 SPI 时与 IPsec 通信失败，显示为 Failed to send message to IPsec when getting SPI • 添加 IPsec SA 失败，显示为：Failed to add phase 2 SA

	• 二阶段报文重传超时，显示为：Retransmission of phase 2 packet timed out • 二阶段双方同时发起协商冲突，显示为：Collision detected in phase 2 negotiation • 未找到匹配的提议，显示为：No matching proposal found between the local and remote ends • 变换载荷编号非递增，显示为：Transform number is not monotonically increasing • 提议载荷存在的变换载荷比指定变换载荷多，显示为：Proposal payload has more transforms than specified in the proposal payload • 提议载荷存在的变换载荷比指定变换载荷少，显示为：Proposal payload has less transforms than specified in the proposal payload • IPsec 变换载荷中属性重复，显示为：Attribute %d is repeated in IPsec transform %d • 报文中 SA_LIFE_TYPE 属性重复，显示为：SA_LIFE_TYPE attribute is repeated in packet • 消息中的 SA_LIFE_TYPE 属性必须在 SA_LIFE_DURATION 属性前，显示为 The SA_LIFE_TYPE attribute must be in front of the SA_LIFE_DURATION attribute • 不支持的 IPsec 属性，显示为：Unsupported IPsec attribute %s • IPsec 安全提议必须指定封装模式，显示为：The encapsulation mode must be specified in the IPsec transform set • IPsec 提议的 SPI 长度超出范围，显示为：Invalid SPI length (%u) in IPsec proposal • IPsec 提议中的 SPI 无效，显示为：Invalid SPI (%u) in IPsec proposal • 变换载荷中的变换 ID 与认证算法不匹配，显示为：The Transform ID (%d) in transform %d doesn't match authentication algorithm %s (%u) • 从提议中获取 SPI 失败，显示为：Failed to get SPI from proposal • IPsec 提议中没有变换载荷，显示为：No transform in IPsec proposal • 同一个提议中存在多个 AH 提议，显示为：A proposal payload contains more than one AH proposal • 提议中存在无效的下一个载荷，显示为：Invalid next payload (%u) in proposal • 没有 ESP 或 AH 提议，显示为：No ESP or AH proposal • 不支持的 DOI，显示为：Unsupported DOI • 不支持的 DOI 场景，显示为：Unsupported IPsec DOI situation (%u) • 无效的 IPsec 提议，显示为：Invalid IPsec proposal %u • 重协商 IPsec SA 时获取 IPsec 策略失败，显示为：Failed to get IPsec policy when renegotiating IPsec SA • P2 阶段响应方获取 IPsec 策略失败，显示为：Failed to get IPsec policy as phase 2 responder $3：建立IPsec SA的角色，发起者或者响应者 $4：本端IP地址 $5：远端IP地址 $6-$11: 数据流 $12: 内部VPN实例 $13: 外部VPN实例 $14: 入方向AH SPI $15: 出方向AH SPI $16: 入方向ESP SPI $17: 出方向ESP SPI

	$18-$19: 发起者Cookie和响应者Cookie $20: 消息ID $21: 连接号 $22: IKE Tunnel编号，默认值为4294967295
日志等级	6 (Informational)
举例	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA in IKE_P2_STATE_GETSPI state. Reason: Failed to get SPI from proposal. SA information: • Role: Responder • Local address: 2.2.2.2 • Remote address: 1.1.1.1 • Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP • Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP • Inside VPN instance: aaa • Outside VPN instance: bbb • Inbound AH SPI: 192365458 • Outbound AH SPI: 13654581 • Inbound ESP SPI: 292334583 • Outbound ESP SPI: 5923654586 • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1 • Tunnel ID: 1
对系统的影响	无法建立IPsec SA
日志产生原因	• 两端的 IPsec 安全提议参数、IPsec 认证算法、IPsec 加密算法、IPsec 封装模式不一致 • 两端的 IPsec policy 配置不一致 • 两端引用的 ACL 配置不为镜像配置 • 物理链路状态不佳或对等体网络不可达
处理建议	• 检查两端的 IPsec 安全提议参数、IPsec 认证算法、IPsec 加密算法、IPsec 封装模式是否一致，若不一致请修改为一致 • 检查两端的 IPsec policy 配置是否一致，若不一致请修改为一致 • 检查两端引用的 ACL 配置是否为镜像配置，若不为镜像配置请修改为镜像配置 • 检查物理链路状态和对等体网络是否可达，若物理链路状态不佳或对等体网络不可达请排查网络故障 执行以上检查后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

53.3 IKE_P2_SA_TERMINATE

日志内容	The IKE phase 2 SA was deleted. Reason: [STRING]. SA information: • Role: [STRING] • Local address: [STRING] • Remote address: [STRING] • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Message ID: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32]
日志含义	IKE第二阶段SA删除
参数解释	$1：删除原因： • 硬超时，显示为：The SA expired • 收到 IPsec SA 删除消息，显示为：An IPsec SA deletion message was received from peer • 新的 P2 SA 已协商，旧的删除，显示为：New P2 SA had been negotiated, and the old one was deleted • 删除所有 SA，显示为：All P2 SAs were deleted • 按 SPID 删除 SA，显示为：The P2 SA was deleted by SPID • 按接口删除 SA，显示为：The P2 SA was deleted by IFIndex • 按 SA 索引删除 SA，显示为：The P2 SA was deleted by SA index $2：建立IPsec SA的角色，发起者或者响应者 $3：本端IP地址 $4：远端IP地址 $5-$10: 数据流 $11: 内部VPN实例 $12: 外部VPN实例 $13: 入方向AH SPI $14: 出方向AH SPI $15: 入方向ESP SPI $16: 出方向ESP SPI $17-$18: 发起者Cookie和响应者Cookie

	$19: 消息ID. $20: 连接号 $21: IKE Tunnel编号，默认值为4294967295
日志等级	6 (Informational)
举例	IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted. Reason: An IPsec SA deletion message was received. SA information: • Role: Responder • Local address: 2.2.2.2 • Remote address: 1.1.1.1 • Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP • Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP • Inside VPN instance: aaa • Outside VPN instance: bbb • Inbound AH SPI: 192365458 • Outbound AH SPI: 13654581 • Inbound ESP SPI: 292334583 • Outbound ESP SPI: 5923654586 • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1 • Tunnel ID: 1
对系统的影响	IKE第二阶段SA被删除，该SA承载的IPsec业务中断
日志产生原因	IKE第二阶段SA由于过期失效被删除，或者手工删除了SA，具体原因见日志内容原因字段
处理建议	• 由于本日志所列原因导致的 SA 被删除后，SA 会重新协商建立，属于正常情况，无需处理 • 如果是其他原因导致 SA 被删除，请收集配置文件、日志信息和告警信息，并联系技术支持人员

53.4 IKE_VERIFY_CERT_FAIL

日志内容	Failed to verify the peer certificate. Reason: [STRING].
日志含义	验证对端证书失败
参数解释	$1：失败原因： • 获取颁发者证书失败，显示为：unable to get issuer certificate. • 无法获取证书的 CRL，显示为：unable to get certificate CRL. • 无法解密 CRL 的签名，显示为：unable to decrypt CRL's signature. • 无法解析颁发者的公钥，显示为：unable to decode issuer public key. • 证书签名错误，显示为：certificate signature failure. • CRL 签名失败，显示为：CRL signature failure. • 解密证书签名失败，显示为：unable to decrypt certificate's signature. • 证书尚未生效，显示为：certificate is not yet valid. • 证书已失效，显示为：certificate has expired. • CRL 尚未生效，显示为：CRL is not yet valid. • CRL 已经失效，显示为：CRL has expired. • 证书的起始时间格式错误，显示为：format error in certificate's notBefore field. • 证书的结束时间格式错误，显示为：format error in certificate's notAfter field. • CRL 的上次更新时间格式错误，显示为：format error in CRL's lastUpdate field. • CRL 的下次更新时间格式错误，显示为：format error in CRL's nextUpdate field. • 内存不足，显示为：out of memory. • 自签名证书，显示为：self signed certificate. • 证书链中存在自签名证书，显示为：self signed certificate in certificate chain. • 获取本地颁发者证书失败，显示为：unable to get local issuer certificate. • 验证首个证书失败，显示为：unable to verify the first certificate. • 证书链过长，显示为：certificate chain too long. • 证书被撤回，显示为：certificate revoked. • 无效的 CA 证书，显示为：invalid CA certificate. • 无效的非 CA 证书，显示为：invalid non-CA certificate (has CA markings). • 超过路径深度约束，显示为：path length constraint exceeded. • 超过代理路径深度约束，显示为：proxy path length constraint exceeded. • 代理证书不通过，请设置合适的标记，显示为：proxy certificates not allowed, please set the appropriate flag. • 不支持的证书用途，显示为：unsupported certificate purpose. • 证书不被信任，显示为：certificate not trusted. • 证书被拒绝，显示为：certificate rejected. • 证书应用验证失败，显示为：application verification failure. • 证书主题颁发者不匹配，显示为：subject issuer mismatch. • 授权和主题密钥认证人不匹配，显示为：authority and subject key identifier mismatch. • 授权和颁发者序列号不匹配，显示为：authority and issuer serial number

	mismatch. • 密钥用途不包括证书签名，显示为：key usage does not include certificate signing. • 获取 CRL 颁发者证书失败，显示为：unable to get CRL issuer certificate. • 不受控的决定性的扩展，显示为：unhandled critical extension. • 密钥用途不包括 CRL 签名，显示为：key usage does not include CRL signing. • 密钥用途不包括数字签名，显示为：key usage does not include digital signature. • 不受控的决定性的 CRL 扩展，显示为：unhandled critical CRL extension. • 无效或不一致的证书扩展，显示为：invalid or inconsistent certificate extension. • 无效或不一致的证书策略扩展，显示为：invalid or inconsistent certificate policy extension. • 不存在明确的策略，显示为：no explicit policy. • CRL 范围不同，显示为：Different CRL scope. • 不支持的扩展特性，显示为：Unsupported extension feature. • RFC 3779 资源不是父资源的子集，显示为：RFC 3779 resource not subset of parent's resources. • 被允许的子树违规，显示为：permitted subtree violation. • 被排除的子树违规，显示为：excluded subtree violation. • 名字约束的最小和最大范围不支持，显示为：name constraints minimum and maximum not supported. • 不支持的名字约束类型，显示为：unsupported name constraint type. • CRL 路径检验失败，显示为：CRL path validation error. • 不支持的或无效的名字语法，显示为：unsupported or invalid name syntax. • 不支持的或无效的名字约束语法，显示为：unsupported or invalid name constraint syntax. • Suite B：证书版本号无效，显示为：Suite B: certificate version invalid. • Suite B：无效的公钥算法，显示为：Suite B: invalid public key algorithm. • Suite B：无效的 ECC 曲线，显示为：Suite B: invalid ECC curve. • Suite B：无效的签名算法，显示为：Suite B: invalid signature algorithm. • Suite B：曲线不被本 LOS 准许，显示为：Suite B: curve not allowed for this LOS. • Suite B：不能使用 P-256 给 P-384 签名，显示为：Suite B: cannot sign P-384 with P-256. • 主机名不匹配，显示为：Hostname mismatch. • 邮件地址不匹配，显示为：Email address mismatch. • IP 地址不匹配，显示为：IP address mismatch. • 无效的证书认证上下文，显示为：Invalid certificate verification context. • 颁发者证书检查失败，显示为：Issuer certificate lookup error. • 代理主题名称不规范，显示为：proxy subject name violation.

日志等级	6 (Informational)
举例	IKE/6/IKE_VERIFY_CERT_FAIL: Failed to verify the peer certificate. Reason: invalid or inconsistent certificate extension.
对系统的影响	IKE协商失败
日志产生原因	证书格式错误、证书签名错误等，具体原因见日志内容原因字段
处理建议	• 请根据错误提示信息检查证书问题 • 如果问题仍然无法解决，请收集配置文件、日志信息和告警信息，并联系技术支持人员

54 IMA

本节介绍 IMA（Integrity Measurements Architecture，完整性度量架构）模块输出的日志信息。

54.1 IMA_ALLOCATE_FAILED

日志内容	Failed to allocate resource for file [STRING].
日志含义	给目标文件分配资源失败
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	IMA/4/IMA_ALLOCATE_FAILED: Failed to allocate resource for file /sbin/tcsmd.
对系统的影响	可信状态变为不可信
日志产生原因	IMA给度量目标文件分配资源失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

54.2 IMA_DATA_ERROR

日志内容	Can't collect data of file [STRING].
日志含义	收集目标文件的数据失败
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	IMA/4/IMA_DATA_ERROR: Can't collect data of file /sbin/tcsmd.
对系统的影响	可信状态变为不可信
日志产生原因	可能有如下原因： • 打开或读取文件失败 • 计算文件 Hash 值出错
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

54.3 IMA_FILE_HASH_FAILED

日志内容	Hash value of file [STRING] is not consistent with that in the RM file.
日志含义	目标文件的Hash值与RM文件中该文件的Hash值不匹配
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	IMA/4/IMA_FILE_HASH_FAILED: Hash value of file /sbin/tcsmd is not consistent with that in the RM file.
对系统的影响	可信状态变为不可信
日志产生原因	目标文件的Hash值与RM文件中该文件的Hash值不匹配
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

54.4 IMA_RM_FILE_MISS

日志内容	File [STRING] is missing in the RM file.
日志含义	RM文件中未找到目标文件的信息
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	IMA/4/IMA_RM_FILE_MISS: File /sbin/tcsmd is missing in the RM file.
对系统的影响	可信状态变为不可信
日志产生原因	RM文件中未找到目标文件的信息
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

54.5 IMA_RM_HASH_MISS

日志内容	Hash value of file [STRING] is missing in the RM file.
日志含义	RM文件中没有目标文件的Hash值
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	IMA/4/IMA_RM_HASH_MISS: Hash value of file /sbin/tcsmd is missing in the RM file.
对系统的影响	可信状态变为不可信
日志产生原因	可能目标文件在度量时使用的Hash算法在RM中不支持
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

54.6 IMA_TEMPLATE_ERROR

日志内容	Failed to extend template hash value of file [STRING] to the PCR.
日志含义	将目标文件的模板Hash值扩展到PCR失败
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	IMA/4/IMA_TEMPLATE_ERROR: Failed to extend template hash value of file /sbin/tcsmd to the PCR.
对系统的影响	可信状态变为不可信
日志产生原因	将目标文件的模板Hash值扩展到PCR失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

55 iNOF

本节包含 iNOF（Intelligent Lossless NVMe Over Fabric，智能无损存储网络）模块的日志消息。

55.1 INOF_ADD_HOST

日志内容	The iNOF host is created from the [STRING] device, host's IP is [STRING], port name is [STRING].
日志含义	iNOF检测到新主机上线，打印主机的相关信息
参数解析	$1：设备分类，取值为： • Local：表示主机通过本设备上线 • Remote：表示主机通过 iNOF 网络中的其它传输设备上线 $2：主机的IP地址 $3：当设备分类为Local时，本参数表示主机的接入端口；当设备分类为Remote时，本参数表示设备同步到主机信息的端口
日志等级	5 (Notification)
举例	INOF/5/INOF_ADD_HOST: The iNOF host is created from the local device, host's IP is 1.1.1.1, port name is GE0/0/1.
对系统的影响	对系统无影响
日志产生原因	iNOF检测到新主机上线
处理建议	无需处理

55.2 INOF_DELETE_HOST

日志内容	The iNOF host is deleted from the [STRING] device, because of [STRING], host's IP is [STRING], port name is [STRING].
日志含义	iNOF检测到主机下线，打印下线原因以及主机的相关信息
参数解析	$1：设备分类 • Local：表示主机通过本设备上线 • Remote：表示主机通过 iNOF 网络中的其它传输设备上线 $2：设备下线原因，取值为： • link down：链接断开 • pfc deadlock：PFC 死锁 • network malfunction：网络故障 • zone configuration changes：域配置变更 • endpoint configuration changes：主机配置发生了变化（例如 IP 地址变化等） • lldp aged out：LLDP 老化 • unknown：未知 $3：主机的IP地址 $4：接入端口
日志等级	5 (Notification)
举例	INOF/5/INOF_DELETE_HOST: The iNOF host is deleted from the local device, because of link down. host's IP is 1.1.1.1, port name is GE0/0/1.
对系统的影响	对系统无影响
日志产生原因	iNOF检测到主机下线
处理建议	请根据主机下线的原因进行处理： • 如果下线原因为 link down，请检查主机与 iNOF 传输设备之间的链路是否通畅 • 如果下线原因为 pfc deadlock，请检查 PFC 状态 • 如果下线原因为 network malfunction，请检查网络状态 • 如果下线原因为 zone configuration changes，请检查 iNOF 域的配置是否正确 • 如果下线原因为 endpoint configuration changes，请检查主机的配置信息 • 如果下线原因为lldp aged out，请使用 **`display lldp status`**命令检查设备的LLDP状态

55.3 INOF_LICENSE_ACTIVE

日志内容	The license for the iNOF feature is activated and the iNOF service will run normally.
日志含义	iNOF特性License已经激活，iNOF服务即将正常运行
参数解释	无
日志等级	5 (Notification)
举例	INOF/5/INOF_LICENSE_ACTIVE: The license for the iNOF feature is activated and the iNOF service will run normally.
对系统的影响	对系统无影响
日志产生原因	安装了iNOF特性License
处理建议	无需处理

55.4 INOF_LICENSE_EXPIRE

日志内容	The license for the iNOF feature will expire in [UINT32] days.
日志含义	iNOF License将在指定天数后过期
参数解释	$1：License即将过期的天数，取值范围为1到30天
日志等级	5 (Notification)
举例	INOF/5/INOF_LICENSE_EXPIRE: The license for the iNOF feature will expire in 5 days.
对系统的影响	对系统无影响
日志产生原因	iNOF License将在指定天数后过期
处理建议	请在License过期前安装新的License。否则，License到期后，将不允许使用iNOF功能

55.5 INOF_NO_LICENSE

日志内容	The iNOF feature is disabled, because its license has expired or has been uninstalled.
日志含义	iNOF特性被禁用，因为iNOF License过期或者被卸载了
参数解释	无
日志等级	4 (Warning)
举例	INOF/4/INOF_NO_LICENSE: The iNOF feature is disabled, because its license has expired or has been uninstalled.
对系统的影响	不允许使用iNOF功能
日志产生原因	iNOF特性被禁用，因为iNOF License过期或者被卸载了
处理建议	请尽快安装iNOF License

56 iNQA

本节介绍 iNQA（Intelligent Network Quality Analyzer，智能网络质量分析）模块输出的日志信息。

56.1 INQA_BWD_LOSS_EXCEED

日志内容	Packet loss rate of the backward flow in instance [UINT] exceeded the upper limit.
日志含义	反向流的丢包率大于丢包超限告警值
参数解释	$1：实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_BWD_LOSS_EXCEED: Packet loss rate of the backward flow in instance 1 exceeded the upper limit.
对系统的影响	丢包率过大，可能无法满足业务对丢包率的要求，影响业务
日志产生原因	开启反向流的丢包统计，iNQA会按周期统计丢包率。如果连续五个周期的丢包率都大于等于丢包超限阈值，表示该实例中丢包过多，Analyzer会生成丢包超限日志 产生此日志的可能原因包括： • 异常流量造成网络拥塞 • 链路状态不稳定
处理建议	1. 检查此日志生成时网络中是否存在异常流量 2. 检查此日志生成时网络中链路状态是否稳定。排查并消除链路状态不稳定的因素 3. 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

56.2 INQA_BWD_LOSS_RECOV

日志内容	Packet loss rate of the backward flow in instance [UINT] recovered.
日志含义	反向流的丢包率恢复到正常状态
参数解释	$1：实例号
日志等级	6 (Informational)
举例	INQA/6/INQA_BWD_LOSS_RECOV: Packet loss rate of the backward flow in instance 1 recovered.
对系统的影响	对系统无影响
日志产生原因	iNQA在按周期统计反向流的丢包率时，如果连续五个周期的丢包率都小于丢包超限恢复阈值，表示该实例中丢包率已经恢复到正常范围，Analyzer会生成此日志
处理建议	无需处理

56.3 INQA_DEBUG_FAIL

日志内容	Setting debugging switch to drive failed.
日志含义	将iNQA日志开关配置下发给驱动失败
参数解释	无
日志等级	5 (Notification)
举例	INQA/5/INQA_DEBUG_FAIL: Setting debugging switch to drive failed.
对系统的影响	对系统无影响
日志产生原因	iNQA Debug开关配置下发驱动失败
处理建议	1. 执行 **display debugging**命令查看iNQA Debug开关的开启状态 2. 在用户视图使用 **debugging inqa**命令重新配置iNQA Debug开关

56.4 INQA_FLAG_DIFF

日志内容	Flags of collectors bound with the analyzer instance [UINT] are inconsistent.
日志含义	Analyzer实例下关联的Collector上配置的染色位不一致
参数解释	$1：Analyzer实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_FLAG_DIFF: Flags of collectors bound with the analyzer instance 1 are inconsistent.
对系统的影响	对系统无影响
日志产生原因	配置错误
处理建议	1. 执行 **display inqa analyzer instance**命令，检查该Analyzer实例下关联的所有Collector的ID 2. 分别登录每台Collector，执行 **display inqa collector**命令查看Loss-measure flag字段的取值，如果配置错误，请在Collector视图下，使用 **flag**命令修改配置

56.5 INQA_FLAG_FAIL

日志内容	Setting coloring bit to drive failed.
日志含义	将染色位配置下发给驱动失败
参数解释	无
日志等级	5 (Notification)
举例	INQA/5/INQA_FLAG_FAIL: Setting coloring bit to drive failed.
对系统的影响	对系统无影响
日志产生原因	可能为原因为：硬件资源不够
处理建议	1. 使用 **display qos-acl resource**命令查看设备的ACL资源是否足够。如果ACL资源不足，请删除暂时无需使用的ACL后，再重新配置染色位 2. 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

56.6 INQA_FLOW_DIFF

日志内容	Flows of collectors bound with the analyzer instance [UINT] are inconsistent.
日志含义	Analyzer实例下关联的Collector端发送过来的报文中携带的目标流参数不一致
参数解释	$1：Analyzer实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_FLOW_DIFF: Flows of collectors bound with the analyzer instance 1 are inconsistent.
对系统的影响	对系统无影响
日志产生原因	配置错误
处理建议	1. 执行 **display inqa analyzer instance**命令，检查该Analyzer实例下关联的所有Collector的ID 2. 分别登录每台Collector，执行 **display inqa collector**命令查看Flow configuration字段的取值。如果配置不一致，请在Collector实例视图下，使用 **flow**命令修改配置

56.7 INQA_FWD_LOSS_EXCEED

日志内容	Packet loss rate of the forward flow in instance [UINT] exceeded the upper limit.
日志含义	正向流的丢包率大于丢包超限告警值
参数解释	$1：实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_FWD_LOSS_EXCEED: Packet loss rate of the forward flow in instance 1 exceeded the upper limit.
对系统的影响	丢包率过大，可能无法满足业务对丢包率的要求，影响业务
日志产生原因	开启正向流的丢包统计，iNQA会按周期统计丢包率。如果连续五个周期的丢包率都大于等于丢包超限阈值，表示该实例中丢包过多，Analyzer会生成丢包超限日志 产生此日志的可能原因包括： • 异常流量造成网络拥塞 • 链路状态不稳定
处理建议	**1.** 检查此日志生成时网络中是否存在异常流量 **2.** 检查此日志生成时网络中链路状态是否稳定。排查并消除链路状态不稳定的因素 **3.** 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

56.8 INQA_FWD_LOSS_RECOV

日志内容	Packet loss rate of the forward flow in instance [UINT] recovered.
日志含义	正向流的丢包率恢复到正常状态
参数解释	$1：实例号
日志等级	6 (Informational)
举例	INQA/6/INQA_FWD_LOSS_RECOV: Packet loss rate of the forward flow in instance 1 recovered.
对系统的影响	对系统无影响
日志产生原因	iNQA在按周期统计正向流的丢包率时，如果连续五个周期的丢包率都小于丢包超限恢复阈值，表示该实例中丢包率已经恢复到正常范围，Analyzer会生成此日志
处理建议	无需处理

56.9 INQA_INIT_ERROR

日志内容	Failed to issue the configuration of instance [UINT] to drive because the MPs in the instance are mutually exclusive.
日志含义	由于该实例中MP之间的配置互斥，导致实例配置下发给驱动失败
参数	$1：实例的编号
日志等级	5 (Notification)
举例	INQA/5/INQA_INIT_ERROR: Failed to issue the configuration of instance 1 to drive because the MPs in the instance are mutually exclusive.
对系统的影响	这个iNQA实例无法正常工作
日志产生原因	该实例中MP之间的配置互斥
处理建议	检查实例下的配置，删除冲突配置

56.10 INQA_INST_FAIL

日志内容	Setting instance [UINT] information to drive failed.
日志含义	将iNQA实例配置下发给驱动失败
参数解释	$1：实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_INST_FAIL: Setting instance 1 information to drive failed.
对系统的影响	对系统无影响
日志产生原因	可能原因为：硬件资源不足
处理建议	1. 使用 **display qos-acl resource**命令查看设备的ACL资源是否足够。如果ACL资源不足，请删除暂时无需使用的ACL后，再重新配置iNQA实例参数 2. 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

56.11 INQA_INTVL_DIFF

日志内容	Intervals of collectors bound with analyzer instance [UINT] are inconsistent.
日志含义	Analyzer实例下关联的Collector端发送过来的报文携带的iNQA统计周期值不一致
参数解释	$1：Analyzer实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_INTVL_DIFF: Intervals of collectors bound with analyzer instance 1 are inconsistent.
对系统的影响	对系统无影响
日志产生原因	配置错误
处理建议	1. 执行 **display inqa analyzer instance**命令，检查该Analyzer实例下关联的所有Collector的ID 2. 分别登录每台Collector，执行 **display inqa collector**命令查看Interval字段的取值。如果配置错误，请在Collector实例视图下，使用 **interval**命令修改配置

56.12 INQA_MP_NOIF

日志内容	No statistics on MP [UINT]. Reason: [TEXT],
日志含义	iNQA实例配置失败
参数解释	$1：无统计信息的原因，取值为： • The MP does not bound to any interface：MP 没有绑定接口 • The interface bound with the MP does not exist：MP 绑定的接口不存在
日志等级	5 (Notification)
举例	INQA/5/INQA_MP_NOIF: No statistics on MP 1. Reason: The MP does not bound to any interface.
对系统的影响	对系统无影响
日志产生原因	MP上没有统计到数据，原因是MP没有绑定任何接口
处理建议	1. 执行 **display inqa collector instance**命令显示Collector实例的配置信息，通过显示信息中的MP configuration字段查看MP的配置以及MP绑定的接口 2. 如果接口绑定错误或者未绑定接口，请在接口视图下执行 **inqa mp**命令将接口和MP绑定 3. 如果MP绑定了正确的接口，请执行 **display interface**命令查看接口状态。如果接口状态为down，请先解决接口故障 4. 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

56.13 INQA_NO_RESOURCE

日志内容	Failed to configure instance [UINT] due to insufficient resources.
日志含义	iNQA实例配置失败
参数解释	$1：实例号
日志等级	5 (Notification)
举例	INQA/5/INQA_NO_RESOURCE: Failed to configure instance 1 due to insufficient resources.
对系统的影响	对系统无影响
日志产生原因	由于ACL表项资源不足，导致iNQA实例配置失败
处理建议	1. 使用 **display qos-acl resource**命令查看设备的ACL资源是否足够。如果ACL资源不足，请删除暂时无需使用的ACL后，再重新配置iNQA实例 2. 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

56.14 INQA_NO_SUPPORT

日志内容	iNQA is not supported in this slot.
日志含义	指定slot不支持iNQA功能
参数解释	无
日志等级	5 (Notification)
举例	INQA/5/INQA_NO_SUPPORT: **-Slot=1**; iNQA is not supported in this slot.
对系统的影响	对系统无影响
日志产生原因	硬件不支持iNQA功能
处理建议	iNQA功能需要硬件支持。请更换支持iNQA的单板，或者将需要测量的流量切换到支持iNQA的slot上

56.15 INQA_SMOOTH_BEGIN_FAIL

日志内容	Setting smoothing beginning to kernel failed.
日志含义	iNQA模块通知内核平滑开始，通知失败（平滑指的是iNQA将用户态的iNQA表项和内核的iNQA表项进行比较、同步的操作，以便确保用户态的iNQA表项和内核的iNQA表项完全相同）
参数解释	无
日志等级	5 (Notification)
举例	INQA/5/INQA_SMOOTH_BEGIN_FAIL: Setting smoothing beginning to kernel failed.
对系统的影响	对系统无影响
日志产生原因	软件内部通信故障
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

56.16 INQA_SMOOTH_END_FAIL

日志内容	Setting smoothing ending to kernel failed.
日志含义	iNQA模块通知内核平滑结束，通知失败（平滑指的是iNQA将用户态的iNQA表项和内核的iNQA表项进行比较、同步的操作，以便确保用户态的iNQA表项和内核的iNQA表项完全相同）
参数解释	无
日志等级	5 (Notification)
举例	INQA/5/INQA_SMOOTH_END_FAIL: Setting smoothing ending to kernel failed.
对系统的影响	对系统无影响
日志产生原因	软件内部通信故障
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

57 IP6ADDR

本节介绍 IPv6 地址模块输出的日志信息。

57.1 IP6ADDR_CREATEADDRESS_ERROR

日志内容	Failed to create an address by the prefix. Reason: [STRING] on [STRING] and [STRING] on [STRING] overlap.
日志含义	引用前缀生成接口IPv6地址失败，原因是不同接口的IPv6地址前缀覆盖
参数解释	$1：IPv6地址前缀 $2：接口名称 $3：IPv6地址前缀 $4：接口名称
日志等级	4 (Warning)
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_ERROR: Failed to create an address by the prefix. Reason: 2001::/ 64 on GigabitEthernet1/0/2 and 2001::/64 on GigabitEthernet1/0/1 overlap.
对系统的影响	接口上生成IPv6地址失败，影响业务正常运行
日志产生原因	使用**ipv6 address** *prefix-number*命令配置接口通过引用前缀生成IPv6地址时，可能由于同一台设备的不同接口前缀覆盖，导致IPv6地址生成失败
处理建议	根据日志信息，检查对应接口下的IPv6地址前缀，取消冲突接口上的通过前缀生成IPv6地址的配置，重新配置其他前缀的IPv6地址

57.2 IP6ADDR_CREATEADDRESS_INVALID

日志内容	Can't configure the unspecified address or loopback address on [STRING] by using a prefix with all zeros.
日志含义	引用全零的IPv6地址前缀生成接口IPv6地址时不能配置未指定地址或者环回地址
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_INVALID: Can't configure the unspecified address or loopback address on GigabitEthernet1/0/1 by using a prefix with all zeros.
对系统的影响	接口上生成IPv6地址失败，影响业务正常运行
日志产生原因	使用**ipv6 prefix**命令配置了全零的IPv6地址前缀，并通过**ipv6 address** *prefix-number*命令引用全零的IPv6地址前缀时为接口配置了未指定地址或者环回地址
处理建议	根据日志信息，取消该接口下的无效配置，重新为该接口配置新的IPv6地址

57.3 IP6ADDR_FUNCTION_FAIL

日志内容	Failed to enable IPv6 on interface [STRING]. Reason: [STRING].
日志含义	使能IPv6功能失败
参数解释	$1：接口名称 $2：使能IPv6功能失败的原因，取值包括： • Insufficient resources：资源不足 • IPv6 is not supported：由于设备不支持 IPv6，接口上不支持配置 IPv6 地址 • Unknown error：未知错误
日志等级	6 (Informational)
举例	IP6ADDR/6/IP6ADDR_FUNCTION_FAIL: Failed to enable IPv6 on interface GigabitEthernet1/0/1. Reason: Insufficient resources.
对系统的影响	影响IPv6业务正常运行
日志产生原因	产生此日志的可能原因包括： • 系统资源不足 • 设备不支持 IPv6 功能，接口上不支持配置 IPv6 地址 • 未知错误
处理建议	1. 如果失败原因是资源不足，则根据网络规划和业务部署，检查设备上是否存在非必需使能 IPv6 功能的接口 o 如果存在非必需使能IPv6 功能的接口，执行 **undo ipv6 address**命令删除该接口的所有IPv6 地址，然后再重新配置产生日志的接口上的IPv6 地址 o 如果不存在非必需使能 IPv6 功能的接口，请收集配置文件、日志信息、告警信息，并联系技术支持人员 2. 如果失败原因是设备不支持 IPv6，则无需处理 3. 如果失败原因是未知错误，请收集配置文件、日志信息、告警信息，并联系技术支持人员

58 IP6FW

本节包含 IP6FW（IPv6 Forwarding）日志信息。

58.1 IPv6_MTU_SET_DRV_NOT_SUPPORT

日志内容	The operation is not supported to set driver IPv6 interface MTU: interface is [STRING], MTU is [UINT32].
日志含义	接口MTU值不支持下驱动
参数解释	$1：接口名称 $2：IP MTU值
日志等级	5 (Notification)
举例	IP6FW/5/IPv6_MTU_SET_DRV_NOT_SUPPORT: The operation is not supported to set driver IPv6 interface MTU: interface is GigabitEthernet1/0/1, MTU is 1400.
对系统的影响	不支持下驱动的MTU值不生效
日志产生原因	硬件转发设备不支持配置接口上发送IPv6报文的MTU，对于软件转发设备可能是驱动侧问题
处理建议	1. 对于硬件转发的设备，无需处理 2. 对于软件转发的设备，请收集设备的配置文件、日志信息和告警信息，并联系技术支持人员

59 IPADDR

本节介绍 IP 地址模块输出的日志信息。

59.1 IPADDR_HA_EVENT_ERROR

日志内容	A process failed HA upgrade because [STRING].
日志含义	进程HA升级失败

参数解释	$1：进程HA升级失败原因： • IPADDR failed the smooth upgrade：板间平滑失败 • IPADDR failed to reupgrade to the master process：重新升级为主失败 • IPADDR stopped to restart the timer：重启定时器停止 • IPADDR failed to upgrade to the master process：升级为主进程失败 • IPADDR failed to restart the upgrade：重新尝试升级失败 • IPADDR failed to add the unicast object to the master task epoll：将 sync 单播对象挂主任务 epoll 失败 • IPADDR failed to create an unicast object：创建单播失败 • IPADDR role switchover failed when the standby process switched to the master process：备升主时角色转换失败 • IPADDR switchover failed when the master process switched to the standby process：主变备时降级失败 • IPADDR HA upgrade failed：HA 升级失败 • IPADDR failed to set the interface filtering criteria：设置接口选择句柄失败 • IPADDR failed to register interface events：注册接口事件失败 • IPADDR failed to subscribe port events：订阅端口事件失败 • IPADDR failed to add a VPN port event to the master epoll：添加 VPN 的端口事件到主 Epoll 失败 • IRDP failed to open DBM：打开 DBM 数据库失败 • IRDP failed to initiate a connection to the device management module：向设备管理建立连接失败 • IRDP failed to add the master task epoll with the handle used to connect to the device management module ：与设备管理建立连接的句柄加 Epoll 失败 • IRDP failed to register device management events：注册设备管理事件失败 • IRDP failed to subscribe port events：订阅协议使能端口事件失败 • IRDP failed to add the master task epoll with the handle used to subscribe port events：订阅协议使能端口事件的句柄加 Epoll 失败 • IRDP failed to set the interface filtering criteria：设置接口选择句柄失败 • IRDP failed to register interface events：注册接口事件失败 • IRDP failed to register network events：注册网络事件失败 • IRDP failed to create the interface control block storage handle：创建接口控制块存储句柄失败 • IRDP failed to create the timer：创建定时器失败 • IRDP failed to add the master task epoll with the handle used to create the timer：创建定时器的句柄加 Epoll 失败 • IRDP failed to set the schedule time for the timer：设置定时器调度时间失败 • IRDP failed to set the timer to unblocked status：设置定制器为非阻塞失败 • IRDP failed to create a timer instance：创建定时器实例失败

日志等级	4 (Warning)
举例	IPADDR/4/IPADDR_HA_EVENT_ERROR: A process failed HA upgrade because IPADDR failed the smooth upgrade.
对系统的影响	IP地址模块未响应HA事件，主备倒换业务不生效
日志产生原因	进程HA升级失败，原因是板间平滑失败，重新升级为主失败等
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

59.2 IPADDR_HA_STOP_EVENT

日志内容	The device received an HA stop event.
日志含义	设备收到HA STOP事件
参数解释	无
日志等级	4 (Warning)
举例	IPADDR/4/IPADDR_HA_STOP_EVENT: The device received an HA stop event.
对系统的影响	设备从主设备降为备设备
日志产生原因	设备收到HA STOP事件
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

60 IPCC

本节介绍 IPCC 模块输出的日志信息。

60.1 IPCC_LICENSE_ACTIVE

日志内容	The IPCC license has been activated and the IPCC feature is available.
日志含义	IPCC License已激活，IPCC功能可以正常使用
参数解释	无
日志等级	5 (Notification)
举例	IPCC/5/IPCC_LICENSE_ACTIVE: The IPCC license has been activated and the IPCC feature is available.
对系统的影响	对系统无影响
日志产生原因	IPCC License已经激活
处理建议	无需处理

60.2 IPCC_LICENSE_EXPIRE

日志内容	The IPCC license will expire in [UINT32] days.
日志含义	IPCC License将在指定天数后失效
参数解释	$1：天数，取值范围为1到30天
日志等级	5 (Notification)
举例	IPCC/5/IPCC_LICENSE_EXPIRE: The IPCC license will expire in 5 days.
对系统的影响	对系统无影响
日志产生原因	IPCC License将在指定天数后失效
处理建议	请在License失效前，安装新的IPCC License

60.3 IPCC_NO_LICENSE

日志内容	The IPCC feature is not available, because the IPCC license has expired or has been uninstalled.
日志含义	IPCC License已过期或者已被卸载导致IPCC功能无法使用
参数解释	无
日志等级	4 (Warning)
举例	IPCC/4/IPCC_NO_LICENSE: The IPCC feature is not available, because the IPCC license has expired or has been uninstalled.
对系统的影响	IPCC功能无法正常使用
日志产生原因	IPCC License已过期或者已被卸载
处理建议	请重新安装IPCC License

61 IPFW

本节包含 IPFW（IP Forwarding）日志信息。

61.1 IPFW_ECMPTHRES_DRV_NOT_SUPPORT

日志内容	Setting ECMP FIR thresholds is not supported.
日志含义	设备不支持配置等价路由FIR模式中主用链路带宽使用率的上限和下限
参数解释	无
日志等级	5 (Notification)
举例	IPFW/5/IPFW_ECMPTHRES_DRV_NOT_SUPPORT: Setting ECMP FIR thresholds is not supported.
对系统的影响	无
日志产生原因	在不支持本功能的设备上进行配置
处理建议	**1.** 请确保设备支持配置等价路由 FIR 模式中主用链路带宽使用率的上限和下限 **2.** 请收集告警信息、日志信息和配置信息，并联系技术支持工程师

61.2 IPFW_FAILURE

日志内容	The card doesn't support the split horizon forwarding configuration.
日志含义	单板不支持配置转发水平分割
参数解释	无
日志等级	5 (Notification)
举例	IPFW/5/IPFW_FAILURE: -MDC=1; The card doesn't support the split horizon forwarding configuration.
对系统的影响	无
日志产生原因	在不支持本功能的设备上进行配置
处理建议	**1.** 请确保所属单板支持转发水平分割配置 **2.** 请收集告警信息、日志信息和配置信息，并联系技术支持工程师

日志内容	Failed to configure split horizon forwarding on the card.
日志含义	单板配置转发水平分割失败
参数解释	无
日志等级	5 (Notification)
举例	IPFW/5/IPFW_FAILURE: -MDC=1; Failed to configure split horizon forwarding on the card.
对系统的影响	转发水平分割功能不可用
日志产生原因	单板配置转发水平分割失败时打印该日志
处理建议	请收集告警信息、日志信息和配置信息，并联系技术支持工程师

61.3 IPFW_SETTING_FAILED_PACKETDROP

日志内容	Failed to enable packet-drop statistics. Error code: [STRING].
日志含义	开启接口丢包统计功能失败
参数解释	$1：错误码编号 0x40010001：驱动下发错误 0x40010008：驱动不支持 0x4001000b：驱动资源不足 0x20010002：驱动参数错误
日志等级	6 (Informational)
举例	IPFW/6/IPFW_SETTING_FAILED_PACKETDROP: Failed to enable packet-drop statistics. Error code: 0x40010001
对系统的影响	接口丢包统计功能不可用
日志产生原因	硬件不支持或资源不足
处理建议	1. 请确保设备支持配置接口丢包统计功能 2. 请收集告警信息、日志信息和配置信息，并联系技术支持工程师

61.4 IPv4_MTU_SET_DRV_NOT_SUPPORT

日志内容	The operation is not supported to set driver IPv4 interface MTU: interface is [STRING], MTU is [UINT32].
日志含义	接口MTU值不支持下驱动
参数解释	$1：接口名称 $2：IP MTU值
日志等级	5 (Notification)
举例	IPFW/5/IPv4_MTU_SET_DRV_NOT_SUPPORT: The operation is not supported to set driver IPv4 interface MTU: interface is GigabitEthernet1/0/1, MTU is 1400.
对系统的影响	不支持下驱动的MTU值不生效
日志产生原因	硬件转发设备不支持配置接口上发送IPv4报文的MTU，对于软件转发设备可能是驱动侧问题
处理建议	1. 对于硬件转发的设备，无需处理，设备不支持配置接口上发送 IPv4 报文的 MTU 2. 对于软件转发的设备，请收集设备的配置文件、日志信息和告警信息，并联系技术支持人员

62 IPSEC

本节介绍 IPsec 模块输出的日志信息。

62.1 IPSEC_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
日志含义	IPsec添加流表失败
参数解释	$1：失败原因
日志等级	4 (Warning)
举例	IPSEC/4/IPSEC_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
对系统的影响	当前和后续的IPsec SA无法正常建立
日志产生原因	硬件资源不足导致IPsec添加流表失败
处理建议	对于硬件资源不足情况，请收集配置文件、日志信息和告警信息，并联系技术支持

62.2 IPSEC_ANTI-REPLAY_WINDOWS_ERROR

日志内容	Anti-replay dropped a packet: src=[STRING]; time-sent=[STRING], [UINT32] [STRING] [UINT32] [UINT32]:[UINT32]:[UINT32] [UINT32]us; time-received=[STRING], [UINT32] [STRING] [UINT32] [UINT32]:[UINT32]:[UINT32] [UINT32]us; time-diff=[UINT32]us; window-size=+-[FLOAT]ms.
日志含义	抗重放丢弃报文
参数解释	$1：被丢弃报文的源IP地址 $2：发送报文的星期 $3：发送报文的日期 $4：发送报文的月份 $5：发送报文的年份 $6：发送报文的小时 $7：发送报文的分钟 $8：发送报文的秒数 $9：发送报文的微妙数 $10：接收报文的星期 $11：接收报文的日期 $12：接收报文的月份 $13：接收报文的年份 $14：接收报文的小时 $15：接收报文的分钟 $16：接收报文的秒数 $17：接收报文的微妙数 $18：发送接收之间的时间差，微秒数 $19：时间窗口的一半，毫秒数
日志等级	6 (Informational)
举例	IPSEC/6/IPSEC_ANTI-REPLAY_WINDOWS_ERROR: Anti-replay dropped a packet: src=192.168.58.178;time-sent=Sat, 23 Apr 2016 11:17:29 594565us; time-received =Sat, 23 Apr 2016 11:17:26 707866us; time-diff=2886699us; window-size =+-2500ms.
对系统的影响	对系统无影响
日志产生原因	报文被丢弃。触发该日志的原因可能有如下几种： • 报文发送和接收之间的时间差超出窗口大小 • 接收端抗重放使能而收到的报文没有抗重放头 • 隧道模式下，抗重放未使能但是收到带有抗重放头的报文
处理建议	• 请根据日志信息显示的原因进行排查 • 请收集配置文件、日志信息和告警信息，并联系技术支持

62.3 IPSEC_SA_ESTABLISH

日志内容	IPsec SA was established. SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
日志含义	IPsec SA创建成功
参数解释	$1：建立IPsec SA的角色，发起者或者响应者 $2：本端IP地址 $3：远端IP地址 $4-$9：数据流 $10: 内部VPN实例 $11: 外部VPN实例 $12: 入方向AH SPI $13: 出方向AH SPI $14: 入方向ESP SPI $15: 出方向ESP SPI $16: ACL编号，默认值为4294967295 $17: ACL名称，ACL编号与ACL名称只会显示其中一种
日志等级	6 (Informational)
举例	IPSEC/6/IPSEC_SA_ESTABLISH: IPsec SA was established. SA information: Role: Responder Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586

	ACL number: 3101
对系统的影响	对系统无影响
日志产生原因	IPsec SA创建成功
处理建议	系统正常运行时产生的信息，无需处理

62.4 IPSEC_SA_ESTABLISH_FAIL

日志内容	Failed to establish IPsec SA. Reason: [STRING]. SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
日志含义	IPsec SA创建失败
参数解释	$1：IPsec SA创建失败的原因： • 获取 SP 时 SP 配置不完整，显示为：Get SP: Required configuration is missing in the SP. SP ID=%u. • 获取 SP 时本地地址不匹配，显示为：Get SP: The SP's local address doesn't match the local address configured in the IKE profile. SP ID=%u, SP's local address=%s, p2policy's local address=%s. • 获取 SP 时远端地址不存在，显示为：Get SP: The remote address doesn't exist. SP ID=%u, hostname=%s. • 远端地址不匹配，显示为：Get SP: The SP's remote address doesn't match the remote address configured in the IKE profile. SP ID=%u, SP's remote address=%s, p2policy's remote address=%s. • ACL 或 profile 配置错误，显示为：The policy contains incorrect ACL or IKE profile configuration. • 获取 SP 时在 SP 中未找到 IPsec 安全提议，显示为：Get SP: The SP doesn't have an IPsec transform set. • 创建临时 SA 失败，显示为：Get SP: Failed to create larval SA. • 填充 SA 数据失败，显示为：Create SA: Failed to fill the SA. • 添加 IKE SA 失败，显示为：Create SA: Failed to create SA. • 添加 IKE SA 时未找到 SP，显示为：Create SA: Can't find SP. • Tunnel 已存在，显示为：Failed to create tunnel because a tunnel with the same index and sequence number already exists. Tunnel index=%d, tunnel seq=%d. • 切换 SA 未找到入方向 SA，显示为：Failed to switch SA because the inbound SA can't be found. SPI=%u. • 切换 SA 时 SA 状态错误，显示为：Failed to switch SA because the SA state is incorrect. • 切换 SA，未找到出方向 SA，显示为：Failed to switch SA because the outbound SA can't be found. • 切换 SA 时未找到使用另一种安全协议的 SA，显示为：Failed to switch SA because

	the outbound SA using another security protocol can't be found. • 内核态切换 SA 失败，显示为：Failed to switch SA in kernel. • 通知内核链路层变化失败，显示为：Failed to notify kernel of the link state change. • Tunnel 数达到能力上限，显示为：Number of IPsec tunnels reached the crypto capacity of the device. • Tunnel 个数达到上限，显示为：Maximum number of IPsec tunnels already reached. • 添加 Tunnel 失败，显示为：Failed to add IPsec tunnel. • 获取 SP 时 IPsec 正在平滑，显示为：Getting SP: IPsec is smoothing. • 获取 SP 时 IPsec 进程未运行，显示为：Getting SP: IPsec is not running. • 获取 SP 时，通过 index 和 SeqNum 查找 SP 失败，显示为：Getting SP: Failed to find SP by index and sequence number. • 获取 SP 时生成 SA 超时，显示为：Getting SP: Creating SA timed out. • 获取 SP 时，通过普通接口获取 SP 时，目标板不在线，显示为：Getting SP by interface: Target node not online. • 获取 SP 时，按照 mGRE 方式获取 SP，获取接口失败，显示为：Getting SP by mGRE: Failed to get interface. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，无效的接口类型，显示为：Getting SP: Failed to get SP by mGRE because interface type was invalid. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，缺少相关配置，显示为：Getting SP: Failed to get SP by mGRE because of no tunnel protection configuration. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，未找到 profile，显示为：Getting SP: Failed to get SP by mGRE because profile %s was not found. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，profile 类型错误，显示为：Getting SP: Failed to get SP by mGRE because of wrong profile type. • 获取 SP 时，按照 mGRE 方式获取 SP，通过 profile 查找 SP 失败，显示为：Getting SP by mGRE: Failed to find profile SP by profile %s. • 尝试按照 mGRE 方式获取 SP 失败，显示为：Getting SP: Failed to get SP by mgre. • 尝试按照 SVTI 方式获取 SP 失败，无效的接口类型，显示为：Getting SP: Failed to get SP by SVTI because of invalid interface type. • 尝试按照 SVTI 方式获取 SP 失败，缺少相关配置，显示为：Getting SP: Failed to get SP by SVTI because of no tunnel protection configuration with interface %s. • 尝试按照 SVTI 方式获取 SP 失败，未找到 profile，显示为：Getting SP: Failed to get SP by SVTI because profile %s was not found. • 获取 SP 时，尝试按照 SVTI 方式获取 SP 失败，profile 类型错误，显示为：Getting SP: Failed to get SP by SVTI because of wrong type of profile %s. • 按照 SVTI 方式获取 SP 时，通过 profile 查找 SP 失败，显示为：Getting SP by SVTI: Failed to find profile SP by profile %s. • 尝试按照 SVTI 方式获取 SP 失败，SP 不是 IKE 方式的，显示为：Getting SP: Failed to get SP by SVTI because SP type was not ISAKMP with profile %s. • 尝试按照 SVTI 方式获取 SP 失败，重协商 SP 的 index 或 sequence num 有变化，显示为：Getting SP: Failed to match flow because renegotiation SP's index or Seqnum changed. • 获取 SP 时，匹配 SVTI 流失败，IKE profile 不匹配，显示为：Getting SP: Failed to match SVTI flow because IKE profile was not match. • 匹配 SVTI 流失败，匹配 ACL 失败，显示为：Getting SP: Failed to match SVTI flow because flow was not match with ACL. • 尝试按照 SVTI 方式获取 SP 时，创建 larval SA 失败，显示为：Getting SP by SVTI:

	Failed to create larval SA. • 尝试按照 mGRE 方式获取 SP 失败，显示为：Getting SP: Failed to get SP by SVTI with interface %s. • 通过三层口获取 SP 时，获取接口数据失败，显示为：Getting SP by L3 interface: Failed to get interface data. • 尝试通过三层口获取 SP 失败，根据 SP ENTRY KEY 找不到 SP ENTRY，显示为：Getting SP: Failed to get SP by L3 interface because no SP entry was found by key. • 获取 SP 时，尝试通过共享源接口获取 SP 失败，根据共享源接口的 SP ENTRY KEY 找不到 SP ENTRY，显示为：Getting SP: Failed to get SP by L3 interface because no source interface SP entry was found by key. • 获取 SP 时通过三层口获取 SP 时，匹配 SP 失败，SP 不是 Isakmp 方式的，显示为：Getting SP by L3 interface: Failed to match SP because SP's mode not ISAKMP. • 获取 SP 时通过三层口获取 SP 时，匹配 SP 失败，SP 协商是不完整的，显示为：Getting SP by L3 interface: Failed to match SP because SP negotiation not complete. • 获取 SP 时，IKE 模板方式且未配置 acl，任意流不触发协商，显示为：Getting SP: Rejected peer's request of any flow when SP's mode was isakmp template and no ACL was specified. • 获取 SP 时通过三层口获取 SP 时，匹配 SP 失败，通过 SP 找不到 policy，显示为：Getting SP by L3 interface: Failed to match SP because policy cannot be found by SP. • 获取 SP 时通过三层口获取 SP 时，匹配 SP 失败，ike profile 与 ipsec profile 不匹配，显示为：Getting SP by L3 interface: Failed to match SP because IKE profile was %s while IPsec used profile %s. • 获取 SP 时，匹配流失败，因为 ACL 不匹配，显示为：Getting SP: Failed to match flow because ACL not match. • 获取 SP 时，匹配流失败，重协商 SP 的 index 或 sequence num 有变化，显示为：Getting SP: Failed to match flow because renegotiation SP's index or Seqnum changed. • 获取 SP 时，匹配 SP 失败，掩码校验失败，显示为：Getting SP: Flow netmask check failed. • 获取 SP 时，匹配 SP 失败，流重叠检测失败，显示为：Getting SP: Flow overlap check failed. $2：建立IPsec SA的角色，发起者或者响应者 $3：本端IP地址 $4：远端IP地址 $5-$10: 数据流 $11: 内部VPN实例 $12: 外部VPN实例 $13: 入方向AH SPI $14: 出方向AH SPI $15: 入方向ESP SPI $16: 出方向ESP SPI $17: ACL编号，默认值为4294967295 $18: ACL名称，ACL编号与ACL名称只会显示其中一种

日志等级	6 (Informational)
举例	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA Reason: Failed to add IPsec tunnel. SA information: Role: Responder Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101 ACL name: aaa
对系统的影响	IPsec SA创建失败，无法建立IPsec隧道保护需要保护的报文
日志产生原因	• 两端的 IPsec 安全提议参数、IPsec 认证算法、IPsec 加密算法、IPsec 封装模式不一致 • 两端的 IPsec policy 配置不一致 • 两端引用的 ACL 配置不为镜像配置 • 物理链路状态不佳或对等体网络不可达
处理建议	• 检查两端的 IPsec 安全提议参数、IPsec 认证算法、IPsec 加密算法、IPsec 封装模式是否一致，若不一致请修改为一致 • 检查两端的 IPsec policy 配置是否一致，若不一致请修改为一致 • 检查两端引用的 ACL 配置是否为镜像配置，若不为镜像配置请修改为镜像配置 • 检查物理链路状态和对等体网络是否可达，若物理链路状态不佳或对等体网络不可达请排查网络故障 执行以上检查后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

62.5 IPSEC_SA_INITIATION

日志内容	Began to establish IPsec SA. Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] ACL number: [UINT32] ACL name: [STRING]
日志含义	开始创建IPsec SA
参数解释	$1：本端IP地址 $2：远端IP地址 $3-$8：数据流 $9：内部VPN实例 $10: 外部VPN实例 $11: ACL编号，默认值为4294967295 $12: ACL名称，ACL编号与ACL名称只会显示其中一种
日志等级	6 (Informational)
举例	IPSEC/6/IPSEC_SA_INITIATION: Began to establish IPsec SA. Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb ACL number: 3101 ACL name: aaa
对系统的影响	对系统无影响
日志产生原因	开始创建IPsec SA
处理建议	系统正常运行时产生的信息，无需处理

62.6 IPSEC_SA_TERMINATE

日志内容	The IPsec SA was deleted. Reason: [STRING] SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
日志含义	IPsec SA被删除
参数解释	$1：IPsec SA被删除的原因，如： • SA 空闲超时，显示为：SA idle timeout • 执行了reset命令，显示为：The **reset** command was executed • 内部事件导致 SA 删除，显示为：Internal event • 配置变化导致 SA 删除，显示为：Configuration change • 收到 IKE 的删除消息，显示为：An IKE SA deletion message was received $2：建立IPsec SA的角色，发起者或者响应者 $3：本端IP地址 $4：远端IP地址 $5-$10: 数据流 $11: 内部VPN实例 $12: 外部VPN实例 $13: 入方向AH SPI $14: 出方向AH SPI $15: 入方向ESP SPI $16: 出方向ESP SPI $17: ACL编号，默认值为4294967295 $18: ACL名称，ACL编号与ACL名称只会显示其中一种
日志等级	6 (Informational)
举例	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted. Reason: SA idle timeout. SA information: Role: initiator Local address: 2.2.2.2

	Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101 ACL name: aaa
对系统的影响	IPsec SA被删除，该SA承载的IPsec业务中断
日志产生原因	IPsec SA被删除。触发该日志的原因可能有：SA空闲超时或者执行了reset命令
处理建议	• 由于本日志所列原因导致的 SA 被删除后，SA 会重新协商建立，属于正常情况，无需处理 • 如果是其他原因导致 SA 被删除，请收集配置文件、日志信息和告警信息，并联系技术支持人员

63 IPSG

本节介绍 IPSG（IP Source Guard）模块输出的日志信息。

63.1 IPSG_ADDENTRY_ERROR

日志内容	Failed to add an IP source guard binding on interface [STRING]: IP=[STRING], MAC=[STRING], VLAN=[UINT16]. Reason: [STRING].
日志含义	IP Source Guard绑定表项下发失败
参数解释	$1：接口名称（如果没有指定，则显示为N/A） $2：IPv4地址或IPv6地址（如果没有指定，则显示N/A） $3：MAC地址（如果没有指定，则显示为N/A） $4：VLAN ID（如果没有指定，则显示为无意义值65535） $5：失败原因： • Feature not supported：特性不支持 • Resources not sufficient：资源不足 • Maximum number of IPv4 binding entries already reached： IPv4 绑定表项达到最大规格 • Maximum number of IPv6 binding entries already reached：IPv6 绑定表项达到最大规格 • Unknown error：未知错误
日志等级	6 (Informational)
举例	IPSG/6/IPSG_ADDENTRY_ERROR: Failed to add an IP source guard binding on interface Vlan-interface1: IP=1.1.1.1, MAC=0001-0001-0001, VLAN=1. Reason: Resources not sufficient.
对系统的影响	系统无法利用该表项过滤报文
日志产生原因	参见本日志打印的失败原因
处理建议	• 不支持 IP Source Guard 特性时，添加表项会失败。属于正常运行信息，无需处理 • 当提示硬件资源不足时，关闭部分非必要业务释放硬件资源后再重新添加表项 • 当提示 IPv4 或 IPv6 绑定表项达到最大规格，即用于 IPSG 绑定表项的 ACL 资源不足时，请根据需要删除部分表项释放 ACL 资源 • 如果问题无法定位解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.2 IPSG_ADDEXCLUDEDVLAN_ERROR

日志内容	Failed to add excluded VLANs (VLAN [UINT16] to VLAN [UINT16]). Reason: [STRING].
日志含义	下发免过滤VLAN失败
参数解释	$1：Start VLAN（免过滤VLAN的起始VLAN ID） $2：End VLAN（免过滤VLAN的结束VLAN ID） $3：失败原因： • Feature not supported：特性不支持 • Resources not sufficient：资源不足 • Unknown error：未知错误
日志等级	6 (Informational)
举例	IPSG/6/IPSG_ADDEXCLUDEDVLAN_ERROR: -MDC=1-Slot=4; Failed to add excluded VLANs (VLAN 1 to eVLAN 5). Reason: Resources not sufficient.
对系统的影响	系统不会放行匹配上该免过滤VLAN的报文
日志产生原因	参见本日志打印的失败原因
处理建议	• 不支持 IP Source Guard 特性时，下发免过滤 VLAN 会失败。属于正常运行信息，无需处理 • 因硬件资源不足而引起的免过滤 VLAN 下发失败时，可关闭部分非必要业务释放硬件资源后，再重新执行命令下发免过滤 VLAN • 如果问题无法定位解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.3 IPSG_ARP_LOCALMAC_CONFLICT

日志内容	MAC conflict exists between an ARP entry and a local entry: IP=[STRING], VPN=[STRING], ARPMAC=[STRING], LocalMAC=[STRING].
日志含义	ARP表项和本地绑定表项的MAC地址冲突
参数解释	$1：IP地址 $2：VPN实例的名称 $3：ARP表项MAC地址 $4：本地绑定表项MAC地址
日志等级	5 (Notification)
举例	IPSG/5/IPSG_ARP_LOCALMAC_CONFLICT: MAC conflict exists between an ARP entry and a local entry: IP=1.1.1.1, VPN=1, ARPMAC=0008-0008-0008, LocalMAC=0008-0008-0009.
对系统的影响	影响正常业务运行
日志产生原因	当存在恶意的ARP攻击时，如果ARP表项和本地绑定表项的IP地址相同，但两者的MAC地址不同，则系统输出该日志
处理建议	• 请根据本日志打印的信息定位 ARP 表项的来源设备，若存在攻击行为则进行处理 • 如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.4 IPSG_ARP_REMOTEMAC_CONFLICT

日志内容	MAC conflict exists between an ARP entry and a remote entry: IP=[STRING], VPN=[STRING], ARPMAC=[STRING], RemoteMAC=[STRING].
日志含义	ARP表项和远端绑定表项的MAC地址冲突
参数解释	$1：IP地址 $2：VPN实例的名称 $3：ARP表项MAC地址 $4：远端绑定表项MAC地址
日志等级	5 (Notification)
举例	IPSG/5/IPSG_ARP_REMOTEMAC_CONFLICT: MAC conflict exists between an ARP entry and a remote entry: IP=1.1.1.1, VPN=1, ARPMAC=0008-0008-0008, RemoteMAC=0008-0008-0009.
对系统的影响	若打印本日志的原因为存在恶意ARP攻击，则将影响正常业务运行；若打印本日志的原因为漫游用户本地上线，则对系统无影响
日志产生原因	• 存在恶意的 ARP 攻击，设备学习到非法用户的 ARP 表项与远端绑定表项的 IP 地址相同，但两者的 MAC 地址不同 • 远端用户漫游到本地上线，使得设备学习到该漫游用户的 ARP 表项与远端绑定表项的 IP 地址相同，但两者的 MAC 地址不同
处理建议	• 当存在恶意 ARP 攻击时，请根据本日志打印的信息定位 ND 表项的来源设备并进行处理。如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理 • 对于漫游用户本地上线，无需处理

63.5 IPSG_DELENTRY_ERROR

日志内容	Failed to delete an IP source guard binding on interface [STRING]: IP=[STRING], MAC=[STRING], VLAN=[UINT16]. Reason: [STRING].
日志含义	删除IP Source Guard绑定表项失败
参数解释	$1：接口名（如果没有指定，则显示为N/A） $2：IP地址（如果没有指定，则显示N/A） $3：MAC地址（如果没有指定，则显示为N/A） $4：VLAN ID（如果没有指定，则显示为无意义值65535） $5：失败原因： • Feature not supported： 特性不支持 • Unknown error：未知错误
日志等级	6 (Informational)
举例	IPSG/6/IPSG_DELENTRY_ERROR: Failed to delete an IP source guard binding on interface Vlan-interface1: IP=1.1.1.1, MAC=0001-0001-0001, VLAN=1. Reason: Unknown error.
对系统的影响	系统仍可以利用该表项过滤报文
日志产生原因	参见本日志打印的失败原因
处理建议	• 不支持 IP Source Guard 特性时，删除表项会失败。属于正常运行信息，无需处理 • 如果问题无法定位解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.6 IPSG_DELEXCLUDEDVLAN_ERROR

日志内容	Failed to delete excluded VLANs (VLAN [UINT16] to VLAN [UINT16]). Reason: [STRING].
日志含义	删除免过滤VLAN失败
参数解释	$1：Start VLAN（免过滤VLAN的起始VLAN ID） $2：End VLAN（免过滤VLAN的结束VLAN ID） $3：失败原因： • Feature not supported：特性不支持 • Resources not sufficient：资源不足 • Unknown error：未知错误
日志等级	6 (Informational)
举例	IPSG/6/IPSG_DELEXCLUDEDVLAN_ERROR: -MDC=1-Slot=4; Failed to delete excluded VLANs (VLAN 1 to VLAN 5). Reason: Resources not sufficient.
对系统的影响	系统仍会放行匹配上该免过滤VLAN的报文
日志产生原因	参见本日志打印的失败原因
处理建议	• 不支持 IP Source Guard 特性时，删除免过滤 VLAN 会失败。属于正常运行信息，无需处理 • 因硬件资源不足而引起的免过滤 VLAN 删除失败时，可关闭部分非必要业务释放硬件资源后，再重新执行命令删除免过滤 VLAN • 如果问题无法定位解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.7 IPSG_IPV4_ALARMCLEAR

日志内容	The packet dropping rate on [STRING] dropped below [UINT32] pps.
日志含义	接口上每秒丢弃报文数恢复到告警阈值以下
参数解释	$1：接口名称 $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV4_ALARMCLEAR: The packet dropping rate on GigabitEthernet1/0/1 dropped below 100 pps.
对系统的影响	对系统无影响
日志产生原因	在接口上配置IPv4接口绑定告警功能后，当该接口上每秒丢弃报文数恢复到告警阈值以下时，系统输出此日志
处理建议	无需处理

63.8 IPSG_IPV4_ALARMEMERGE

日志内容	The packet dropping rate on [STRING] reached or exceeded [UINT32] pps.
日志含义	接口上每秒丢弃报文数大于或等于告警阈值
参数解释	$1：接口名称 $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV4_ALARMEMERGE: The packet dropping rate on GigabitEthernet1/0/1 reached or exceeded 100 pps.
对系统的影响	当系统生成此告警时，设备可能受到了非法报文的攻击。如果攻击流量过大，则将占用过多系统资源，可能导致合法用户业务中断
日志产生原因	在接口上配置IPv4接口绑定告警功能后，当该接口上每秒丢弃报文数大于等于告警阈值时，系统输出此日志
处理建议	1. 请在任意视图下执行 **display ip source binding**命令查看IP Source Guard绑定表项，并通过端口镜像抓取该接口上收到的报文： ○ 如果接口上收到大量与绑定表项不匹配的报文，则认为接口受到攻击，请根据需要排查攻击源头 ○ 如果接口上未收到大量与绑定表项不匹配的报文，则认为接口未受到攻击。请根据需要通过 **ip verify source alarm**命令调整告警阈值，也可通过配置静态IP Source Guard表项放行合法用户报文 2. 如果以上步骤未解决问题，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.9 IPSG_IPV4_VLAN_ALARMCLEAR

日志内容	The packet dropping rate in VLAN [UINT16] dropped below [UINT32] pps.
日志含义	VLAN内每秒丢弃报文数恢复到告警阈值以下
参数解释	$1：VLAN ID $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV4_VLAN_ALARMCLEAR: The packet dropping rate in VLAN 10 dropped below 100 pps.
对系统的影响	对系统无影响
日志产生原因	在VLAN视图下配置IPv4接口绑定告警功能后，当该VLAN内每秒丢弃报文数恢复到告警阈值以下时，系统输出此日志
处理建议	无需处理

63.10 IPSG_IPV4_VLAN_ALARMEMERGE

日志内容	The packet dropping rate in VLAN [UINT16] reached or exceeded [UINT32] pps.
日志含义	VLAN内每秒丢弃报文数大于或等于告警阈值
参数解释	$1：VLAN ID $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV4_VLAN_ALARMEMERGE: The packet dropping rate in VLAN 10 reached or exceeded 100 pps.
对系统的影响	当系统生成此告警时，设备可能受到了非法报文的攻击。如果攻击流量过大，则将占用过多系统资源，可能导致合法用户业务中断
日志产生原因	在VLAN视图下配置IPv4接口绑定告警功能后，当该VLAN内每秒丢弃报文数大于等于告警阈值时，系统输出此日志
处理建议	1. 请在任意视图下执行 **display ip source binding**命令查看IP Source Guard绑定表项，并通过端口镜像抓取该VLAN下收到的报文： ○ 如果 VLAN 下收到大量与绑定表项不匹配的报文，则认为接口受到攻击，请根据需要排查攻击源头 ○ 如果VLAN下未收到大量与绑定表项不匹配的报文，则认为接口未受到攻击。请根据需要通过 **ip verify source alarm**命令调整告警阈值，也可通过配置静态IP Source Guard表项放行合法用户报文 2. 如果以上步骤未解决问题，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.11 IPSG_IPV6_ALARMCLEAR

日志内容	The packet dropping rate on [STRING] dropped below [UINT32] pps.
日志含义	接口上每秒丢弃报文数恢复到告警阈值以下
参数解释	$1：接口名称 $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV6_ALARMCLEAR: The packet dropping rate on GigabitEthernet1/0/1 dropped below 100 pps.
对系统的影响	对系统无影响
日志产生原因	在接口上配置IPv6接口绑定告警功能后，当该接口上每秒丢弃报文数恢复到告警阈值以下时，系统输出此日志
处理建议	无

63.12 IPSG_IPV6_ALARMEMERGE

日志内容	The packet dropping rate on [STRING] reached or exceeded [UINT32] pps.
日志含义	接口上每秒丢弃报文数大于或等于告警阈值
参数解释	$1：接口名称 $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV6_ALARMEMERGE: The packet dropping rate on GigabitEthernet1/0/1 reached or exceeded 100 pps.
对系统的影响	当系统生成此告警时，设备可能受到了非法报文的攻击。如果攻击流量过大，则将占用过多系统资源，可能导致合法用户业务中断
日志产生原因	在接口上配置IPv6接口绑定告警功能后，当该接口上每秒丢弃报文数大于等于告警阈值时，系统输出此日志
处理建议	1. 请在任意视图下执行 **display ipv6 source binding**命令查看IP Source Guard绑定表项，并通过端口镜像抓取该接口上收到的报文。 o 如果接口上收到大量与绑定表项不匹配的报文，则认为接口受到攻击，请根据需要排查攻击源头 o 如果接口上未收到大量与绑定表项不匹配的报文，则认为接口未受到攻击。请根据需要通过 **ipv6 verify source alarm**命令调整告警阈值，也可通过配置静态IP Source Guard表项放行合法用户报文 2. 如果以上步骤未解决问题，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.13 IPSG_IPV6_VLAN_ALARMCLEAR

日志内容	The packet dropping rate in VLAN [UINT16] dropped below [UINT32] pps.
日志含义	VLAN内每秒丢弃报文数恢复到告警阈值以下
参数解释	$1：VLAN ID $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV6_VLAN_ALARMCLEAR: The packet dropping rate in VLAN 10 dropped below 100 pps.
对系统的影响	对系统无影响
日志产生原因	在VLAN视图下配置IPv6接口绑定告警功能后，当该VLAN内每秒丢弃报文数恢复到告警阈值以下时，系统输出此日志
处理建议	无需处理

63.14 IPSG_IPV6_VLAN_ALARMEMERGE

日志内容	The packet dropping rate in VLAN [UINT16] reached or exceeded [UINT32] pps.
日志含义	VLAN内每秒丢弃报文数大于或等于告警阈值
参数解释	$1：VLAN ID $2：告警阈值
日志等级	4 (Warning)
举例	IPSG/4/IPSG_IPV4_VLAN_ALARMEMERGE: The packet dropping rate in VLAN 10 reached or exceeded 100 pps.
对系统的影响	当系统生成此告警时，设备可能受到了非法报文的攻击。如果攻击流量过大，则将占用过多系统资源，可能导致合法用户业务中断
日志产生原因	在VLAN视图下配置IPv6接口绑定告警功能后，当该VLAN内每秒丢弃报文数大于等于告警阈值以下时，系统输出此日志
处理建议	1. 请在任意视图下执行 **display ipv6 source binding**命令查看IP Source Guard绑定表项，并通过端口镜像抓取该VLAN下收到的报文。 o 如果 VLAN 下收到大量与绑定表项不匹配的报文，则认为接口受到攻击，请根据需要排查攻击源头 o 如果VLAN下未收到大量与绑定表项不匹配的报文，则认为接口未受到攻击。请根据需要通过 **ipv6 verify source alarm**命令调整告警阈值，也可通过配置静态IP Source Guard表项放行合法用户报文 2. 如果以上步骤未解决问题，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.15 IPSG_MAC_CONFLICT

日志内容	MAC conflict exists between a local entry and a remote entry: IP=[STRING], VPN=[STRING], LocalMAC=[STRING], RemoteMAC=[STRING].
日志含义	远端绑定表项和本地绑定表项的MAC地址冲突
参数解释	$1：IP地址 $2：VPN实例的名称 $3：本地绑定表项MAC地址 $4：远端绑定表项MAC地址
日志等级	5 (Notification)
举例	IPSG/5/IPSG_MAC_CONFLICT: MAC conflict exists between a local entry and a remote entry: IP=1.1.1.1, VPN=1, LocalMAC=0008-0008-0008, RemoteMAC=0008-0008-0009.
对系统的影响	对系统无影响
日志产生原因	当本地学习到一个远端绑定表项时，若该绑定表项的IP地址与本地已有某绑定表项的IP地址相同，但两者的MAC地址不同，则系统输出本日志
处理建议	无需处理

63.16 IPSG_ND_LOCALMAC_CONFLICT

日志内容	MAC conflict exists between an ND entry and a local entry: IPv6=[STRING], VPN=[STRING], NDMAC=[STRING], LocalMAC=[STRING].
日志含义	ND表项和本地绑定表项的MAC地址冲突
参数解释	$1：IP地址 $2：VPN实例的名称 $3：ND表项MAC地址 $4：本地绑定表项MAC地址
日志等级	5 (Notification)
举例	IPSG/5/IPSG_ND_LOCALMAC_CONFLICT: MAC conflict exists between an ND entry and a local entry: IPv6=1::1, VPN=1, NDMAC=0008-0008-0008, LocalMAC=0008-0008-0009.
对系统的影响	影响正常业务运行
日志产生原因	当存在恶意的ND攻击时，如果ND表项和本地绑定表项的IP地址相同，但两者的MAC地址不同，则系统输出本日志
处理建议	• 请根据本日志打印的信息定位 ND 表项的来源设备，若存在攻击行为则进行处理 • 如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

63.17 IPSG_ND_REMOTEMAC_CONFLICT

日志内容	MAC conflict exists between an ND entry and a remote entry: IPv6=[STRING], VPN=[STRING], NDMAC=[STRING], RemoteMAC=[STRING].
日志含义	ND表项和远端绑定表项的MAC地址冲突
参数解释	$1：IP地址 $2：VPN实例的名称 $3：ND表项MAC地址 $4：远端绑定表项MAC地址
日志等级	5 (Notification)
举例	IPSG/5/IPSG_ND_REMOTEMAC_CONFLICT: MAC conflict exists between an ND entry and a remote entry: IPv6=1::1, VPN=1, NDMAC=0008-0008-0008, RemoteMAC=0008-0008-0009.
对系统的影响	若打印本日志的原因为存在恶意ND攻击，则将影响正常业务运行；若打印本日志的原因为漫游用户本地上线，则对系统无影响
日志产生原因	• 存在恶意的 ND 攻击，设备学习到非法用户的 ND 表项与远端绑定表项的 IPv6 地址相同，但两者的 MAC 地址不同 • 远端用户漫游到本地上线，使得设备学习到该漫游用户的 ND 表项与远端绑定表项的 IPv6 地址相同，但两者的 MAC 地址不同
处理建议	• 当存在恶意 ARP 攻击时，请根据本日志打印的信息定位 ND 表项的来源设备并进行处理。如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理 • 对于漫游用户本地上线，无需处理

64 IPSGT

本节介绍 IP-SGT 模块输出的日志信息。

64.1 IPSGT_CRITICAL_MAPPINGS_MAXIMUM

日志内容	The number of critical mappings reaches the upper limit.
日志含义	设备可存储的IP-SGT逃生用户映射表项数达到上限
参数解释	无
日志等级	4 (Warning)
举例	IPSGT/4/IPSGT_CRITICAL_MAPPINGS_MAXIMUM: The number of critical mappings reaches the upper limit.
对系统的影响	设备不再存储新的逃生用户生成的IP-SGT映射表项，新逃生用户的流量无法通过硬件转发，只能上送CPU通过软件转发。当上送CPU的流量过多时，会对CPU造成冲击
日志产生原因	当设备存储的IP-SGT逃生用户映射表项数达到IP-SGT逃生映射表项的最大数目（通过**ipsgt max-critical-map**命令配置）时，系统输出此日志
处理建议	执行**display current-configuration | include max-critical-map**命令查看当前设备上配置的可存储的IP-SGT逃生映射表项的最大数目： • 如果该值过小，则请重新配置 • 如果该值符合应用场景，但仍有大量逃生用户上线，则系统可能受到用户报文攻击，请请收集告警信息、日志信息和配置信息，并联系 H3C 技术支持工程师进行处理

65 IRDP

本节介绍 IRDP 模块输出的日志信息。

65.1 IRDP_EXCEED_ADVADDR_LIMIT

日志内容	The number of advertisement addresses on interface [STRING] exceeded the limit 255.
日志含义	接口待通告地址超上限
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	IRDP/6/IRDP_EXCEED_ADVADDR_LIMIT: The number of advertisement addresses on interface Ethernet1/1/0/2 exceeded the limit 255.
对系统的影响	无
日志产生原因	接口上待通告的地址数超过了上限值
处理建议	删除接口上不需要的从IP地址

66 IRF

本节介绍 IRF（Intelligent Resilient Framework，智能弹性架构）模块输出的日志信息。

66.1 IRF_LINK_BLOCK

日志内容	IRF port went blocked.
日志含义	IRF端口状态变为blocked
参数解释	无
日志等级	2 (Critical)
举例	IRF/2/IRF_LINK_BLOCK: IRF port went blocked.
对系统的影响	设备无法和其它设备组成IRF
日志产生原因	新设备加入IRF时，新设备的成员编号和IRF中已有设备的成员编号冲突，新设备上会打印该日志信息 处于该状态的IRF端口不能转发数据报文，只能收发IRF协议报文
处理建议	1. 登录设备执行 **display irf**命令查看设备的成员编号，如果设备的成员编号和IRF中现有设备的成员编号相同，请使用 **irf member renumber**命令将设备的成员编号修改成IRF内的唯一值，再重启设备恢复故障 2. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

66.2 IRF_LINK_DOWN

日志内容	IRF port went down.
日志含义	IRF端口状态变为down
参数解释	无
日志等级	3 (Error)
举例	IRF/3/IRF_LINK_DOWN: IRF port went down.
对系统的影响	会导致设备和IRF系统分裂
日志产生原因	IRF端口绑定的所有物理端口全部Down
处理建议	登录本设备，执行**display irf link**命令，查看设备使用的IRF物理端口。针对这些物理端口可以进行以下处理： **1.** 确认对端设备是否正常运行。执行**display device**命令查看设备状态，如果设备处于非正常工作状态，请先定位设备故障 **2.** 在对端设备执行**display irf link**命令，查看对端IRF端口的配置是否正确。如果配置错误，请在IRF端口视图下，重新绑定IRF物理端口 **3.** 确保物理连线正确。本端IRF端口 1 需要和对端的IRF端口 2 连接，本端IRF端口 2 需要和对端的IRF端口 1 连接。两台设备组成的IRF系统，请使用链型拓扑，不要使用环形拓扑。确保物理连线正确后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **4.** 更换接口。在IRF端口视图下执行**port group interface**命令将IRF端口和其它物理端口绑定，并将IRF连线插入新绑定的物理端口。更换接口后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **5.** 更换网线或光纤。更换网线或光纤后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **6.** 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

66.3 IRF_LINK_UP

日志内容	IRF port came up.
日志含义	IRF端口链路状态变为up
参数解释	无
日志等级	6 (Informational)
举例	IRF/6/IRF_LINK_UP: IRF port came up.
对系统的影响	导致IRF合并
日志产生原因	IRF链路恢复
处理建议	无需处理

66.4 IRF_MEMBERID_CONFLICT

日志内容	IRF member ID conflict occurred. The ID [UINT32] has been used for another device with CPU-Mac: [STRING].
日志含义	在同一广播域中发现跟自己成员编号相同的设备
参数解释	$1：设备的成员编号 $2：设备的CPU MAC
日志等级	4 (Warning)
举例	IRF/4/IRF_MEMBERID_CONFLICT:-slot = 5; IRF member ID conflict occurred, The ID 5 has been used for another device with CPU-Mac: 000c-29d7-c1ae.
对系统的影响	对系统无影响
日志产生原因	成员编号冲突，在同一广播域中有其它设备的成员编号和本设备的成员编号相同
处理建议	在IRF中的设备成员编号保持不变，请登录未加入IRF的那台设备，并在该设备上执行**irf member renumber**命令将设备的成员编号修改为IRF中其它未被使用的编号

66.5 IRF_MERGE

日志内容	IRF merge occurred.
日志含义	IRF发生合并
参数解释	无
日志等级	4 (Warning)
举例	IRF/4/IRF_MERGE: IRF merge occurred.
对系统的影响	对系统无影响
日志产生原因	IRF链路状态恢复到up
处理建议	无需处理

66.6 IRF_MERGE_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system needs a reboot.
日志含义	IRF发生合并，本地IRF系统需要重启
参数解释	无
日志等级	4 (Warning)
举例	IRF/4/IRF_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
对系统的影响	本地IRF系统重启期间无法提供服务
日志产生原因	IRF链路状态恢复到up，导致IRF发生合并，且本地IRF系统在角色选举中失败
处理建议	重启本地IRF系统。本地IRF系统重启后，本地IRF系统的所有成员设备会以备设备的身份加入竞选成功的IRF系统中

66.7 IRF_MERGE_NOT_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system does not need to reboot.
日志含义	IRF发生合并时，本地IRF系统无需重启
参数解释	无
日志等级	5 (Notification)
举例	IRF/5/IRF_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
对系统的影响	对系统无影响
日志产生原因	IRF链路状态恢复到up，导致IRF发生合并，且本地IRF系统在角色选举中成功
处理建议	无需处理

67 ISIS

本节介绍 IS-IS 模块输出的日志信息。

67.1 ISIS_LSP_CONFLICT

日志内容	IS-IS [UINT16], [STRING] LSP, LSPID=[STRING], SeqNum=[HEX], system ID conflict might exist.
日志含义	网络中可能存在System ID冲突
参数解释	$1：进程ID $2：IS类型，值为Level-1或Level-2 $3：LSP ID $4：LSP序列号
日志等级	5 (Notification)
举例	ISIS/5/ISIS_LSP_CONFLICT: -MDC=1; IS-IS 1, Level-1 LSP, LSPID=1111.1111.1111.00-00, SeqNum=0x000045bf, system ID conflict might exist.
对系统的影响	可能会导致LSP不断刷新，造成路由振荡
日志产生原因	网络中可能存在System ID冲突
处理建议	**1.** 排查并修改拓扑中设备的 System ID 配置，保证拓扑内设备的 System ID 不重复。 **2.** 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

67.2 ISIS_NBR_CHG

日志内容	IS-IS [UINT16], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING], Reason: [STRING].
日志含义	IS-IS邻居状态变化以及状态变化的原因
参数解释	$1：IS-IS进程ID $2：IS-IS邻居等级 $3：邻居ID $4：接口名称 $5：当前邻居状态，包括DOWN、UP和INIT $6：邻居状态变化原因，包括： • circuit data clean：邻居状态发生变化时，清除路由数据，导致邻居状态变为 down • holdtime expired：没有收到邻居发送的 Hello 报文，则认为邻居失效，将邻居状态置为 down • BFD session down：BFD 检测到链路故障并通知 IS-IS，IS-IS 将邻居状态置为 down • peer reset：执行 **reset isis peer**命令，导致邻居状态变为down • circuit ID conflicts：收到邻居发送的 Hello 报文中，circuit ID 不一致，导致邻居状态变为 down • P2P peer GR down：GR 恢复过程中，收到邻居发送的 Hello 报文中没有携带 GR 选项，导致邻居状态变为 down • 2way-pass：IS-IS 邻居建立成功，邻居状态变为 UP • 2way-fail：收到邻居发送的 one-way Hello 报文，邻居状态变为 INIT
日志等级	5 (Notification)
举例	ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency 0000.0000.0001 (GigabitEthernet1/0/1), state changed to DOWN, Reason: circuit data clean.
对系统的影响	可能导致IS-IS重新计算路由，造成路由振荡，以及业务流量振荡
日志产生原因	• IS-IS 邻接关系 Up 或 Down • IS-IS 配置错误 • 系统繁忙导致 IS-IS 邻居关系闪断 • 链路故障导致 IS-IS 邻居关系变化
处理建议	邻居状态变化原因为circuit data clean时，处理建议如下： 1. 请执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看IS-IS接口物理层状态，如果接口物理层状态为Down，请先处理接口故障问题。如果接口物理状态为Up，则请执行步骤2。 2. 请执行 **ping**命令，检查设备链路是否故障（包括传输设备故障）。如果链路正常，则请执行步骤 3。 3. 请使用 **display current-configuration configuration isis**命令检查IS-IS配置是否正确。 o 如果配置正确，则请执行步骤 4。 o 如果配置不正确，请修改为正确的配置。然后检查是否还会产生此日志。如果不再产生此日志，则处理过程结束。如果还会产生此日志，则请执行步骤 4。 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

邻居状态变化原因为holdtime expired时，处理建议如下：

5. 请使用 **ping**命令检查本端到对端的链路状态是否良好。
   - 如果链路正常，则请执行步骤 2。
   - 如果链路故障，则请执行步骤 4。
6. 在对端设备上使用 **display current-configuration configuration isis** 命令检查IS-IS配置是否正确。
   - 如果配置正确，则请执行步骤 3。
   - 如果配置不正确，请修改为正确的配置。然后检查是否还会产生此日志。如果不再产生此日志，则处理过程结束。如果还会产生此日志，则请执行步骤 7。
7. 请使用 **display cpu-usage**命令检查CPU利用率是否过高。
   - 如果 CPU 利用率过高，则请执行步骤 6。
   - 如果 CPU 利用率不高，则请执行步骤 7。
8. 请排除链路故障，然后使用 **display isis packet hello by-interface** *interface-type interface-number*命令检查本端是否能够收到邻居发送的Hello报文。其中，*interface-type interface-number*为日志中的接口名称和编号。
   - 如果无法收到邻居发送的 Hello 报文，则请执行步骤 7。
   - 如果可以收到邻居发送的 Hello 报文，则请执行步骤 5。
9. 修改 IS-IS 配置，然后检查邻居状态是否变为 UP。
   - 如果邻居状态变为 UP，则处理过程结束。
   - 如果邻居状态没有变为 UP，则请执行步骤 7。
10. 请使用 **display current-configuration**命令检查本端设备的配置，删除不必要的配置。然后检查邻居状态是否变为UP。
    - 如果邻居状态变为 UP，则处理过程结束。
    - 如果邻居状态没有变为 UP，则请执行步骤 7。
11. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

邻居状态变化原因为BFD session down时，处理建议如下：

12. 请使用 **ping**命令检查本端到对端的链路状态是否良好。
    - 如果链路正常，则请执行步骤 3。
    - 如果链路故障，则请执行步骤 2。
13. 请排除链路故障。
14. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

邻居状态变化原因为peer reset时，处理建议如下：

15. 请使用 **display isis troubleshooting**命令检查邻居状态变为Down的原因是否为“the reset isis peer command was executed”。
    - 如果是，说明用户执行了 **reset isis peer**命令导致邻居状态变化，则该日志为系统正常运行时产生的信息，无需处理。
    - 如果不是，则请执行步骤 2。
16. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

邻居状态变化原因为circuit ID conflicts时，检查邻居是否反复修改了使能IS-IS的接口。

邻居状态变化原因为P2P peer GR down时，检查邻居设备是否支持GR能力。

邻居状态变化原因为2way-fail时，处理建议如下：

17. 请使用 **display isis packet hello by-interface** *interface-type interface-number*命令检查本端是否能够收到邻居发送的Hello报文。其中，*interface-type interface-number*为日志中的接口名称和编号。

	○ 如果无法收到邻居发送的 Hello 报文，则请执行步骤 3。 ○ 如果可以收到邻居发送的 Hello 报文，则请执行步骤 5。 **18.** 检查两端的认证配置是否一致。 ○ 如果一致，则请执行步骤 3。 ○ 如果不一致，请修改认证配置，并保证修改后两端的认证配置一致。然后检查是否还会产生此日志。如果不再产生此日志，则处理过程结束。如果还会产生此日志，则请执行步骤 3。 **19.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

68 ISSU

本节介绍 ISSU 模块输出的日志信息。

68.1 ISSU_LOAD_FAILED

日志内容	Failed to execute the issu load command.
日志含义	用户执行**issu load**命令进行ISSU升级失败
参数解释	无
日志等级	5 (Notification)
举例	ISSU/5/ISSU_LOAD_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the issu load command.
对系统的影响	ISSU升级失败
日志产生原因	用户执行**issu load**命令进行ISSU升级失败，需根据提示信息分析原因
处理建议	请根据提示信息采取相应措施

68.2 ISSU_LOAD_SUCCESS

日志内容	Executed the issu load command successfully.
日志含义	用户执行**issu load**命令进行ISSU升级成功
参数解释	无
日志等级	5 (Notification)
举例	ISSU/5/ISSU_LOAD_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the issu load command successfully.
对系统的影响	对系统无影响
日志产生原因	用户执行**issu load**命令进行ISSU升级成功
处理建议	无需处理

68.3 ISSU_PROCESSWITCHOVER

日志内容	Switchover completed. The standby process became the active process.
日志含义	用户执行**issu run switchover**进行主备倒换完成，备进程已升级为主进程
参数解释	无
日志等级	5 (Notification)
举例	ISSU/5/ISSU_PROCESSWITCHOVER: Switchover completed. The standby process became the active process.
对系统的影响	对系统无影响
日志产生原因	用户执行**issu run switchover**进行主备倒换完成
处理建议	无需处理

68.4 ISSU_ROLLBACKCHECKNORMAL

日志内容	The rollback might not be able to restore the previous version for [STRING] because the status is not normal.
日志含义	由于有升级过的板状态不为Normal导致回滚到升级前的版本失败
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	4 (Warning)
举例	ISSU/4/ISSU_ROLLBACKCHECKNORMAL: The rollback might not be able to restore the previous version for chassis 1 slot 2 because the status is not normal.
对系统的影响	导致回滚到升级前的版本失败
日志产生原因	ISSU升级过程中，且ISSU状态为Switching，用户执行**issu rollback**命令回滚或ISSU回滚定时器超时自动回滚，如果有升级过的板状态不为Normal，会输出该日志
处理建议	1. 执行 **display device**命令查看单板状态，请等到升级过的单板状态为Normal后，再执行 **issu rollback**命令回滚 2. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

69 KPI

本节介绍 KPI 数据采集模块输出的日志信息。

69.1 INDICATOR_UPPERLIMIT_ALARM

日志内容	CHASSIS [[INT32]] SLOT [[INT32]] CPU [[INT32]] Module [[STRING]] Object [[STRING]] Indicator [[STRING]] Value [[STRING]] exceeded the upper limit of [STRING].
日志含义	KPI采样到的指标超出上限
参数解释	$1：KPI采样的指标所属框号 $2：KPI采样的指标所属槽号 $3：KPI采样的指标所属CPU ID $4：KPI采样的指标所属模块 $5：KPI采样的指标所属对象 $6：KPI采样的指标 $7：KPI采样的指标值 $8：指标的上限
日志等级	5 (Notification)
举例	KPI/5/INDICATOR_UPPERLIMIT_ALARM: CHASSIS [0] SLOT [2] CPU [0] Module [ifmgr] Object [GigabitEthernet2/0/1] Indicator [if actual speed] Value [950] exceeded the upper limit of 900.
对系统的影响	根据具体超限的指标对系统影响不同，例如 • CPU 利用率超出上限则可能导致系统负载超限，系统异常 • ACL 资源利用率超出上限可能导致无法新增 ACL 规则 • FIB 转发表项利用率超出上限可能导致报文转发失败
日志产生原因	开启智能监控功能之后，KPI采集到的指标值超出上限
处理建议	系统正常运行时产生的信息，无需处理

69.2 INDICATOR_LOWERLIMIT_ALARM

日志内容	CHASSIS [[INT32]] SLOT [[INT32]] CPU [[INT32]] Module [[STRING]] Object [[STRING]] Indicator [[STRING]] Value [[STRING]] is below the lower limit of [STRING].
日志含义	KPI采样到的指标低于下限
参数解释	$1：KPI采样的指标所属框号 $2：KPI采样的指标所属槽号 $3：KPI采样的指标所属CPU ID $4：KPI采样的指标所属模块 $5：KPI采样的指标所属对象 $6：KPI采样的指标 $7：KPI采样的指标值 $8：指标的下限
日志等级	5 (Notification)
举例	KPI/5/INDICATOR_LOWERLIMIT_ALARM: CHASSIS [0] SLOT [2] CPU [0] Module [ifmgr] Object [GigabitEthernet2/0/1] Indicator [if actual speed] Value [50] is below the lower limit of 100.
对系统的影响	对系统无影响
日志产生原因	开启智能监控功能之后，KPI采集到的指标值低于下限
处理建议	系统正常运行时产生的信息，无需处理

69.3 INDICATOR_RECOVER_ALARM

日志内容	CHASSIS [[INT32]] SLOT [[INT32]] CPU [[INT32]] Module [[STRING]] Object [[STRING]] Indicator [[STRING]] Value [[STRING]] returned to normal between [STRING] and [STRING].
日志含义	KPI采集到指标值从超限状态恢复到正常的水平
参数解释	$1：KPI采样的指标所属框号 $2：KPI采样的指标所属槽号 $3：KPI采样的指标所属CPU ID $4：KPI采样的指标所属模块 $5：KPI采样的指标所属对象 $6：KPI采样的指标 $7：KPI采样的指标值 $8：指标的下限 $9：指标的上限
日志等级	5 (Notification)
举例	KPI/5/INDICATOR_RECOVER_ALARM:CHASSIS [0] SLOT [2] CPU [0] Module [ifmgr] Object [GigabitEthernet2/0/1] Indicator [if actual speed] Value [500] returned to normal between 100 and 900.
对系统的影响	对系统无影响
日志产生原因	开启智能监控功能之后，KPI采集到指标值恢复到上限和下限之间
处理建议	系统正常运行时产生的信息，无需处理

69.4 INDICATOR_PREDICT_UPPERLIMIT_ALARM

日志内容	CHASSIS [[INT32]] SLOT [[INT32]] CPU [[INT32]] Module [[STRING]] Object [[STRING]] Indicator [[STRING]] Predict Value [[STRING]] exceeded the upper limit of [STRING].
日志含义	根据KPI采集指标值预测得到未来该指标值将超出上限
参数解释	$1：KPI采样的指标所属框号 $2：KPI采样的指标所属槽号 $3：KPI采样的指标所属CPU ID $4：KPI采样的指标所属模块 $5：KPI采样的指标所属对象 $6：KPI采样的指标 $7：KPI采样的指标值 $8：指标的上限
日志等级	5 (Notification)
举例	KPI/5/INDICATOR_PREDICT_UPPERLIMIT_ALARM: CHASSIS [0] SLOT [2] CPU [0] Module [ifmgr] Object [GigabitEthernet2/0/1] Indicator [if actual speed] Predict Value [950] exceeded the upper limit of 900.
对系统的影响	在未来30天之后，指标值存在超限风险，根据具体超限的指标对系统影响不同，例如 • CPU 利用率超出上限则可能导致系统负载超限，系统异常 • ACL 资源利用率超出上限可能导致无法新增 ACL 规则 • FIB 转发表项利用率超出上限可能导致报文转发失败
日志产生原因	开启智能预测功能之后，预测得到指标值高于上限
处理建议	系统正常运行时产生的信息，无需处理

69.5 INDICATOR_PREDICT_LOWERLIMIT_ALARM

日志内容	CHASSIS [[INT32]] SLOT [[INT32]] CPU [[INT32]] Module [[STRING]] Object [[STRING]] Indicator [[STRING]] Predict Value [[STRING]] is below the lower limit of [STRING].
日志含义	根据KPI采集指标值预测得到未来该指标值将低于上限
参数解释	$1：KPI采样的指标所属框号 $2：KPI采样的指标所属槽号 $3：KPI采样的指标所属CPU ID $4：KPI采样的指标所属模块 $5：KPI采样的指标所属对象 $6：KPI采样的指标 $7：KPI采样的指标值 $8：指标的下限
日志等级	5 (Notification)
举例	KPI/5/INDICATOR_PREDICT_LOWERLIMIT_ALARM: CHASSIS [0] SLOT [2] CPU [0] Module [ifmgr] Object [GigabitEthernet2/0/1] Indicator [if actual speed] Predict Value [50] is below the lower limit of 100.
对系统的影响	对系统无影响
日志产生原因	开启智能预测功能之后，预测得到指标值低于下限
处理建议	系统正常运行时产生的信息，无需处理

69.6 INDICATOR_PREDICT_RECOVER_ALARM

日志内容	CHASSIS [[INT32]] SLOT [[INT32]] CPU [[INT32]] Module [[STRING]] Object [[STRING]] Indicator [[STRING]] Predict Value [[STRING]] returned to normal between [STRING] and [STRING].
日志含义	根据KPI采集指标值预测得到未来该指标值将从超限状态恢复到正常的水平
参数解释	$1：KPI采样的CHASSIS [0] SLOT [2] CPU [0]框号 $2：KPI采样的CHASSIS [0] SLOT [2] CPU [0]槽号 $3：KPI采样的CHASSIS [0] SLOT [2] CPU [0]CPU ID $4：KPI采样的CHASSIS [0] SLOT [2] CPU [0]模块 $5：KPI采样的CHASSIS [0] SLOT [2] CPU [0]对象 $6：KPI采样的指标 $7：KPI采样的指标值 $8：指标的下限 $9：指标的上限
日志等级	5 (Notification)
举例	KPI/5/INDICATOR_PREDICT_RECOVER_ALARM: CHASSIS [0] SLOT [2] CPU [0] Module [ifmgr] Object [GigabitEthernet2/0/1] Indicator [if actual speed] Predict Value [500] returned to normal between 100 and 900.
对系统的影响	对系统无影响
日志产生原因	智能预测得到的指标值恢复到上限和下限之间
处理建议	系统正常运行时产生的信息，无需处理

70 L2PT

本节介绍 L2PT 模块输出的日志信息。

70.1 L2PT_ADD_GROUPMEMBER_FAILED

日志内容	Failed to add [STRING] as a member to the VLAN tunnel group for [STRING].
日志含义	接口加入指定协议的VLAN Tunnel组播组失败
参数解释	$1：接口名称 $2：协议类型
日志等级	4 (Warning)
举例	L2PT/4/L2PT_ADD_GROUPMEMBER_FAILED: Failed to add GigabitEthernet2/0/1 as a member to the VLAN tunnel group for STP.
对系统的影响	该接口无法透明传输指定协议的报文
日志产生原因	如需L2PT功能生效，需要端口创建并加入指定协议的VLAN Tunnel组播组，在此过程中，设备下发L2PT功能相关的驱动失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

70.2 L2PT_CREATE_TUNNELGROUP_FAILED

日志内容	Failed to create a VLAN tunnel group for [STRING].
日志含义	创建执行协议的VLAN Tunnel组播组失败
参数解释	$1：协议类型
日志等级	4 (Warning)
举例	L2PT/4/L2PT_CREATE_TUNNELGROUP_FAILED: Failed to create a VLAN tunnel group for STP.
对系统的影响	接口无法透明传输指定协议的报文
日志产生原因	如需L2PT功能生效，需要端口创建并加入指定协议的VLAN Tunnel组播组，在此过程中，设备下发L2PT功能相关的驱动失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

70.3 L2PT_ENABLE_DROP_FAILED

日志内容	Failed to enable [STRING] packet drop on [STRING].
日志含义	接口上开启指定协议的L2PT Drop功能失败
参数解释	$1：协议类型 $2：接口名称
日志等级	4 (Warning)
举例	L2PT/4/L2PT_ENABLE_DROP_FAILED: Failed to enable STP packet drop on GigabitEthernet2/0/1.
对系统的影响	该接口无法对指定协议的报文使用L2PT Drop功能
日志产生原因	设备下发L2PT功能相关的驱动失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

70.4 L2PT_SET_MULTIMAC_FAILED

日志内容	Failed to set a tunnel destination MAC address to [MAC].
日志含义	配置Tunnel报文的组播目的MAC地址失败
参数解释	$1：MAC地址
日志等级	4 (Warning)
举例	L2PT/4/L2PT_SET_MULTIMAC_FAILED: Failed to set a tunnel destination MAC address to 010f-e200-0003.
对系统的影响	L2PT功能无法为二层协议报文封装日志指定的组播MAC地址进行传输
日志产生原因	设备下发L2PT功能相关的驱动失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

71 L2TPV2

本节介绍 L2TPV2 模块输出的日志信息。

71.1 L2TPV2_SESSION_EXCEED_LIMIT

日志内容	Number of L2TP sessions exceeded the limit.
日志含义	设备上建立的L2TP会话数目达到最大值
参数解释	无
日志等级	4 (Warning)
举例	L2TPV2/4/L2TPV2_SESSION_EXCEED_LIMIT: Number of L2TP sessions exceeded the limit.
对系统的影响	无法再创建新的L2TP会话，即不允许新的L2TP用户上线
日志产生原因	设备上建立的L2TP会话数目已经达到最大值
处理建议	如需上线新的L2TP用户，需要等老的L2TP用户下线释放L2TP会话资源，或者管理员执行**reset ppp access-user**命令强制下线部分老的L2TP用户以释放L2TP会话资源

71.2 L2TPV2_TUNNEL_EXCEED_LIMIT

日志内容	Number of L2TP tunnels exceeded the limit.
日志含义	设备上建立的L2TP隧道数目达到最大值
参数解释	无
日志等级	4 (Warning)
举例	L2TPV2/4/L2TPV2_TUNNEL_EXCEED_LIMIT: Number of L2TP tunnels exceeded the limit.
对系统的影响	无法再创建新的L2TP隧道
日志产生原因	设备上建立的L2TP隧道数目达到最大值
处理建议	要想建立新的L2TP隧道，可以通过**reset l2tp tunnel**命令立即断开空闲的L2TP隧道，或等待Hello定时器超时后设备自动断开空闲的L2TP隧道

72 L2VPN

本节介绍 L2VPN 模块输出的日志信息。

72.1 L2VPN_ARP_MOBILITY_SUPPRESS (public instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was suppressed in the public instance due to frequent ARP mobility events.
日志含义	ARP迁移频率超过限制
参数解释	$1：IP地址 $2：MAC地址
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_ARP_MOBILITY_SUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was suppressed in the public instance due to frequent ARP mobility events.
对系统的影响	该ARP无法迁移
日志产生原因	开启ARP反复迁移抑制功能后，ARP迁移频率超过限制，抑制该ARP迁移
处理建议	ARP迁移频率过高的原因可能是网络中存在IP地址冲突。请检查网络中的IP地址配置，避免IP地址冲突

72.2 L2VPN_ARP_MOBILITY_SUPPRESS (VPN instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was suppressed in VPN instance [STRING] due to frequent ARP mobility events.
日志含义	ARP迁移频率超过限制
参数解释	$1：IP地址 $2：MAC地址 $3：VPN实例名称
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_ARP_MOBILITY_SUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was suppressed in VPN instance vpna due to frequent ARP mobility events.
对系统的影响	该ARP无法迁移
日志产生原因	开启ARP反复迁移抑制功能后，ARP迁移频率超过限制，抑制该ARP迁移
处理建议	ARP迁移频率过高的原因可能是网络中存在IP地址冲突。请检查网络中的IP地址配置，避免IP地址冲突

72.3 L2VPN_ARP_MOBILITY_UNSUPPRESS (public instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was unsuppressed in the public instance.
日志含义	解除指定ARP的迁移抑制
参数解释	$1：IP地址 $2：MAC地址 $3：VPN实例名称
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_ARP_MOBILITY_UNSUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was unsuppressed in the public instance.
对系统的影响	无
日志产生原因	执行**undo evpn route arp-mobility suppress**命令后，解除指定ARP的迁移抑制，可以向远端通告该ARP信息
处理建议	无需处理

72.4 L2VPN_ARP_MOBILITY_UNSUPPRESS (VPN instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was unsuppressed in VPN instance [STRING].
日志含义	解除指定ARP的迁移抑制
参数解释	$1：IP地址 $2：MAC地址 $3：VPN实例名称
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_ARP_MOBILITY_UNSUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was unsuppressed in VPN instance vpna.
对系统的影响	无
日志产生原因	执行**undo evpn route arp-mobility suppress**命令后，解除指定ARP的迁移抑制，可以向远端通告该ARP信息
处理建议	无需处理

72.5 L2VPN_MAC_MOBILITY_SUPPRESS

日志内容	MAC address [STRING] was suppressed in VSI [STRING] due to frequent MAC mobility events.
日志含义	MAC地址迁移频率超过限制
参数解释	$1：MAC地址 $2：VSI名称
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_MAC_MOBILITY_SUPPRESS: MAC address 0001-0001-0001 was suppressed in VSI vpna due to frequent MAC mobility events.
对系统的影响	该MAC地址无法迁移
日志产生原因	开启MAC地址反复迁移抑制功能后，MAC地址迁移频率超过限制，抑制该MAC地址迁移
处理建议	MAC地址迁移频率过高的原因可能是网络中存在MAC地址冲突。请检查网络中的MAC地址配置，避免MAC地址冲突

72.6 L2VPN_MAC_MOBILITY_UNSUPPRESS

日志内容	MAC address [STRING] was unsuppressed in VSI [STRING].
日志含义	解除指定MAC地址的迁移抑制
参数解释	$1：MAC地址 $2：VSI名称
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_MAC_MOBILITY_UNSUPPRESS: MAC address 0001-0001-0001 was unsuppressed in VSI vpna.
对系统的影响	无
日志产生原因	执行**undo evpn route mac-mobility suppress**命令后，解除指定MAC地址的迁移抑制，可以向远端通告该MAC地址
处理建议	无需处理

72.7 L2VPN_BGPVC_CONFLICT_LOCAL

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with local site.
日志含义	本端Site ID和另一个远端Site ID冲突
参数解释	$1：冲突的远端Site ID $2：引发冲突的远端Site的IP地址 $3：引发冲突的远端Site的Route Distinguisher
日志等级	5 (Notification)
举例	L2VPN/5/L2VPN_BGPVC_CONFLICT_LOCAL: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with local site.
对系统的影响	无法建立PW
日志产生原因	本端Site ID和另一个远端Site ID冲突。触发该日志的原因可能有： • 新接收到一个远端 Site ID 和本端 Site ID 相同 • 新配置本端 Site ID 和已接收到的一个远端 Site ID 相同
处理建议	更改远端或本端Site ID，或者修改配置使得远端Site不引入到本端Site所在实例

72.8 L2VPN_BGPVC_CONFLICT_REMOTE

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with another remote site.
日志含义	两个远端的Site ID冲突
参数解释	$1：冲突的远端Site ID $2：引发冲突的远端Site的IP地址 $3：引发冲突的远端Site的Route Distinguisher
日志等级	5 (Notification)
举例	L2VPN/5/L2VPN_BGPVC_CONFLICT_REMOTE: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with another remote site.
对系统的影响	本端设备只能与一个远端设备建立PW
日志产生原因	两个远端的Site ID冲突。触发该日志的原因可能为：在已经接收一个远端Site的情况下，接收到另一个远端Site，两者的Site ID相同
处理建议	更改其中一个远端Site ID，或者修改配置使得两个远端不引入到同一个实例中

72.9 L2VPN_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for L2VPN.
日志含义	L2VPN硬件资源不足
参数解释	无
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH: No enough hardware resource for L2VPN.
对系统的影响	无法再创建新的SI、PW或AC
日志产生原因	L2VPN硬件资源不足
处理建议	请检查是否生成了当前业务不需要的VSI、PW或AC，是则删除对应配置

72.10 L2VPN_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for L2VPN are restored.
日志含义	L2VPN硬件资源恢复
参数解释	无
日志等级	6 (Informational)
举例	L2VPN/6/L2VPN_HARD_RESOURCE_RESTORE: Hardware resources for L2VPN are restored.
对系统的影响	无
日志产生原因	L2VPN硬件资源恢复
处理建议	无需处理

72.11 L2VPN_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for a static PW in [STRING] [STRING] is duplicate.
日志含义	配置的静态PW的入标签已被占用
参数解释	$1：入标签值 $2：L2VPN类型，交叉连接组或者VSI $3：交叉连接组或者VSI的名称
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_LABEL_DUPLICATE: Incoming label 1024 for a static PW in Xconnect-group aaa is duplicate.
对系统的影响	当前配置的PW无法创建
日志产生原因	交叉连接组或者VSI的静态PW的入标签被静态LSP或者静态CRLSP占用。触发该日志的原因可能有： • 在 MPLS 已使能的情况下，配置了一条入标签被静态 LSP 或者静态 CRLSP 占用的静态 PW • 在入标签被静态 LSP 或静态 CRLSP 占用的静态 PW 存在的情况下，使能 MPLS
处理建议	删除该静态PW，重新配置一条静态PW，并指定新的入标签值

72.12 L2VPN_MLAG_AC_CONFLICT

日志内容	The dynamic AC created for Ethernet service instance [INT32] on interface [STRING] causes a conflict.
日志含义	peer-link链路上生成的动态AC冲突
参数解释	$1：以太网服务实例编号 $2：以太网服务实例所在的接口
日志等级	4 (Warning)
举例	L2VPN/4/L2VPN_MLAG_AC_CONFLICT: The dynamic AC created for Ethernet service instance 10 on interface Bridge-Aggregation 5 causes a conflict.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	EVPN支持M-LAG组网中，peer-link链路由隧道切换为聚合链路时，根据不同的静态AC生成的动态AC相互冲突
处理建议	删除引发冲突的动态AC对应的静态AC，再重新配置静态AC，并为AC指定合理的报文匹配规则

72.13 PROCESS

日志内容	The EVPN global MAC address is a reserved MAC.
日志含义	配置的EVPN全局MAC地址为当前设备的预留MAC地址
参数解释	无
日志等级	7 (Debug)
举例	L2VPN/7/PROCESS: The EVPN global MAC address is a reserved MAC.
对系统的影响	设备的预留MAC地址被占用，可使用的预留MAC地址减少
日志产生原因	配置的EVPN全局MAC地址为当前设备的预留MAC地址
处理建议	修改EVPN全局MAC地址

73 LAGG

本节介绍 LAGG 模块输出的日志信息。

73.1 LAGG_ACTIVE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the active state.
日志含义	聚合组内某成员端口成为选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_ACTIVE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the active state.
对系统的影响	无
日志产生原因	聚合组内某成员端口成为选中端口
处理建议	无需处理

73.2 LAGG_AUTO_AGGREGATION

日志内容	Failed to assign automatic assignment-enabled interface [STRING] to the aggregation group. Please check the configuration on the interface.
日志含义	因为配置原因，导致接口无法自动加入聚合组
参数解释	$1：端口名称
日志等级	6 (Informational)
举例	LAGG/6/LAGG_AUTO_AGGREGATON: Failed to assign automatic assignment-enabled interface FGE1/0/1 to the aggregation group. Please check the configuration on the interface.
对系统的影响	接口无法自动加入聚合组
日志产生原因	开启自动聚合功能后，由于以下原因导致接口无法加入聚合组： • 该接口的属性类配置和聚合接口不同 • 该接口上存在不能加入聚合组的配置
处理建议	• 修改对应接口上的属性类配置，以保证和聚合接口一致 • 删除对应接口上与加入聚合组互斥的功能

73.3 LAGG_INACTIVE_AICFG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_AICFG: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内某成员端口的属性类配置与聚合接口属性类配置不同，该成员端口成为去选中端口
处理建议	修改该成员端口的属性类配置，使其与聚合接口属性类配置一致

73.4 LAGG_INACTIVE_BFD

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the BFD session state of the port is down.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_BFD: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the BFD session state of the port is down.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	聚合成员端口上的BFD会话down时，该成员端口变为非选中状态
处理建议	排查链路故障、检查该非选中状态的成员端口的操作key和属性类配置是否与参考端口一致

73.5 LAGG_INACTIVE_CONFIGURATION

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of the port is incorrect.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_CONFIGURATION: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of the port is incorrect.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内某成员端口配置限制，该成员端口变为非选中状态
处理建议	检查该端口是下是否存在与聚合功能冲突的配置

73.6 LAGG_INACTIVE_DUPLEX

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the duplex mode is different between the member port and the reference port.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_DUPLEX: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the duplex mode is different between the member port and the reference port.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内某成员端口的双工模式与参考端口不一致，该成员端口变为非选中状态
处理建议	修改该端口双工模式，使其与参考端口一致

73.7 LAGG_INACTIVE_HARDWAREVALUE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because of the port's hardware restirction.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_HARDWAREVALUE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because of the port's hardware restirction.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	聚合组内某成员端口因硬件限制与参考端口不一致，该成员端口变为非选中状态
处理建议	检查成员端口之间是否存在硬件差异

73.8 LAGG_INACTIVE_IFCFG_DEFAULT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because no LACPDU was received by the reference port.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_IFCFG_DEFAULT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because no LACPDU was received by the reference port.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内参考端口没有收到对端的LACPDU，该成员端口变为非选中状态
处理建议	检查对端是否发送LACPDU

73.9 LAGG_INACTIVE_IFCFG_LOOPPORT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the reference port received its own LACPDUs.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_IFCFG_LOOPPORT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the reference port received its own LACPDUs.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内参考端口收到自己的LACPDU，该成员端口变为非选中状态
处理建议	检查对端设备是否存在环路

73.10 LAGG_INACTIVE_IFCFG_NONAGG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link of the port was not aggregatable.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_IFCFG_NONAGG: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the link of the port was not aggregatable.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内端口所在链路不可聚合，该成员端口变为非选中状态
处理建议	修改端口配置

73.11 LAGG_INACTIVE_KEY_INVALID

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port's operational key was invalid.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_KEY_INVALID: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the port's operational key was invalid.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内参考端口操作Key无效，该成员端口变为非选中状态
处理建议	修改参考端口配置

73.12 LAGG_INACTIVE_LACP_ISOLATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link-aggregation lacp isolate setting had been configured.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_LACP_ISOLATE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the link-aggregation lacp isolate setting had been configured.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	开启聚合流量隔离功能，导致聚合成员端口变为非选中状态
处理建议	关闭聚合流量隔离功能

73.13 LAGG_INACTIVE_LOWER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of Selected ports was below the lower limit.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_LOWER_LIMIT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of Selected ports was below the lower limit.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	因聚合组内选中端口数量未达到配置的最小选中端口数，聚合组内某成员端口变为非选中状态
处理建议	增加选中端口数量，使其达到最小选中端口数

73.14 LAGG_INACTIVE_NODEREMOVE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the card that hosts the port was absent.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_NODEREMOVE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the card that hosts the port was absent.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内端口所在单板被拔出，该成员端口变为非选中状态
处理建议	检查接口所在板已插入

73.15 LAGG_INACTIVE_OPERSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the peer port did not have the Synchronization flag.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_OPERSTATE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the peer port did not have the Synchronization flag.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组对端成员端口所在链路未处于同步状态，本端成员端口变为非选中状态
处理建议	检查对端发送的LACPDU

73.16 LAGG_INACTIVE_PARTNER

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link aggregation configuration of its peer port was incorrect.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_PARTNER: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the link aggregation configuration of its peer port was incorrect.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	动态聚合组内，由于对端端口聚合配置不正确变为非选中状态，本端端口变为非选中状态
处理建议	无需处理

73.17 LAGG_INACTIVE_PARTNER_KEY_WRONG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the operational key of the peer port was different from that of the reference port.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_PARTNER_KEY_WRONG: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the operational key of the peer port was different from that of the reference port.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组对端操作Key与参考端口不一致，本端成员端口变为非选中状态
处理建议	修改对端操作Key与参考端口一致

73.18 LAGG_INACTIVE_PARTNER_MAC_WRONG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the system MAC address of the peer port was different from that of the peer port for the reference port.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_PARTNER_MAC_WRONG: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the system MAC address of the peer port was different from that of the peer port for the reference port.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组对端系统MAC地址与参考端口的对端端口不一致，本端成员端口变为非选中状态
处理建议	修改对端系统MAC地址与参考端口一致

73.19 LAGG_INACTIVE_PARTNER_NONAGG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link of the peer port was not aggregatable.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_PARTNER_NONAGG: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the link of the peer port was not aggregatable.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内对端端口所在链路不可聚合，本端成员端口变为非选中状态
处理建议	修改对端端口配置

73.20 LAGG_INACTIVE_PHYSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the physical or line protocol state of the port was down.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_PHYSTATE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the physical or line protocol state of the port was down.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	聚合组内某成员端口处于down状态，该成员端口变为非选中状态
处理建议	使该端口处于UP状态

73.21 LAGG_INACTIVE_PORT_DEFAULT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port had not received LACPDUs.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_PORT_DEFAULT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the port had not received LACPDUs.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内成员端口未收到LACPDU，该成员端口变为非选中状态
处理建议	检查对端是否发送LACPDU

73.22 LAGG_INACTIVE_RDIRHANDLE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because link-aggregation traffic redirection was triggered on the local port.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_RDIRHANDLE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because link-aggregation traffic redirection was triggered on the local port.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组本端端口触发聚合重定向功能，该成员端口变为非选中状态
处理建议	修改端口配置

73.23 LAGG_INACTIVE_REDUNDANCY

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port was in secondary state in a redundancy group.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_ REDUNDANCY: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the port was in secondary state in a redundancy group.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内端口处于冗余备份状态，该成员端口变为非选中状态
处理建议	冗余组节点中使本端端口处于工作状态

73.24 LAGG_INACTIVE_RESOURCE_INSUFICIE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because hardware resources were not enough.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	3 (Error)
举例	LAGG/3/LAGG_INACTIVE_RESOURCE_INSUFICIE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because hardware resources were not enough.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	聚合资源不足导致聚合组内成员端口变为非选中端口
处理建议	无需处理

73.25 LAGG_INACTIVE_SPEED

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the speed configuration of the port was different from that of the reference portincorrect.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_SPEED: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the speed configuration of the port was different from that of the reference portincorrect.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	聚合组内某成员端口速率与参考端口不一致，该端口变为非选中状态
处理建议	修改该端口速率，使其与参考端口一致

73.26 LAGG_INACTIVE_STANDBY

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port was in Standby state.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_INACTIVE_STANDBY: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the port was in Standby state.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	由于聚合组内端口处于standby状态，该成员端口变为非选中状态
处理建议	等待一段时间再查看成员端口状态，确认是否处于选中状态，如果处于非选中状态，则根据**display link-aggregation troubleshooting**命令定位非选中原因及处理建议

73.27 LAGG_INACTIVE_UPPER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of Selected ports had reached the upper limit.
日志含义	成员端口成为非选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	3 (Error)
举例	LAGG/3/LAGG_INACTIVE_UPPER_LIMIT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of Selected ports had reached the upper limit.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	动态聚合组内选中端口数量已达到上限。后加入的成员端口成为选中端口，致使某成员端口变为非选中状态
处理建议	无需处理

73.28 LAGG_LACP_RECEIVE_TIMEOUT

日志内容	LACPDU reception timed out on member port [STRING] in aggregation group [STRING].
日志含义	接收对端的LACPDU超时
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_RECEIVE_TIMEOUT: LACPDU reception timed out on member port GE1/0/1 in aggregation group BAGG1.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	聚合组内成员端口接收对端的LACPDU超时
处理建议	查看线路是否正常

73.29 LAGG_PORT_DISCARDING_STATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the discarding state.
日志含义	聚合组内某成员端口成为阻塞端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_PORT_DISCARDING_STATE: Member port GE1/0/50 of aggregation group BAGG1 changed to the discarding state.
对系统的影响	该成员端口无法转发业务流量
日志产生原因	聚合组内某成员端口成为阻塞端口，无法转发业务流量
处理建议	执行**display link-aggregation troubleshooting**命令查看聚合组成员端口的选中状态及原因，并根据显示信息中的解决建议（Advice字段）排查并解决问题

73.30 LAGG_PORT_FORWARDING_STATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the forwarding state.
日志含义	聚合组内某成员端口成为选中端口
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6 (Informational)
举例	LAGG/6/LAGG_PORT_FORWARDING_STATE: Member port GE1/0/50 of aggregation group BAGG1 changed to the forwarding state.
对系统的影响	无

日志产生原因	聚合组内某成员端口成为选中端口，可以转发业务流量
处理建议	无需处理

73.31 LAGG_SELECTPORT_INCONSISTENT

日志内容	The maximum number of Selected ports for [STRING] on PEXs is inconsistent with that on the parent fabric. Please reconfigure this setting.
日志含义	PEX设备上聚合组中选中端口数超过了父设备上聚合组的最大选中端口数
参数解释	$1：聚合接口编号
日志等级	4 (Warning)
举例	LAGG/4/LAGG_SELECTPORT_INCONSISTENT: The maximum number of Selected ports for Route-Aggregation1 on PEXs is inconsistent with that on the parent fabric. Please reconfigure this setting.
对系统的影响	接口无法加入聚合组
日志产生原因	PEX设备上聚合组中选中端口数超过了父设备上聚合组的最大选中端口数，需要用户重新配置。触发该日志的原因可能有：以太网接口加入或退出聚合组
处理建议	用户重新配置父设备上聚合组的最大选中端口数或减少PEX设备上聚合组的选中端口，使得父设备与PEX设备的最大选中端口数保持一致

74 LDP

本节介绍 LDP 模块输出的日志信息。

74.1 LDP_ADJACENCY_DOWN

日志内容	ADJ ([STRING], [STRING], [STRING]) is down [STRING]. ([STRING])
日志含义	LDP邻接体down

参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0
	$2：VPN实例名。如果该会话属于公网，显示为public instance
	$3：接口名称。如果是Target Hello，该字段不显示
	$4：邻接体down的原因
	$5：邻接体相关信息：
	• Type：邻接体类型，取值包括：
	  ○ Link：表示 Link Hello 邻接关系
	  ○ Target：表示 Target Hello 邻接关系
	• SourceAddr：邻接体的源地址
	• DestinationAddr：邻接体的目的地址
	• TransportAddr：邻接体的传输地址
	• ADJUpTime：邻接体建立的持续时间，格式为 DD:HH:MM
	• HelloHoldTime：Hello 保持时间，单位为秒
	• HelloSentCount：本地发送 Hello 消息的总数
	• HelloRcvdCount：本地接收 Hello 消息的总数

日志等级	5 (Notification)
举例	LDP/5/LDP_ADJACENCY_DOWN: ADJ (10.200.0.60:0, public instance, GE2/0/1) is down (Hello timer expired). (Type=Link, SourceAddr=100.12.1.2, DestinationAddr=224.0.0.2, TransportAddr=22.2.2.2, ADJUpTime=0000:00:02, HelloHoldTime=15s, HelloSentCount=27, HelloRcvdCount=25)
对系统的影响	可能导致本地与LDP邻接体之间的LDP会话down
日志产生原因	LDP邻接体的状态变为down

处理建议	当LDP邻接体状态是down时，根据邻接体down的原因检查接口状态、链路状态和其他相关配置
	LDP邻接体down的原因包括：
	• VPN instance changed on interface：接口所属的VPN实例已更改。请在接口视图下配置 **ip binding vpn-instance**命令来修改接口与VPN实例的关联关系
	• LDP disabled on interface：接口上关闭LDP功能。请在接口视图下配置 **mpls ldp enable**命令来开启接口的LDP能力
	• MPLS disabled on interface：接口上关闭MPLS功能。请在接口视图下配置 **mpls enable**命令来开启接口的MPLS能力
	• interface not operational：接口不可用。请检查接口状态是否正常、接口的 IPv4 或 IPv6 地址配置是否正确
	• targeted peer deleted：手工删除LDP targeted Peer。请在LDP视图下执行 **target-peer**命令来恢复远程会话的配置
	• L2VPN disabled targeted peer：L2VPN 注销 targeted peer
	  ○ 对于MPLS L2VPN网络，请开启MPLS和L2VPN能力、创建交叉连接，并在交叉连接视图下执行 **peer**命令创建交叉连接PW
	  ○ 对于VPLS网络，请开启MPLS和L2VPN能力、创建VSI，并在VSI视图下执行 **peer**

	命令创建VPLS的PW
	• TE tunnel disabled targeted peer：TE 隧道注销 targeted peer。
	  ○ 执行 **display interface tunnel**命令来检查TE隧道的接口状态是否UP，若不是UP状态，则请检查MPLS TE隧道沿途的所有设备和接口上是否均开启MPLS和MPLS TE能力。若采用RSVP协议建立MPLS TE隧道，则需检查沿途所有设备和接口上是否均开启RSVP能力、链路上带宽和亲和属性等配置是否正确、RSVP协议验证功能配置是否准确。若静态建立MPLS TE隧道，则需检查静态CRLSP或SRLSP相关配置是否正确
	  ○ 执行 **display mpls ldp interface**命令检查该接口的MPLS和LDP能力是否正确配置，若未配置，则请在接口上执行 **mpls enable**和 **mpls ldp enable**命令
	• session protection disabled targeted peer：会话保护注销targeted peer。请在LDP视图下执行 **session protection**命令来恢复会话保护的配置
	• OSPF Remote LFA disabled targeted peer：OSPF Remote LFA 注销 targeted peer。OSPF 路由计算出 Remote LFA 的 PQ 节点地址变化，故注销旧 PQ 节点地址对应的 target peer。这是网络拓扑变化时的正常运行信息，无需处理
	• IS-IS Remote LFA disabled targeted peer：IS-IS Remote LFA 注销 targeted peer。IS-IS 路由计算出 Remote LFA 的 PQ 节点地址变化，故注销旧 PQ 节点地址对应的 target peer。这是网络拓扑变化时的正常运行信息，无需处理
	• process deactivated：LDP进程降级。等待LDP进程升级后自动恢复会话。建议在LDP视图下执行 **non-stop-routing**命令开启NSR功能，以降低进程升降级带来的影响
	• LDP instance deleted：LDP实例已删除。请在LDP视图下配置 **vpn-instance**命令来恢复指定VPN实例的LDP能力
	• hello hold timer expired：Hello 保持时间超时。检查链路是否稳定，更换链路或排除链路故障，使链路稳定
	• no IPv6 transport address：没有IPv6 传输地址。请在接口视图或LDP对等体视图下执行 **mpls ldp transport-address**命令配置IPv6 传输地址

74.2 LDP_MPLSLSRID_CHG

日志内容	Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
日志含义	MPLS LSR ID变化
参数解释	无
日志等级	5 (Notification)
举例	LDP/5/LDP_MPLSLSRID_CHG: Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
对系统的影响	对系统无影响
日志产生原因	公网LDP和VPN实例LDP的LSR ID选择方式为： **1.** 如果配置了 LDP LSR ID，则 LDP 的 LSR ID 为此命令配置的值 **2.** 否则，LDP 的 LSR ID 为 MPLS LSR ID 未配置公网LDP或VPN实例LDP的LSR ID时，修改MPLS LSR ID，会触发该日志
处理建议	当公网LDP或VPN实例LDP的LSR ID未配置时，使用命令**display mpls ldp parameter**查看已生效的LSR ID，并将其与配置的MPLS LSR ID进行比较。如果不一致，请手动重启公网LDP或VPN实例LDP会话，使得新配置的MPLS LSR ID生效

74.3 LDP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING] ([STRING]). ([STRING])
日志含义	LDP会话状态变化

参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0
	$2：VPN实例名。如果该会话属于公网，显示为public instance
	$3：会话状态，up或者down
	$4：会话失败的原因，仅在会话状态为down时显示
	$5：会话信息。仅在会话状态为down时，显示会话相关信息：
	• LocalTransportAddr：本地传输地址
	• PeerTransportAddr：对端传输地址
	• SessionRole：本地 LSR 在会话中的角色，取值为：
	  ○ Active：主动方
	  ○ Passive：被动方
	• SessionUpTime：会话处于 Operational 状态的持续时间，格式为 DD:HH:MM
	• KeepaliveTime：协商出来的 Keepalive 时间值，单位为秒
	• KeepaliveSentCount：本地发送的 Keepalive 消息的总数
	• KeepaliveRcvdCount：本地接收的 Keepalive 消息的总数
	• GracefulRestart：对等体上是否使能了 LDP GR 功能：
	  ○ On：表示使能
	  ○ Off：表未使能
	• SocketID：会话的套接字 ID
	• WaitSendMsgCount：等待发送的 TCP 消息数量
	• CPUusage：会话 down 时的 CPU 使用率
	• MemoryState：会话 down 时内存门限状态，取值包括：
	  ○ Normal：正常
	  ○ Minor：一级门限
	  ○ Severe：二级门限
	  ○ Critical：三级门限

日志等级	4 (Warning)
举例	LDP/4/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up. LDP/4/LDP_SESSION_CHG: Session (22.22.22.2:0, VPN instance: vpn1) is down (hello hold timer expired). (LocalTransportAddr=11.1.1.1, PeerTransportAddr=22.2.2.2, SessionRole=Passive, SessionUpTime=0000:00:35, KeepaliveTime=45s, KeepaliveSentCount=143, KeepaliveRcvdCount=148, GracefulRestart=Off, SocketID=35, WaitSendMsgCount=0, CPUUsage=19%, MemoryState=Normal)
对系统的影响	当会话状态变为up时，对系统无影响 当会话状态变为down时，基于该LDP会话的所有业务将中断
日志产生原因	LDP会话的状态发生改变
处理建议	当会话状态变为up时，为正常运行信息，无需处理 当会话状态变为down时，根据会话失败原因检查接口状态、链路状态和其他相关配置 会话失败原因及其处理建议为：

	• interface not operational：接口不可用。请检查接口状态是否正常、接口的 IPv4 或 IPv6 地址配置是否正确 • MPLS disabled on interface：接口上关闭MPLS功能。请在接口视图下配置 **mpls enable**命令来开启接口的MPLS能力 • LDP disabled on interface：接口上关闭LDP功能。请在接口视图下配置 **mpls ldp enable**命令来开启接口的LDP能力 • VPN instance changed on interface：接口所属的VPN实例已更改。请在接口视图下配置 **ip binding vpn-instance**命令来修改接口与VPN实例的关联关系 • LDP instance deleted：LDP实例已删除。请在LDP视图下配置 **vpn-instance**命令来恢复指定VPN实例的LDP能力 • targeted peer deleted：手工删除LDP targeted Peer。请在LDP视图下执行 **target-peer**命令来恢复远程会话的配置 • L2VPN disabled targeted peer：L2VPN 注销 targeted peer o 对于MPLS L2VPN网络，请开启MPLS和L2VPN能力、创建交叉连接，并在交叉连接视图下执行 **peer**命令创建交叉连接PW o 对于VPLS网络，请开启MPLS和L2VPN能力、创建VSI，并在VSI视图下执行 **peer**命令创建VPLS的PW • TE tunnel disabled targeted peer：TE 隧道注销 targeted peer o 执行 **display interface tunnel**命令来检查TE隧道的接口状态是否UP，若不是UP状态，则请检查MPLS TE隧道沿途的所有设备和接口上是否均开启MPLS和MPLS TE能力。若采用RSVP协议建立MPLS TE隧道，则需检查沿途所有设备和接口上是否均开启RSVP能力、链路上带宽和亲和属性等配置是否正确、RSVP协议验证功能配置是否准确。若静态建立MPLS TE隧道，则需检查静态CRLSP或SRLSP相关配置是否正确 o 执行 **display mpls ldp interface**命令检查该接口的MPLS和LDP能力是否正确配置，若未配置，则请在接口上执行 **mpls enable**和 **mpls ldp enable**命令 • session protection disabled targeted peer：会话保护注销targeted peer。请在LDP视图下执行 **session protection**命令来恢复会话保护的配置 • OSPF Remote LFA disabled targeted peer：OSPF Remote LFA 注销 targeted peer。OSPF 路由计算出 Remote LFA 的 PQ 节点地址变化，故注销旧 PQ 节点地址对应的 target peer。这是网络拓扑变化时的正常运行信息，无需处理 • IS-IS Remote LFA disabled targeted peer：IS-IS Remote LFA 注销 targeted peer。IS-IS 路由计算出 Remote LFA 的 PQ 节点地址变化，故注销旧 PQ 节点地址对应的 target peer。这是网络拓扑变化时的正常运行信息，无需处理 • process deactivated：LDP进程降级。等待LDP进程升级后自动恢复会话。建议在LDP视图下执行 **non-stop-routing**命令开启NSR功能，以降低进程升降级带来的影响 • failed to receive the initialization message：未收到初始化信息。执行“ping -a 本端地址 -c 次数（100 以上） 目的地址”命令，检查链路状态是否正常，是否出现丢包。若出现丢包，请收集告警信息和配置信息，联系技术支持。其中，本端地址和目的地址是指本端和目的设备的LSR ID，可以执行 **display mpls ldp parameter**命令查看本端和目的端设备的LSR ID • graceful restart reconnect timer expired：平滑重启重连时间超时。执行“ping -a 本端地址 -c 次数（100 以上）目的地址”命令，检查链路状态是否正常，是否出现丢包。若出现丢包，请收集告警信息和配置信息，联系技术支持。其中，本端地址和目的地址是指本端和目的设备的LSR ID，可以执行 **display mpls ldp parameter**命令查看本端和目的端设备的LSR ID • failed to recover adjacency by NSR：NSR恢复邻接关系失败。执行 **display ha service-group ldp**命令，查看显示信息中的State字段。如果State字段取值为

Realtime Backup状态，则表示数据备份完毕，需要等待State状态变为Realtime Backup状态，然后再做主备倒换

- failed to upgrade session by NSR：NSR升级会话失败。执行 **display ha service-group ldp**命令，查看显示信息中的State字段。如果State字段取值为Realtime Backup状态，则表示数据备份完毕，需要等待State状态变为Realtime Backup状态，然后再做主备倒换
- closed the GR session：GR会话关闭。执行“ping -a 本端地址 -c 次数（100 以上）目的地址”命令，检查链路状态是否正常，是否出现丢包。若出现丢包，请收集告警信息和配置信息，联系技术支持。其中，本端地址和目的地址是指本端和目的设备的LSR ID，可以执行 **display mpls ldp parameter**命令查看本端和目的端设备的LSR ID
- keepalive hold timer expired：keepalive保持时间超时。执行“ping -a 本端地址 -c 次数（100 以上） 目的地址”命令，检查链路状态是否正常，是否出现丢包。若出现丢包，请收集告警信息和配置信息，联系技术支持。其中，本端地址和目的地址是指本端和目的设备的LSR ID，可以执行 **display mpls ldp parameter**命令查看本端和目的端设备的LSR ID
- hello hold timer expired：Hello 保持时间超时。检查链路是否稳定，更换链路或排除链路故障，使链路稳定
- session reset：重启会话。用户手动重建会话，无需处理，等待会话重建即可
- TCP connection down：TCP连接断开。执行“ping -a 本端地址 -c 次数（100 以上）目的地址”命令，检查链路状态是否正常，是否出现丢包。若出现丢包，请收集告警信息和配置信息，联系技术支持。其中，本端地址和目的地址是指本端和目的设备的LSR ID，可以执行 **display mpls ldp parameter**命令查看本端和目的端设备的LSR ID
- received a fatal notification message ：收到致命的通知信息。需要结合告警信息，明确 Notification 消息的错误原因，再做进一步处理
- internal error：内部错误。LDP 内部错误，请收集告警信息和配置信息，联系技术支持
- memory in critical state：内存达到 critical 状态。内存进入三级告警，请收集告警信息和配置信息，联系技术支持
- transport address changed on interface：接口上的传输地址更改。请在接口视图下执行 **mpls ldp transport-address**命令来恢复接口的传输地址配置
- MD5 password changed：会话MD5 密码变化。LDP视图下执行 **display this**，查看 **md5-authentication**配置，确保会话两端配置的MD5 认证的密码相同
- Auto targeted peer deleted：自动建立的远程会话被删除。请在LDP视图下执行 **display this**，查看 **accept target-hello**命令配置：
  - 若没有 **accept target-hello**配置，则请确认配置是否被误删除
  - 若配置为 **accept target-hello prefix-list** *prefix-list-name*，则通过 **display ip prefix-list name** *prefix-list-name*，查看该IP前缀列表是否允许远程设备的LSR ID通过。若不允许，则请修改IP前缀列表配置
  - 若是其他情况，则请收集告警信息和配置信息，联系技术支持
- Modify LDP local LSR ID：修改配置引起会话down，为正常运行信息，无需处理，等待会话 UP 即可
- LDP process stopped：LDP进程终止。请执行 **display current-configuration configuration ldp**命令检查LDP配置是否存在。若存在，则表示进程异常终止，请收集告警信息和配置信息，联系技术支持。若LDP配置不存在，则请确认LDP配置是否被误删除。
  - 如下信息表示 LDP 配置存在：

```
<Sysname> display current-configuration configuration  ldp
#
```

	mpls ldp # return ○ 如下信息表示 LDP 配置不存在： <Sysname> display current-configuration configuration ldp # return

74.4 LDP_SESSION_GR

日志内容	Session ([STRING], [STRING]): ([STRING]).
日志含义	LDP会话的GR过程
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话平滑重启的状态，取值包括： • Start reconnection：启动会话重连 • Reconnection failed：会话重连失败 • Start recovery：会话重连成功，进入标签通告恢复过程 • Recovery completed：会话恢复全过程完成
日志等级	5 (Notification)
举例	LDP/5/LDP_SESSION_GR: Session (22.22.22.2:0, VPN instance: vpn1): Start reconnection.
对系统的影响	会话平滑重启状态为Reconnection failed时，基于该LDP会话的所有业务将中断；为其他状态时，无影响
日志产生原因	当已协商支持对端设备LDP平滑重启的LDP会话down时，输出该日志。日志显示会话平滑重启过程的状态变化
处理建议	从LDP_SESSION_CHG日志消息可以查看会话平滑重启的原因 当会话平滑重启状态显示为Reconnection failed时，根据会话失败原因检查接口状态、链路状态、TCP连接状态和其他相关配置（详细处理建议请参见“74.3 LDP_SESSION_CHG”），其他情况无需处理

74.5 LDP_SESSION_SP

日志内容	Session ([STRING], [STRING]): ([STRING]).
日志含义	LDP的会话保护过程
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话保护状态，取值包括： • Hold up the session：保持会话，等待 Link hello 邻接关系恢复 • Session recovered successfully：Link hello 邻接关系恢复成功 • Session recovery failed：Link hello 邻接关系恢复失败
日志等级	5 (Notification)
举例	LDP/5/LDP_SESSION_SP: Session (22.22.22.2:0, VPN instance: vpn1): Hold up the session.
对系统的影响	会话保护状态为Session recovery failed时，若会话保护持续时间到达后，仍未建立Link hello邻接关系，则基于该LDP会话的所有业务将中断；为其他状态时，无影响
日志产生原因	当会话的最后一个Link hello邻接关系丢失时，输出该日志。日志显示会话保护过程的状态变化
处理建议	当会话保护状态为Session recovery failed时，根据LDP会话失败原因检查接口状态、链路状态和其他相关配置（详细处理建议请参见“74.3 LDP_SESSION_CHG”），其他情况无需处理

75 LIPC

本节包含 LIPC（Leopard Inter-process Communication，Leopard 版本进程间通信）模块的日志消息。

75.1 LIPC_CHECK

日志内容	The quality of the link is poor. Owner=[STRING], VRF=[INTEGER], local address/port=[INTEGER]/[INTEGER], remote address/port=[INTEGER]/[INTEGER].
日志含义	LIPC链接的质量差
参数解释	$1：建立该LIPC链接的进程的名称 $2：LIPC链接所属的VPN $3：LIPC链接的四元组信息之本地节点的LIP地址 $4：LIPC链接的四元组信息之本地节点端口号 $5：LIPC链接的四元组信息之对端节点的LIP地址 $6：LIPC链接的四元组信息之对端节点端口号
日志等级	4 (Warning)
举例	LIPC/4/LIPC_CHECK: The quality of the link is poor. Owner=1, VRF=0, local address/port=0/20415, remote address/port=8/10515.
对系统的影响	会影响进程间的通信
日志产生原因	进程在需要进行内部通信时，会自动建立LIPC链接。LIPC STCP模块会自动按周期检测这些LIPC链接的质量。当LIPC链接的质量不佳，输出该日志
处理建议	系统会自动尝试修复质量不佳的LIPC链接，如果修复失败，系统会自动关闭该LIPC链接，再重新创建LIPC链接

75.2 LIPC_MTCP_CHECK

日志内容	Data stays in the receive buffer for an over long time. Owner=[STRING], VRF=[INTEGER], MDC=[INTEGER], Group=[INTEGER], MID=[INTEGER].
日志含义	数据在MTCP接收缓冲区停留时间太长未被处理
参数解释	$1：进程的名称 $2：LIPC链接所属的VPN $3：LIPC链接所属的MDC的编号 $4：LIPC链接的组播组号 $5：LIPC链接的组播组的成员ID
日志等级	4 (Warning)
举例	LIPC/4/LIPC_MTCP_CHECK: Data stays in the receive buffer for an over long time. Owner=fsd, VRF=0, MDC=1, Group=134, MID=10001.
对系统的影响	进程可能运行异常
日志产生原因	进程在需要进行内部通信时，会自动建立LIPC链接，LIPC MTCP模块会给进程分配接收缓存区。LIPC MTCP模块会自动按周期检测这些缓冲区是否有数据未被进程收走。如果进程长时间未来“接收缓存区”取数据，则表示数据有积压，进程可能运行异常
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

75.3 LIPC_STCP_CHECK

日志内容	Data stays in the receive buffer for an over long time. Owner=[STRING], VRF=[INTEGER], MDC=[INTEGER], local address/port=[INTEGER]/[INTEGER], remote address/port=[INTEGER]/[INTEGER].
日志含义	数据在STCP接收缓冲区停留时间太长未被处理
参数解释	$1：进程的名称 $2：LIPC链接所属的VPN $3：LIPC链接本地节点所属的MDC的编号 $4：LIPC链接的四元组信息之本地节点的LIP地址 $5：LIPC链接的四元组信息之本地节点端口号 $6：LIPC链接的四元组信息之对端节点的LIP地址 $7：LIPC链接的四元组信息之对端节点端口号
日志等级	4 (Warning)
举例	LIPC/4/LIPC_STCP_CHECK: Data stays in the receive buffer for an over long time. Owner=fsd, VRF=0, MDC=1, local address/port=8/10515, remote address/port=0/20415.
对系统的影响	进程可能运行异常
日志产生原因	进程在需要进行内部通信时，会自动建立LIPC链接，LIPC STCP模块会给进程分配接收缓存区。LIPC STCP模块会自动按周期检测这些缓冲区是否有数据未被进程收走。如果进程长时间未来“接收缓存区”取数据，则表示数据有积压，进程可能运行异常
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

75.4 LIPC_SUDP_CHECK

日志内容	Data stays in the receive buffer for an over long time. Owner=[STRING], VRF=[INTEGER], MDC=[INTEGER], local address/port=[INTEGER]/[INTEGER], remote address/port=[INTEGER]/[INTEGER].
日志含义	数据在SUDP接收缓冲区停留时间太长未被处理
参数解释	$1：进程的名称 $2：LIPC链接所属的VPN $3：LIPC链接所属的MDC的编号 $4：LIPC链接的四元组信息之本地节点的LIP地址 $5：LIPC链接的四元组信息之本地节点端口号 $6：LIPC链接的四元组信息之对端节点的LIP地址 $7：LIPC链接的四元组信息之对端节点端口号
日志等级	4 (Warning)
举例	LIPC/4/LIPC_SUDP_CHECK: Data stays in the receive buffer for an over long time. Owner=snmpd, VRF=0, MDC=1, local address/port=0/10525, remote address/port=32768/0.
对系统的影响	进程可能运行异常
日志产生原因	进程在需要进行内部通信时，会自动建立LIPC链接，LIPC SUDP模块会给进程分配接收缓存区。LIPC SUDP模块会自动按周期检测这些缓冲区是否有数据未被进程收走。如果进程长时间未来“接收缓存区”取数据，则表示数据有积压，进程可能运行异常
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

75.5 PORT_CHANGE

日志内容	STCP: Node where the listening port number [INTGER] (MDC: [INTGER] VRF: [INTGER]) resides changed from LIP [INTGER] to LIP [INTGER].
日志含义	STCP模块为业务模块分配的侦听端口号变更
参数解释	$1：LIPC全局端口号 $2：LIPC全局端口号所在的MDC $3：LIPC全局端口号所在的VRF $4：LIPC全局端口号侦听位置变化之前所在的节点 $5：LIPC全局端口号侦听位置变化之后所在的节点
日志等级	5 (Notification)
举例	LIPC/5/PORT_CHANGE: STCP: Node where the listening port number 620 (MDC: 1 VRF: 1) resides changed from LIP 1 to LIP 3.
对系统的影响	对系统无影响
日志产生原因	STCP模块根据业务模块的请求，为作为服务端的业务模块分配全局端口号，业务模块侦听该端口号。通常情况下，业务模块只能在申请成功的节点上侦听该端口号，如果业务模块在其他节点上同时侦听该端口号时，输出该日志。STCP会将侦听端口从原节点迁移到新侦听的节点上
处理建议	无需处理

76 LLDP

本节介绍 LLDP 模块输出的日志信息。

76.1 LLDP_CREATE_NEIGHBOR

日志内容	[STRING] agent neighbor created on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
日志含义	LLDP邻居建立
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的端口号
日志等级	6 (Informational)
举例	LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet10/0/15 (IfIndex 599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet6/0/5.
对系统的影响	对系统无影响
日志产生原因	端口收到来自新邻居的LLDP报文
处理建议	无需处理

76.2 LLDP_DELETE_NEIGHBOR

日志内容	[STRING] agent neighbor deleted on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
日志含义	LLDP邻居删除
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的接口号
日志等级	6 (Informational)
举例	LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted on port Ten-GigabitEthernet10/0/15 (IfIndex 599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet6/0/5.
对系统的影响	该LLDP邻居断开
日志产生原因	端口收到邻居删除消息
处理建议	1. 在邻居设备上查看相关配置，查看该邻居是否关闭了 LLDP 功能： o 如果是，请在邻居设备上执行 **lldp enable**命令以及 **lldp global enable** 命令，开启LLDP功能 o 如果否，请执行步骤 2 2. 执行 **display interface**命令，查看本端设备与邻居设备之间是否存在链路故障： o 如果是，请排查解决链路故障，如果无法排查链路故障，请执行步骤 3 o 如果否，请执行步骤 3 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

76.3 LLDP_LESS_THAN_NEIGHBOR_LIMIT

日志内容	The number of [STRING] agent neighbors maintained by port [STRING] (IfIndex [UINT32]) is less than [UINT32], and new neighbors can be added.
日志含义	端口下的LLDP邻居数量尚未达到上限，可以增加新邻居
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：接口可以维护的最大邻居数
日志等级	6 (Informational)
举例	LLDP/6/LLDP_LESS_THAN_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by port Ten-GigabitEthernet10/0/15 (IfIndex 599) is less than 5, and new neighbors can be added.
对系统的影响	对系统无影响
日志产生原因	端口下的邻居数量发生变化
处理建议	无需处理

76.4 LLDP_NEIGHBOR_AGE_OUT

日志内容	[STRING] agent neighbor aged out on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
日志含义	因老化时间超时导致邻居被老化
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的接口号
日志等级	5 (Notification)
举例	LLDP/5/LLDP_NEIGHBOR_AGE_OUT: Nearest bridge agent neighbor aged out on port Ten-GigabitEthernet10/0/15 (IfIndex599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet6/0/5.
对系统的影响	该LLDP邻居断开
日志产生原因	端口在一段时间内没有收到来自邻居的LLDP报文
处理建议	1. 执行 **display interface**命令，查看本端设备与邻居设备之间是否存在链路故障导致LLDP报文丢失或拥塞： ○ 如果是，请排查解决链路故障，如果无法排查链路故障，请执行步骤 2 ○ 如果否，请执行步骤 2 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

76.5 LLDP_NEIGHBOR_PROTECTION_BLOCK

日志内容	The status of port [STRING] changed to blocked ([STRING]) for the [STRING] agent.
日志含义	由于触发邻居保护，本端设备上的接口被阻塞
参数解释	$1：接口名称 $2：接口保护类型，取值包括： • aging：邻居超时保护 • validation：邻居验证保护 • black hole：LLDP 黑洞探测功能触发的保护 • cross domain：LLDP 跨域探测功能触发的保护 $3：代理类型
日志等级	4 (Warning)
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_BLOCK: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to blocked (aging) for the nearest bridge agent.
对系统的影响	该端口被阻塞，无法处理数据业务
日志产生原因	原因一： 邻居识别信息有误导致触发邻居验证保护 原因二： 长时间未收到LLDP报文，邻居老化导致触发邻居超时保护 原因三： 端口开启LLDP黑洞探测功能后，检测到LLDP报文黑洞 原因四： 端口开启LLDP跨域探测功能后，检测到与本地域ID不同的LLDP报文
处理建议	原因一： 1. 执行 **display interface**命令，查看本端设备与邻居设备之间是否存在链路故障导致LLDP报文丢失或拥塞： o 如果是，请排查解决链路故障，如果无法排查链路故障，请执行步骤 2 o 如果否，请执行步骤 2 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 原因二： 3. 执行 **display lldp neighbor-information**命令，查看来自邻居的LLDP报文信息。从显示信息中读取Chassis ID TLV和Port ID TLV信息 4. 判断来自邻居的Chassis ID TLV和Port ID TLV信息是否与本端通过 **lldp neighbor-identity chassis-id**和 **lldp neighbor-identity port-id**命令配置的识别信息相同： o 如果相同，请执行步骤 4 o 如果不同，请执行步骤 3 5. 执行 **lldp neighbor-identity chassis-id**和 **lldp neighbor-identity port-id**命令修改本端的识别信息为与LLDP邻居发送的相同 6. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 原因三： 无需处理，或修改物理拓扑以消除LLDP报文黑洞

	原因四： 检查本端和对端的LLDP跨域探测功能域ID配置规划，判断两端的域ID是否应该配置为相同值： • 如果是，请在两端设备上通过 **lldp cross-domain-detection domain-id**命令修改两端设备端口使用的域ID为相同值 • 如果否，则无需处理

76.6 LLDP_NEIGHBOR_PROTECTION_DOWN

日志内容	The status of port [STRING] changed to down (aging) for the [STRING] agent.
日志含义	由于触发邻居超时保护功能，本端设备上的接口被关闭
参数解释	$1：接口名称 $2：代理类型
日志等级	4 (Warning)
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_DOWN: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to down (aging) for the nearest bridge agent.
对系统的影响	该接口被关闭，无法处理任何业务
日志产生原因	长时间未收到LLDP报文，邻居老化导致触发邻居超时保护功能
处理建议	1. 执行 **display interface**命令，查看本端设备与邻居设备之间是否存在链路故障导致LLDP报文丢失或拥塞： o 如果是，请排查解决链路故障，如果无法排查链路故障，请执行步骤 2 o 如果否，请执行步骤 2 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

76.7 LLDP_NEIGHBOR_PROTECTION_UNBLOCK

日志内容	The status of port [STRING] changed to unblocked for the [STRING] agent.
日志含义	邻居保护状态解除，接口从阻塞状态恢复为非阻塞状态
参数解释	$1：接口名称 $2：代理类型
日志等级	4 (Warning)
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_UNBLOCK: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to unblocked for the nearest bridge agent.
对系统的影响	对系统无影响
日志产生原因	接口收到LLDP报文或邻居识别信息与本地配置的相同
处理建议	无需处理

76.8 LLDP_NEIGHBOR_PROTECTION_UP

日志内容	The status of port [STRING] changed to up for the [STRING] agent.
日志含义	邻居保护状态解除，接口从DOWN状态恢复到UP状态
参数解释	$1：接口名称 $2：代理类型
日志等级	4 (Warning)
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_UP: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to up for the nearest bridge agent.
对系统的影响	对系统无影响
日志产生原因	在邻居超时保护功能被关闭的接口上，执行**undo lldp neighbor-protection aging**命令或者**undo shutdown**命令
处理建议	无需处理

76.9 LLDP_PVID_INCONSISTENT

日志内容	PVID mismatch discovered on [STRING] (PVID [UINT32]), with [STRING] [STRING] (PVID [STRING]).
日志含义	本端设备与LLDP邻居设备之间的链路两端PVID不一致
参数解释	$1：接口名称 $2：VLAN ID $3：系统名称 $4：接口名称 $5：VLAN ID
日志等级	5 (Notification)
举例	LLDP/5/LLDP_PVID_INCONSISTENT: PVID mismatch discovered on GigabitEthernet1/0/1 (PVID 2), with H3C GigabitEthernet1/0/1 (PVID 1).
对系统的影响	链路两端的PVID不一致可能导致部分协议报文转发失败
日志产生原因	来自邻居的LLDP报文中携带的PVID TLV与本端接收LLDP报文端口的PVID不一致
处理建议	修改本端端口或邻居端口的PVID，使得两端的PVID一致

76.10 LLDP_REACH_NEIGHBOR_LIMIT

日志内容	The number of [STRING] agent neighbors maintained by the port [STRING] (IfIndex [UINT32]) has reached [UINT32], and no more neighbors can be added.
日志含义	端口下的LLDP邻居数量达到最大值
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：接口可以维护的最大邻居数
日志等级	5 (Notification)
举例	LLDP/5/LLDP_REACH_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by the port Ten-GigabitEthernet10/0/15 (IfIndex 599) has reached 5, and no more neighbors can be added.
对系统的影响	该端口无法建立新的LLDP邻居
日志产生原因	当邻居数达到最大值的端口收到新邻居的LLDP报文
处理建议	如果需要建立新的LLDP邻居，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

77 LOAD

本节介绍 LOAD 模块输出的日志信息。

77.1 BOARD_LOADING

日志内容	形式一： Board in chassis [INT32] slot [INT32] is loading software images. 形式二： Board in slot [INT32] is loading software images.
日志含义	单板启动过程中，加载启动软件包
参数解释	形式一： $1：chassis编号 $2：slot编号 形式二： $1：slot编号
日志等级	4 (Warning)
举例	形式一： LOAD/4/BOARD_LOADING: Board in chassis 1 slot 5 is loading software images. 形式二： LOAD/4/BOARD_LOADING: Board in slot 5 is loading software images.
对系统的影响	无
日志产生原因	单板启动过程中，正在加载启动软件包
处理建议	无需处理

77.2 LOAD_FAILED

日志内容	形式一： Board in chassis [INT32] slot [INT32] failed to load software images. 形式二： Board in slot [INT32] failed to load software images.
日志含义	单板在启动过程中，加载启动软件包失败
参数解释	形式一： $1：chassis编号 $2：slot编号 形式二： $1：slot编号
日志等级	3 (Error)
举例	形式一： LOAD/3/LOAD_FAILED: Board in chassis 1 slot 5 failed to load software images. 形式二： LOAD/3/LOAD_FAILED: Board in slot 5 failed to load software images.
对系统的影响	单板启动失败
日志产生原因	单板在启动过程中，加载启动软件包失败
处理建议	1. 使用 **display boot-loader**命令查看单板使用的下次启动软件包 2. 使用 **dir**命令查看启动软件包是否存在。如果不存在或者损坏，请重新获取启动软件包或者设置其它软件包作为该单板的下次启动软件包 3. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

77.3 LOAD_FINISHED

日志内容	形式一： Board in chassis [INT32] slot [INT32] has finished loading software images. 形式二： Board in slot [INT32] has finished loading software images.
日志含义	单板完成文件加载
参数解释	形式一： $1：chassis编号 $2：slot编号 形式二： $1：slot编号
日志等级	5 (Notification)
举例	形式一： LOAD/5/LOAD_FINISHED: Board in chassis 1 slot 5 has finished loading software images. 形式二： LOAD/5/LOAD_FINISHED: Board in slot 5 has finished loading software images.
对系统的影响	无
日志产生原因	单板启动过程中，从主控板加载版本完成
处理建议	无需处理

78 LOGIN

本节介绍 LOGIN（登录管理）模块输出的日志信息。

78.1 LOGIN_FAILED

日志内容	[STRING] failed to log in from [STRING].
日志含义	用户登录失败
参数解释	$1：用户名 $2：用户线名和IP地址
日志等级	5 (Notification)
举例	LOGIN/5/LOGIN_FAILED: TTY failed to log in from console0. LOGIN/5/LOGIN_FAILED: usera failed to log in from 192.168.11.22.
对系统的影响	用户无法登录系统
日志产生原因	用户登录失败
处理建议	• 检查设备与服务器的连接 • 重新输入用户名和密码 • 检查服务器上的设置（例如服务类型）是否正确 • 检查登录用户数是否已经到达上限 • 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持工程师

78.2 LOGIN_INVALID_USERNAME_PWD

日志内容	Invalid username or password from [STRING].
日志含义	用户登录时输入无效的用户名或密码
参数解释	$1：用户线名和IP地址
日志等级	5 (Notification)
举例	LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from console0. LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from 192.168.11.22.
对系统的影响	用户无法登录系统
日志产生原因	用户输入无效的用户名或密码
处理建议	检查登录用户名和密码是否正确

79 LPDT

本节介绍 LPDT 模块输出的日志信息。

79.1 LPDT_LOOPED

日志内容	A loop was detected on [STRING].
日志含义	在指定端口下检测到网络发生环路
参数解释	$1：接口名
日志等级	4 (Warning)
举例	LPDT/4/LPDT_LOOPED: A loop was detected on GigabitEthernet1/0/1.
对系统的影响	设备将根据为该端口配置的环路检测处理模式对该端口进行处理
日志产生原因	端口收到了来自本设备的环路检测报文
处理建议	1. 检查当前网络中存在的二层环路是否为网络部署需要： ○ 如果是，请执行步骤 2 ○ 如果否，请重新规划网络部署，消除二层环路 2. 检查当前环路检测功能对端口进行处理后，网络拓扑是否符合规划的预期： ○ 如果是，则无需处理 ○ 如果否，请修改设备的环路检测配置，使环路检测功能触发后网络拓扑符合需求。如果问题仍未解决，请执行步骤 3 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

79.2 LPDT_RECOVERED

日志内容	All loops were removed on [STRING].
日志含义	端口上所有VLAN的环路均消除
参数解释	$1：接口名
日志等级	5 (Notification)
举例	LPDT/5/LPDT_RECOVERED: All loops were removed on GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	原因一：在所有VLAN内，端口在三倍的环路检测时间间隔内均未收到环路检测报文 原因二：端口被关闭，环路消除
处理建议	无需处理

79.3 LPDT_VLAN_LOOPED

日志内容	A loop was detected on [STRING] in VLAN [UINT16].
日志含义	设备在端口的指定VLAN内检测到环路
参数解释	$1：接口名 $2：VLAN ID
日志等级	4 (Warning)
举例	LPDT/4/LPDT_VLAN_LOOPED: A loop was detected on GigabitEthernet1/0/1 in VLAN 1.
对系统的影响	设备将根据为该端口配置的环路检测处理模式对该端口进行处理
日志产生原因	端口在指定VLAN内收到了来自本设备的环路检测报文
处理建议	**1.** 检查当前网络中存在的二层环路是否为网络部署需要： o 如果是，请执行步骤 2 o 如果否，请重新规划网络部署，消除二层环路 **2.** 检查当前环路检测功能对端口进行处理后，网络拓扑是否符合规划的预期： o 如果是，则无需处理 o 如果否，请修改设备的环路检测配置，使环路检测功能触发后网络拓扑符合需求。如果问题仍未解决，请执行步骤 3 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

79.4 LPDT_VLAN_RECOVERED

日志内容	A loop was removed on [STRING] in VLAN [UINT16].
日志含义	端口在指定VLAN内的环路消除
参数解释	$1：接口名 $2：VLAN ID
日志等级	5 (Notification)
举例	LPDT/5/LPDT_VLAN_RECOVERED: A loop was removed on GigabitEthernet1/0/1 in VLAN 1.
对系统的影响	对系统无影响
日志产生原因	原因一：在所有VLAN内，端口在三倍的环路检测时间间隔内均未收到环路检测报文 原因二：端口被关闭，环路消除
处理建议	无需处理

79.5 LPDT_VSI_LOOPED

日志内容	A loop was detected on VSI [STRING]'s Ethernet service instance srv[UINT8] on [STRING].
日志含义	设备在VSI的AC内检测到环路
参数解释	$1：VSI名称 $2：以太网服务示例编号 $3：接口名
日志等级	4 (Warning)
举例	LPDT/4/LPDT_VSI_LOOPED: A loop was detected on VSI 1's Ethernet service instance srv1 on GigabitEthernet1/0/1.
对系统的影响	设备根据为该VSI配置的环路检测处理模式，对该AC或该AC所在端口进行处理
日志产生原因	AC收到与其属于同一VXLAN的环路检测报文
处理建议	**1.** 检查当前网络中存在的二层环路是否为网络部署需要： ○ 如果是，请执行步骤 2 ○ 如果否，请重新规划网络部署，消除二层环路 **2.** 检查当前环路检测功能对端口进行处理后，网络拓扑是否符合规划的预期： ○ 如果是，则无需处理 ○ 如果否，请修改设备的环路检测配置，使环路检测功能触发后网络拓扑符合需求。如果问题仍未解决，请执行步骤 3 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

79.6 LPDT_VSI_RECOVERED

日志内容	All loops were removed from VSI [STRING]'s Ethernet service instance srv[UINT8] on [STRING].
日志含义	AC内的环路消除
参数解释	$1：VSI名称 $2：以太网服务示例编号 $3：接口名
日志等级	5 (Notification)
举例	LPDT/5/LPDT_VSI_RECOVERED: All loops were removed from VSI 1's Ethernet service instance srv1 on GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	原因一：AC在三倍的环路检测时间间隔内均未收到环路检测报文 原因二：AC所在端口被关闭，环路消除
处理建议	无需处理

79.7 LPDT_VSI_BLOCKFAIL

日志内容	Failed to block [STRING] that hosts VSI [STRING]'s Ethernet service instance srv[UINT8] because of insufficient resources.
日志含义	触发环路检测保护动作后，阻塞AC失败
参数解释	$1：接口名 $2：VSI名称 $3：以太网服务示例编号
日志等级	5 (Notification)
举例	LPDT/5/LPDT_VSI_BLOCKFAIL: Failed to block GigabitEthernet1/0/1 that hosts VSI 1's Ethernet service instance srv1 because of insufficient resources.
对系统的影响	环路无法被消除
日志产生原因	设备阻塞AC失败
处理建议	• 手工关闭检测到环路的 AC 所在的端口 • 切换 AC 所在的 VSI 中的环路检测处理模式为 Shutdown

80 LS

本节包含本地服务器日志信息。

80.1 LOCALSVR_FAIL_TO_WRITETIME2FILE

日志内容	Failed to write the local user creation or login time records to file.
日志含义	本地用户创建或登录成功的时间记录写入文件失败
参数解释	无
日志等级	6 (Informational)
举例	LOCALSVR/6/ LOCALSVR_FAIL_TO_WRITETIME2FILE: Failed to write the local user creation or login time records to file.
对系统的影响	对系统无影响
日志产生原因	设备的本地文件系统存储空间不足
处理建议	请在用户视图下执行**dir**命令查看本地存储介质（例如flash）的剩余容量信息，如果剩余空间不足，则需要删除无用的文件

80.2 LOCALSVR_PROMPTED_CHANGE_PWD

日志内容	Please change the password of [STRING] [STRING], because [STRING].
日志含义	提醒用户修改当前密码
参数解释	$1：密码类型 ○ device management user：设备管理用户 ○ user line：用户线 ○ user line class：用户线类 $2：用户名/用户线编号/用户线类型 $3：提醒修改密码原因 ○ the current password is a weak-password：密码是弱密码 ○ the current password is the default password：密码是缺省密码 ○ it is the first login of the current user or the password had been reset：首次登录或者密码已被重置 ○ the password had expired：密码已经老化
日志等级	6 (Informational)
举例	LOCALSVR/6/LOCALSVR_PROMPTED_CHANGE_PWD: Please change the password of device management user hhh, because the current password is a weak password.
对系统的影响	对系统无影响
日志产生原因	如果用户使用不符合密码策略的密码登录设备，系统会在该用户登录后每隔24小时输出一条日志信息提醒该用户修改当前密码
处理建议	根据用户登录时采用的认证方式不同，处理建议如下： • 认证方式为 scheme 时，请修改用户的本地密码 • 认证方式为 password 时，请修改用户所在用户线/用户线类的认证密码

80.3 LS_ADD_USER_TO_GROUP

日志内容	Admin [STRING] added user [STRING] to group [STRING].
日志含义	管理员添加用户到用户组
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4 (Warning)
举例	LS/4/LS_ADD_USER_TO_GROUP: Admin admin added user user1 to group group1.
对系统的影响	对系统无影响
日志产生原因	管理员将一个本地用户添加到指定的用户组里
处理建议	系统正常运行时产生的信息，无需处理

80.4 LS_AUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed authentication. [STRING]
日志含义	用户本地认证失败
参数解释	$1：用户名 $2：IP地址 $3：失败原因 o 用户没有找到 o 密码认证失败 o 用户未上线 o 接入类型不匹配 o 绑定属性失败 o 用户在黑名单
日志等级	5 (Notification)
举例	LS/5/LS_AUTHEN_FAILURE: User cwf@system from 192.168.0.22 failed authentication. “User not found.”
对系统的影响	用户无法上线
日志产生原因	本地服务器拒绝了一个用户的认证请求，可能的原因有： • 用户没有找到 • 密码认证失败 • 用户未上线 • 接入类型不匹配 • 绑定属性失败 • 用户在黑名单
处理建议	请根据提示的错误原因处理

80.5 LS_AUTHEN_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
日志含义	用户本地认证成功
参数解释	$1：用户名 $2：IP地址
日志等级	6 (Informational)
举例	LS/6/LS_AUTHEN_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
对系统的影响	对系统无影响
日志产生原因	本地服务器接受了一个用户的认证请求
处理建议	系统正常运行时产生的信息，无需处理

80.6 LS_DEL_USER_FROM_GROUP

日志内容	Admin [STRING] delete user [STRING] from group [STRING].
日志含义	管理员将用户从用户组里删除
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4 (Warning)
举例	LS/4/LS_DEL_USER_FROM_GROUP: Admin admin delete user user1 from group group1.
对系统的影响	对系统无影响
日志产生原因	管理员将一个本地用户从指定的用户组里删除
处理建议	系统正常运行时产生的信息，无需处理

80.7 LS_PWD_ADD_BLACKLIST

日志内容	User [STRING] was added to the blacklist due to multiple login failures, [STRING].
日志含义	用户多次登录失败后被加入了黑名单
参数解释	$1：用户名 $2：结果 o 但是可以做其他的尝试 o 被永久阻塞 o 被临时阻塞指定时间（单位：分钟）
日志等级	4 (Warning)
举例	LS/4/LS_PWD_ADD_BLACKLIST: User aaa was added to the blacklist due to multiple login failures, but could make other attempts.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	用户登录认证失败后，系统会将该用户加入密码管理的黑名单，并根据**password-control login-attempt**命令配置的处理措施对其之后的登录行为进行相应的限制。当用户登录失败次数超过指定值后，系统禁止该用户登录，经过一段时间后，再允许该用户重新登录。
处理建议	1. 如果此日志偶尔出现，请检查用户的密码，有可能是用户密码输入有误导致的禁止登录，属于正常现象，建议等待一定的时间后再次尝试重新登录。如果再次使用正确的用户名和密码登录设备遇到同样的问题，请收集日志信息和配置信息，联系技术支持工程师进行处理。 2. 如果此日志频繁出现，那么可能是系统受到了登录攻击，请联系技术支持工程师进行处理

80.8 LS_PWD_CHGPWD

日志内容	The password of local [STRING] user [STRING] was modified.
日志含义	
参数解释	$1：用户接入类型 o network-access：网络接入 o device-management：设备管理 $2：用户名
日志等级	5 (Notification)
举例	LS/5/LS_PWD_CHGPWD: The password of local network-access user abc was modified.
对系统的影响	对系统无影响
日志产生原因	本地用户密码被修改
处理建议	正常情况下无需处理。设备管理员可通过查看此日志审计异常的密码修改行为

80.9 LS_PWD_CHGPWD_FOR_AGEDOUT

日志内容	User [STRING] changed the password because it was expired.
日志含义	用户由于密码已过期而修改了密码
参数解释	$1：用户名
日志等级	4 (Warning)
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEDOUT: User aaa changed the password because it was expired.
对系统的影响	对系统无影响
日志产生原因	用户由于密码已过期而修改了密码
处理建议	系统正常运行时产生的信息，无需处理

80.10 LS_PWD_CHGPWD_FOR_AGEOUT

日志内容	User [STRING] changed the password because it was about to expire.
日志含义	用户修改了即将过期的密码
参数解释	$1：用户名
日志等级	4 (Warning)
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEOUT: User aaa changed the password because it was about to expire.
对系统的影响	对系统无影响
日志产生原因	用户由于密码即将过期而修改了密码
处理建议	系统正常运行时产生的信息，无需处理

80.11 LS_PWD_CHGPWD_FOR_COMPOSITION

日志内容	User [STRING] changed the password because it had an invalid composition.
日志含义	用户由于密码组合错误而修改了密码
参数解释	$1：用户名
日志等级	4 (Warning)
举例	LS/4/LS_PWD_CHGPWD_FOR_COMPOSITION: User aaa changed the password because it had an invalid composition.
对系统的影响	对系统无影响
日志产生原因	用户由于输入的密码组合错误而重新输入了密码
处理建议	系统正常运行时产生的信息，无需处理

80.12 LS_PWD_CHGPWD_FOR_FIRSTLOGIN

日志内容	User [STRING] changed the password at the first login.
日志含义	用户首次登录时修改了密码
参数解释	$1：用户名
日志等级	4 (Warning)
举例	LS/4/LS_PWD_CHGPWD_FOR_FIRSTLOGIN: User aaa changed the password at the first login.
对系统的影响	对系统无影响
日志产生原因	用户首次登录时，因系统的安全性要求而修改了密码
处理建议	系统正常运行时产生的信息，无需处理

80.13 LS_PWD_CHGPWD_FOR_LENGTH

日志内容	User [STRING] changed the password because it was too short.
日志含义	用户因为密码太短而修改了密码
参数解释	$1：用户名
日志等级	4 (Warning)
举例	LS/4/LS_PWD_CHGPWD_FOR_LENGTH: User aaa changed the password because it was too short.
对系统的影响	对系统无影响
日志产生原因	用户因为输入的密码太短而修改了密码
处理建议	系统正常运行时产生的信息，无需处理

80.14 LS_PWD_FAILED2WRITEPASS2FILE

日志内容	Failed to write the password records to file.
日志含义	用户密码记录写文件失败
参数解释	无
日志等级	4 (Warning)
举例	LS/4/LS_PWD_FAILED2WRITEPASS2FILE: Failed to write the password records to file.
对系统的影响	无法修改本地用户密码
日志产生原因	登录期间修改自身密码，或者管理员修改本地用户密码失败，可能的原因有： • 设备的本地文件系统存储空间不足 • 本地 lauth.dat 文件异常
处理建议	1. 请在用户视图下执行 **dir**命令查看本地存储介质（例如flash）的剩余容量信息，如果剩余空间不足，则需要删除无用的文件 2. 请在用户视图下执行 **dir**命令查看本地存储介质中（例如flash）的lauth.dat文件存在情况。如果该文件不存在、大小为 0 或者很小（若小于 20B，则大概率发生了异常），请联系技术支持人员协助处理

80.15 LS_PWD_MODIFY_FAIL

日志内容	Admin [STRING] from [STRING] could not modify the password for user [STRING], because [STRING].
日志含义	管理员修改用户密码失败
参数解释	$1：管理员名 $2：IP地址 $3：用户名 $4：失败原因 ○ old password is incorrect：旧密码不正确 ○ password is too short：新密码太短 ○ password has not minimum different chars：新密码不符合包含不同字符差异的最小要求（要求最少有 4 个不同字符的差异） ○ invalid password composition：无效的密码组合（密码字符的类型和长度不符合要求） ○ password has repeated chars：密码中包含连续三个或以上的相同字符 ○ password contains username：密码中包含用户名 ○ new password must be different from any previous password by a minimum of four chars：新密码至少要与历史密码保持 4 个字符差异 ○ new password must be different from old password by a minimum of four chars：新密码至少要与旧密码保持 4 个字符差异 ○ password used already：密码已经使用（新/旧密码冲突或新密码与历史密码冲突） ○ password is in update-wait time：密码仍在等待更新的时间内 ○ entered passwords did not match：输入的确认密码与新密码不一致 ○ unknown error：其他未知错误
日志等级	4 (Warning)
举例	LS/4/LS_PWD_MODIFY_FAIL: Admin admin from 1.1.1.1 could not modify the password for user user1, because passwords do not match.
对系统的影响	对系统无影响
日志产生原因	可能的原因有： • 旧密码不正确 • 密码太短 • 不同字符的个数不足 4 个 • 无效的密码组合 • 包含连续三个或以上的相同字符 • 包含了用户名 • 与历史密码没有保持至少 4 个字符的差异 • 与旧密码没有保持至少 4 个字符的差异 • 与当前或历史密码重复 • 没有达到更新间隔时间 • 输入的确认密码错误

处理建议	请根据提示的错误原因处理

80.16 LS_PWD_MODIFY_SUCCESS

日志内容	Admin [STRING] from [STRING] modify the password for user [STRING] successfully.
日志含义	管理员成功修改了用户密码
参数解释	$1：管理员名 $2：IP地址 $3：用户名
日志等级	6 (Informational)
举例	LS/6/LS_PWD_MODIFY_SUCCESS: Admin admin from 1.1.1.1 modify the password for user abc successfully.
对系统的影响	对系统无影响
日志产生原因	管理员成功修改了用户密码
处理建议	系统正常运行时产生的信息，无需处理

80.17 LS_REAUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed reauthentication.
日志含义	用户旧密码校验失败
参数解释	$1：用户名 $2：IP地址
日志等级	5 (Notification)
举例	LS/5/LS_REAUTHEN_FAILURE: User abcd from 1.1.1.1 failed reauthentication.
对系统的影响	因输入的旧密码不正确，用户修改自身密码失败
日志产生原因	用户登录期间修改自身密码或登录成功后通过命令行修改自身密码时，系统会要求用户首先输入旧密码，如果旧密码校验失败，系统会输出此日志信息
处理建议	检查本地用户的旧密码，如果旧密码正确请联系技术支持人员协助处理

80.18 LS_UPDATE_PASSWORD_FAIL

日志内容	Failed to update the password for user [STRING].
日志含义	修改用户密码失败
参数解释	$1：用户名
日志等级	4 (Warning)
举例	LS/4/LS_UPDATE_PASSWORD_FAIL: Failed to update the password for user abc.
对系统的影响	无法修改本地用户密码
日志产生原因	通过命令行新增、修改、删除本地用户密码失败，可能的原因有： • 密码不符合安全性要求，例如：密码太短或与当前或历史密码重复 • 设备的本地文件系统存储空间不足 • 本地 lauth.dat 文件异常
处理建议	1. 根据修改密码时系统的提示信息重新设置符合安全性要求的密码 2. 请在用户视图下执行 **dir**命令查看本地存储介质（例如flash）的剩余容量信息，如果剩余空间不足，则需要删除无用的文件 3. 请在用户视图下执行 **dir**命令查看本地存储介质中（例如flash）的lauth.dat文件存在情况。如果该文件不存在、大小为 0 或者很小（若小于 20B，则大概率发生了异常），请联系技术支持人员协助处理

80.19 LS_USER_CANCEL

日志内容	User [STRING] from [STRING] cancelled inputting the password.
日志含义	用户取消输入密码
参数解释	$1：用户名 $2：IP地址
日志等级	5 (Notification)
举例	LS/5/LS_USER_CANCEL: User 1 from 1.1.1.1 cancelled inputting the password.
对系统的影响	对系统无影响
日志产生原因	用户取消输入密码或者没有在90秒内输入密码
处理建议	系统正常运行时产生的信息，无需处理

80.20 LS_USER_PASSWORD_EXPIRE

日志内容	User [STRING]'s login idle timer timed out.
日志含义	用户登录空闲时间超时
参数解释	$1：用户名
日志等级	5 (Notification)
举例	LS/5/LS_USER_PASSWORD_EXPIRE: User 1's login idle timer timed out.
对系统的影响	对系统无影响
日志产生原因	本地用户登录后连续闲置的时长超过空闲超时时间
处理建议	系统正常运行时产生的信息，无需处理

80.21 LS_USER_ROLE_CHANGE

日志内容	Admin [STRING] [STRING] user role [STRING] for [STRING].
日志含义	管理员修改了用户的用户角色
参数解释	$1：管理员名 $2：添加/删除 $3：用户角色 $4：用户名
日志等级	4 (Warning)
举例	LS/4/LS_USER_ROLE_CHANGE: Admin admin added user role network-admin for user abcd.
对系统的影响	对系统无影响
日志产生原因	管理员修改了本地用户的用户角色
处理建议	系统正常运行时产生的信息，无需处理

81 LSM

本节介绍 LSM 模块输出的日志信息。

81.1 LSM_SR_LABEL_CONFLICT

日志内容	Protocol [STRING] assigned label([STRING]) to prefix([STRING]), which already has label([STRING]) assigned by protocol [STRING].
日志含义	SR标签冲突
参数解释	$1：路由协议1 $2：标签值1 $3：前缀地址及掩码 $4：标签值2 $3：路由协议2
日志等级	4 (Warning)
举例	LSM/4/LSM_SR_LABEL_CONFLICT: Protocol ISIS assigned label(16000) to prefix(5.5.5.5/32), which already has label(17000) assigned by protocol OSPF.
对系统的影响	对系统无影响
日志产生原因	在同一SR节点上不同路由协议为同一前缀地址分配不同的标签
处理建议	请确认是否需要为同一前缀在不同协议分配不同的标签。如果不需要，则建议调整配置

81.2 LSM_SR_PREFIX_CONFLICT

日志内容	The label([STRING]) for prefix([STRING]) has been used by prefix([STRING]).
日志含义	前缀地址标签分配冲突
参数解释	$1：标签值 $2：前缀地址1及掩码 $3：前缀地址2及掩码
日志等级	4 (Warning)
举例	LSM/4/LSM_SR_PREFIX_CONFLICT: The label(16700) for prefix(8.8.8.8/32) has been used by prefix(5.5.5.5/32).
对系统的影响	设备只会为存在标签冲突的前缀创建一条ILM表项，可能会导致部分流量转发错误
日志产生原因	同一个标签被分配给两个不同的前缀地址
处理建议	调整SR标签配置，避免出现标签分配冲突的情况

82 LSPV

本节介绍 LSP 验证模块输出的日志信息。

82.1 LSPV_PING_STATIS_INFO

日志内容	Ping statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packets loss, round-trip min/avg/max = [UINT32]/[UINT32]/[UINT32] ms.
日志含义	LSP ping的统计信息
参数解释	$1：FEC $2：发出的请求数 $3：收到的应答数 $4：未收到应答的次数占发送请求总数的比例 $5：最小往返延迟时间 $6：平均往返延迟时间 $7：最大往返延迟时间
日志等级	6 (Informational)
举例	LSPV/6/LSPV_PING_STATIS_INFO: Ping statistics for FEC 192.168.1.1/32: 5 packets transmitted, 5 packets received, 0.0% packets loss, round-trip min/avg/max = 1/2/5 ms.
对系统的影响	对系统无影响
日志产生原因	执行**ping mpls**命令，触发该日志。日志显示ping的统计信息
处理建议	如果没有收到应答报文，则说明LSP隧道或者PW出现故障，需检查网络状况、LSP或PW的相关配置，解决LSP隧道或PW连通性故障问题 如果是LSP故障，则需进行以下处理： 4. 执行 **display ip routing-table**命令，查看是否存在到达目的节点的Loopback接口地址的网段路由。如果不存在，则在Loopback接口和公网接口下使能IGP协议，确保发布对应网段路由 5. 检查路由是否迭代到LSP隧道或存在MPLS标签。执行 **display fib**命令，查看指定前缀的FIB表项。检查该FIB表项是否存在LSP索引号（Token字段）或标签值（Label字段）。如果存在，则继续执行下一步。如果不存在，则表示路由不是FTN表项，需执行 **display mpls lsp**命令，查看是否存在到达路由目的地址的LSP。如果不存在，则确保建立指定类型的LSP： o 对于 LDP LSP，请在接口下使能 MPLS 功能和 MPLS LDP 功能 o 对于SRLSP，请在IS-IS IPv4 单播地址族视图、OSPF视图或BGP IPv4 单播地址族视图下执行 **segment-routing mpls**命令用来开启基于MPLS的SR功能 6. 执行 **display cpu-usage**命令，查看CPU利用率的统计信息 o 如果 CPU 利用率过高，则关闭一些不必要的功能，降低设备 CPU 利用率 o 如果 CPU 利用率正常，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 如果是PW故障，则需要进一步根据**ping mpls pw**命令的回显信息分析和定位故障： • 回显信息为 Unknown PW 时，表示检测的 PW 不存在，需要修改 PW 相关配置，以创建 PW • 回显信息为No suitable control channel for the PW时，表示PW的VCCV控制通道类型配置错误，需要通过 **vccv cc**命令修改PW模板中VCCV控制通道类型 • 回显信息为Please configure pseudowire control-word for control channel时，表示PW引用的PW模板中未开启控制字功能，需要通过 **control-word enable**命令在PW模板下开启控制字功能 • 回显信息为 Request time out 时，请先检查本端 PW 是否 Up，再逐步排查 PW 经过的节点是否存在故障，解决故障节点的网络连接问题

	如果根据回显信息无法解决PW故障，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83 MAC

本节介绍 MAC 模块输出的日志信息。

83.1 MAC_DRIVER_ADD_ENTRY

日志内容	Driver failed to add MAC address entry: MAC address=[STRING], VLAN=[UINT32], State=[UINT32], interface=[STRING].
日志含义	驱动下发MAC地址表项失败
参数解释	$1：MAC地址 $2：VLAN ID $3：表项类型编号 $4：端口名称
日志等级	4 (Warning)
举例	MAC/4/MAC_DRIVER_ADD_ENTRY: Driver failed to add MAC address entry: MAC address=1-1-1, VLAN=1, State=2, interface=GigabitEthernet1/0/1.
对系统的影响	设备无法生成指定的MAC地址表项
日志产生原因	驱动下发MAC地址表项失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.2 MAC_NOTIFICATION

日志内容	形式一： MAC address [STRING] in VLAN [UNIT32] has moved from port [STRING] to port [STRING] for [UNIT32] times. 形式二： MAC address [STRING] in VSI [STRING] has moved from [STRING] service-instance [UNIT32] to [STRING] service-instance [UNIT32] for [UNIT32] times.
日志含义	形式一： MAC地址在端口之间迁移 形式二： MAC地址在以太网服务实例之间迁移
参数解释	形式一： $1： MAC地址 $2：VLAN ID $3：接口名称 $4：接口名称 $5：MAC地址的迁移次数 形式二： $1：MAC地址 $2：VSI名称 $3：接口名称 $4：以太网服务实例的ID $5：接口名称 $6：以太网服务实例的ID $7：MAC地址的迁移次数
日志等级	4 (Warning)
举例	形式一： MAC/4/MAC_NOTIFICATION: MAC address 0000-0012-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times 形式二： MAC/4/MAC_NOTIFICATION: MAC address 0010-9400-0002 in VSI vpna has moved from Twenty-FiveGigE1/0/1 service-instance 40 to Twenty-FiveGigE1/0/3 service-instance 30 for 152499 times.
对系统的影响	如果MAC地址迁移频繁出现，网络中可能存在二层环路导致广播风暴
日志产生原因	原因一：网络中存在二层环路 原因二：网络中存在恶意攻击
处理建议	原因一： 通过正确部署物理网络拓扑消除环路，或部署环网协议（生成树、环路保护、RRPP、ERPS等）进行规避 原因二： 7. 通过 **mac-address mac-learning priority**命令配置接口的MAC地址学习优先级，或通过 **mac-address notification mac-move suppression**命令配置MAC地址迁移抑制功能，以避免恶意攻击造成的影响。如果仍然频繁发生MAC地

	址迁移，请执行步骤 2 **8.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.3 MAC_PROTOCOLPKT_NORES_GLOBAL

日志内容	The card does not have enough hardware resources to send protocol packets destined for [STRING] to the CPU for [STRING],
日志含义	单板硬件资源不足，导致匹配目的MAC地址的报文上送CPU处理失败
参数解释	$1：MAC地址 $2：协议类型
日志等级	5 (Notification)
举例	MAC/5/MAC_PROTOCOLPKT_NORES_GLOBAL: The card does not have enough hardware resources to send protocol packets destined for 0180-C200-000e to the CPU for LLDP.
对系统的影响	该报文无法转发
日志产生原因	单板硬件资源不足
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.4 MAC_PROTOCOLPKT_NORES_PORT

日志内容	The card does not have enough hardware resources to send protocol packets destined for [STRING] to the CPU for [STRING] on [STRING].
日志含义	单板硬件资源不足，导致协议报文上送CPU处理失败
参数解释	$1：MAC地址 $2：协议类型 $3：接口名称
日志等级	5 (Notification)
举例	MAC/5/MAC_PROTOCOLPKT_NORES_PORT: The card does not have enough hardware resources to send protocol packets destined for 0180-C200-000e to the CPU for LLDP on GigabitEthernet2/0/32.
对系统的影响	该协议报文无法转发
日志产生原因	单板硬件资源不足
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.5 MAC_PROTOCOLPKT_NORES_VLAN

日志内容	The card does not have enough hardware resources to send protocol packets destined for [STRING] to the CPU for [STRING] in VLAN [UINT16].
日志含义	单板硬件资源不足，导致VLAN内的报文上送CPU处理失败
参数解释	$1：MAC地址 $3：协议类型 $3：VLAN ID
日志等级	5 (Notification)
举例	MAC/5/MAC_PROTOCOLPKT_NORES_VLAN: The card does not have enough hardware resources to send protocol packets destined for 0180-C200-000e to the CPU for LLDP in VLAN 100.
对系统的影响	该VLAN内的报文无法转发
日志产生原因	单板硬件资源不足
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.6 MAC_TABLE_FULL_GLOBAL

日志内容	The number of MAC address entries reached the maximum number [UINT32].
日志含义	全局MAC地址表项的数量达到了允许的最大数量
参数解释	$1：最大MAC地址数量
日志等级	4 (Warning)
举例	MAC/4/MAC_TABLE_FULL_GLOBAL: The number of MAC address entries reached the maximum number 1024.
对系统的影响	设备无法学习新的MAC地址表项
日志产生原因	全局MAC地址表中的表项数量超过了允许的最大数量
处理建议	1. 执行 **display mac-address**命令，查看当前所有的MAC地址表项 2. 在系统视图下或接口视图下执行 **undo mac-address**命令，删除不需要的MAC地址表项

83.7 MAC_TABLE_FULL_PORT

日志内容	The number of MAC address entries reached the maximum number [UINT32] for interface [STRING].
日志含义	接口的MAC地址表项数量达到了为其配置的最大数量
参数解释	$1：最大MAC地址数量 $2：接口名称
日志等级	4 (Warning)
举例	MAC/4/MAC_TABLE_FULL_PORT: The number of MAC address entries reached the maximum number 1024 for interface GigabitEthernet2/0/32.
对系统的影响	该接口无法学习新的MAC地址表项
日志产生原因	接口的MAC地址表项数量达到了为其配置的最大数量
处理建议	执行**display mac-address interface** *interface-type interface-number*命令，查看达到最大数量的接口下的MAC地址表项是否均为需要的MAC地址表项： • 如果是，请在该接口视图下执行**mac-address max-mac-count**命令增大MAC地址学习上限 • 如果否，请在该接口视图下执行**undo mac-address**命令，删除不需要的MAC地址表项

83.8 MAC_TABLE_FULL_VLAN

日志内容	The number of MAC address entries reached the maximum number [UINT32] in VLAN [UINT32].
日志含义	VLAN的MAC地址表项数量达到了为其配置的最大数量
参数解释	$1：最大MAC地址数量 $2：VLAN ID
日志等级	4 (Warning)
举例	MAC/4/MAC_TABLE_FULL_VLAN: The number of MAC address entries reached the maximum number 1024 in VLAN 2.
对系统的影响	该VLAN无法学习新的MAC地址表项
日志产生原因	VLAN的MAC地址表项数量达到了为其配置的最大数量
处理建议	执行**display mac-address interface vlan** *vlan-id*命令，查看达到最大数量的VLAN内的MAC地址表项是否均为需要的MAC地址表项： • 如果是，请在该VLAN视图下执行**mac-address max-mac-count**命令增大MAC地址学习上限 • 如果否，请在该VLAN视图下执行**undo mac-address**命令，删除不需要的MAC地址表项

83.9 MAC_TABLE_FULL_VSI

日志内容	The number of MAC address entries reached the maximum number [UINT32] in VSI [UINT32].
日志含义	VSI内的MAC地址表项数量达到了为其配置的允许学习的最大数量
参数解释	$1：最大MAC地址表项数量 $2：VSI索引号
日志等级	4 (Warning)
举例	MAC/4/MAC_TABLE_FULL_VSI: The number of MAC address entries reached the maximum number 1024 in VSI 2.
对系统的影响	该VSI无法学习新的MAC地址表项
日志产生原因	VSI内的MAC地址表项数量达到了为其配置的允许学习的最大数量
处理建议	1. 执行 **display l2vpn mac-address**s命令，查看当前已学习到的MAC地址表项是否能够满足使用需求： ○ 如果是，请执行步骤 3 ○ 如果否，请执行步骤 2 2. 执行 **mac-table limit**命令，增加VSI允许学习的MAC地址表项最大数量 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.10 MAC_VLAN_LEARNLIMIT_NORESOURCE

日志内容	The card does not have enough hardware resources to set MAC learning limit for VLAN [UINT16].
日志含义	由于单板硬件资源不足，配置VLAN内允许学习的最大MAC地址数量失败
参数解释	$1：VLAN ID
日志等级	5 (Notification)
举例	MAC/5/MAC_VLAN_LEARNLIMIT_NORESOURCE: The card does not have enough hardware resources to set MAC learning limit for VLAN 100.
对系统的影响	无法配置VLAN内允许学习的最大MAC地址数量
日志产生原因	单板硬件资源不足
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

83.11 MAC_VLAN_LEARNLIMIT_NOTSUPPORT

日志内容	The card does not support setting MAC learning limit for VLAN [UINT16].
日志含义	由于单板不支持，配置VLAN内允许学习的最大MAC地址数量失败
参数解释	$1：VLAN ID
日志等级	5 (Notification)
举例	MAC/5/ MAC_VLAN_LEARNLIMIT_NOTSUPPORT: The card does not support setting MAC learning limit for VLAN 100.
对系统的影响	无法配置VLAN内允许学习的最大MAC地址数量
日志产生原因	单板不支持配置该功能
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

84 MACA

本节介绍 MAC 地址认证模块输出的日志信息。

84.1 MACA_ENABLE_NOT_EFFECTIVE

日志内容	MAC authentication is enabled but is not effective on interface [STRING].
日志含义	MAC地址认证功能在接口上不生效，因为该接口不支持MAC地址认证
参数解释	$1：接口名
日志等级	3 (Error)
举例	MACA/3/MACA_ENABLE_NOT_EFFECTIVE: MAC authentication is enabled but is not effective on interface Ethernet3/1/2.
对系统的影响	MAC地址认证功能在接口上不生效
日志产生原因	在不支持MAC地址认证的接口上配置MAC地址认证功能
处理建议	请关闭该接口上的MAC地址认证功能，在支持MAC地址认证的接口上配置该功能

84.2 MACA_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UserNameFormat=[STRING]; User failed MAC authentication. Reason: [STRING].
日志含义	MAC地址认证用户认证失败
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式 $6：失败原因 • MAC address authorization failed：授权 MAC 地址失败 • VLAN authorization failed：授权 VLAN 失败 • VSI authorization failed：授权 VSI 失败 • ACL authorization failed：授权 ACL 失败 • User profile authorization failed：授权 User Profile 失败 • URL authorization failed：授权 URL 失败 • Microsegment authorization failed：授权微分段失败 • Authentication process failed：认证失败 • VSI authorization failed because of insufficient resources：资源不足，授权 VSI 失败 • ACL authorization failed because of insufficient resources：资源不足，授权 ACL 失败 • MAC address authorization failed after a MAC move：MAC 迁移后授权 MAC 失败 • VLAN authorization failed because of failure in authorization VLAN selection：选择授权 VLAN 失败 • VLAN authorization failed because a free VLAN was assigned as the authorization VLAN：授权 VLAN 为 free VLAN，授权失败 • VLAN authorization failed because of failure in authorization VLAN creation：创建授权 VLAN 失败 • VSI authorization failed because the user belongs to a free VLAN：用户加入了 free vlan，授权 VSI 失败 • VSI authorization failed because the user's access interface does not permit the user VLAN ：接口不允许用户 VLAN 通过，授权 VSI 失败 • VSI authorization failed because of failure in AC creation：创建 AC 失败，授权 VSI 失败 • ACL authorization failed because the specified ACL does not exist ：ACL 不存在，授权 ACL 失败 • ACL authorization failed because of unsupported ACL type：ACL 类型不支持，授权 ACL 失败 • ACL authorization failed because the specified ACL conflicts with other ACLs on the user's access interface：ACL 与所在接口其他 ACL 冲突，授权 ACL 失败 • ACL authorization failed because no rule was obtained for the specified ACL：无法获取任何 ACL 规则，授权 ACL 失败 • ACL authorization failed because of ACL parameter error：ACL 的相关参数出错，授权 ACL 失败

	• User profile authorization failed because an invalid user profile was assigned to the user (the authorization-fail offline feature is enabled)：配置了授权失败下线功能，User Profile 非法 • User profile authorization failed because of failure in issuing the specified user profile to driver：下驱动失败 • URL authorization failed because of insufficient resources：资源不足，授权 URL 失败 • URL authorization failed because of invalid parameter in the specified URL：URL 参数错误，授权 URL 失败 • URL authorization failed because the specified URL was not supported：不支持 URL，授权 URL 失败 • URL authorization failed because of deny rule issuing failure：下发 deny 规则失败，授权 URL 失败 • URL authorization failed because of failure in issuing the specified URL to driver：下驱动失败，授权 URL 失败 • URL authorization failed because no servers were reachable and the url-user-logoff parameter was specified：配置 Critical microsegment、Critical VSI 时指定了 url-user-logoff 参数，服务器不可达时，授权 URL 失败 • URL authorization failed because the escape critical VSI feature of port security was configured：配置了端口安全逃生到 Critical VSI 功能，授权 URL 失败
日志等级	6 (Informational)
举例	MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0000-0001-VLANID=1-Username=0000-0000-0001-UsernameFormat=MAC address; User failed MAC authentication. Reason: VLAN authorization failed.
对系统的影响	MAC地址认证用户无法上线
日志产生原因	参见本日志打印的失败原因
处理建议	**1.** 请确认设备间链路连接正常 **2.** 请确认 MAC 地址认证相关配置正确 **3.** 请根据打印的认证失败原因定位问题。如果是设备或认证服务器上配置错误，请及时修改设备或服务器配置 **4.** 如果问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

84.3 MACA_LOGIN_FAILURE (EAD)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User failed MAC authentication. Reason: [STRING]. Can't trigger MAC authentication for the user before the EAD user entry ages out.
日志含义	用户MAC地址认证失败，在EAD表项老化之前，用户无法再次触发MAC地址认证
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式 $6：失败原因 • MAC address authorization failed：授权 MAC 地址失败 • VLAN authorization failed：授权 VLAN 失败 • VSI authorization failed：授权 VSI 失败 • ACL authorization failed：授权 ACL 失败 • User profile authorization failed：授权 User Profile 失败 • URL authorization failed：授权 URL 失败 • Authentication process failed：认证失败
日志等级	6 (Informational)
举例	MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0000-0001-VLANID=1-Username=0000-0000-0001-UsernameFormat=MAC address; User failed MAC authentication. Reason: VLAN authorization failed. Can't trigger MAC authentication for the user before the EAD user entry ages out.
对系统的影响	MAC地址认证用户无法上线
日志产生原因	参见本日志打印的失败原因
处理建议	1. 请根据打印的认证失败原因定位问题。如果是设备或认证服务器上配置错误，请及时修改设备或服务器配置 2. 如果无需使用 EAD 快速部署功能，请关闭 EAD 快速部署功能或删除当前接口上的 802.1X 配置 3. 如果问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

84.4 MACA_LOGIN_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANID=[STRING]-AuthorizationVLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User passed MAC authentication and came online.
日志含义	MAC地址认证用户认证成功上线
参数解释	$1：接口名 $2：MAC地址 $3：接入VLAN ID $4：授权VLAN ID $5：用户名 $6：用户名格式
日志等级	6 (Informational)
举例	MACA/6/MACA_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-AccessVLANID=444-AuthorizationVLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; User passed MAC authentication and came online.
对系统的影响	MAC地址认证用户上线
日志产生原因	当MAC地址认证用户认证成功上线时，系统生成此日志
处理建议	无需处理

84.5 MACA_LOGIN_SUCC (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; The user that failed MAC authentication passed open authentication and came online.
日志含义	用户MAC地址认证失败但通过开放认证模式认证成功并上线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式
日志等级	6 (Informational)
举例	MACA/6/MACA_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; The user that failed MAC authentication passed open authentication and came online.
对系统的影响	MAC地址认证用户上线
日志产生原因	当用户MAC地址认证失败但通过开放认证模式成功上线时，系统生成此日志
处理建议	无需处理

84.6 MACA_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; MAC authentication user was logged off.
日志含义	MAC地址认证用户下线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式
日志等级	6 (Informational)
举例	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; MAC authentication user was logged off.
对系统的影响	MAC地址认证用户下线
日志产生原因	MAC地址认证用户下线的常见原因包括： • MAC 地址认证用户主动下线 • 同一 MAC 地址的用户采用 802.1X 认证重新上线 • 设备上 MAC 地址认证的相关配置发生变化 • MAC 地址认证用户流量实时计费失败 • MAC 地址认证用户重认证失败 • 服务器强制用户下线 • 开启下线检测后用户下线 • 用户会话超时
处理建议	**1.** 如果用户为正常下线，则无需处理 **2.** 如果用户为异常下线： a. 请确保设备与服务器之间链路正常。如果链路异常，则请恢复链路 b. 请检查用户是否通过 802.1X上线。通过 **display dot1x connection**命令查看当前MAC地址是否通过 802.1X认证成功上线。如果通过 802.1X认证在线，若需要保持MAC地址认证用户身份，则请将相应的 802.1X用户下线并关闭 802.1X认证功能，然后再尝试进行MAC地址认证 c. 请确认设备及服务器上 MAC 地址认证相关配置是否发生变化（如全局或接口 MAC 地址认证功能均开启、服务器与设备认证方式一致、认证域配置等） **3.** 如果问题无法定位及解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

84.7 MACA_LOGOFF (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; MAC authentication open user was logged off.
日志含义	MAC地址认证open用户下线
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式
日志等级	6 (Informational)
举例	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; MAC authentication open user was logged off.
对系统的影响	MAC地址认证open用户下线
日志产生原因	MAC地址认证用户下线的常见原因包括： • MAC 地址认证用户主动下线 • 同一 MAC 地址的用户采用 802.1X 认证重新上线 • 设备上 MAC 地址认证的相关配置发生变化 • MAC 地址认证用户流量实时计费失败 • MAC 地址认证用户重认证失败 • 服务器强制用户下线 • 开启下线检测后用户下线 • 用户会话超时
处理建议	1. 如果用户为正常下线，则无需处理 2. 如果用户为异常下线： a. 请确保设备与服务器之间链路正常。如果链路异常，则请恢复链路 b. 请检查用户是否通过 802.1X上线。通过 **display dot1x connection**命令查看当前MAC地址是否通过 802.1X认证成功上线。如果通过 802.1X认证在线，若需要保持MAC地址认证用户身份，则请将相应的 802.1X用户下线并关闭 802.1X认证功能，然后再尝试进行MAC地址认证 c. 请确认设备及服务器上 MAC 地址认证相关配置是否发生变化（如全局或接口 MAC 地址认证功能均开启、服务器与设备认证方式一致、认证域配置等） 3. 如果问题无法定位及解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

85 MACSEC

本节介绍 MAC Security 模块输出的日志信息。

85.1 MACSEC_MKA_KEEPALIVE_TIMEOUT

日志内容	The live peer with SCI [STRING] and CKN [STRING] aged out on interface [STRING].
日志含义	与对端的MKA安全会话超时
参数解释	$1：SCI $2：CKN $3：接口名
日志等级	4 (Warning)
举例	MACSEC/4/MACSEC_MKA_KEEPALIVE_TIMEOUT: The live peer with SCI 00E00100000A0006 and CKN 80A0EA0CB03D aged out on interface GigabitEthernet1/0/1.
对系统的影响	两端参与者间未建立MKA安全会话，接口不能正常转发报文
日志产生原因	本端参与者和对端参与者相互学习到后，本端参与者为对端参与者启动一个保活定时器。如果本端参与者在保活定时器超时的时间内没有收到对端参与者的MKA报文，则将对端参与者的信息从本端删除掉，并触发该日志
处理建议	1. 在两端设备任意视图下执行 **display interface**命令查看配置了 MACsec功能的接口状态： o 如果接口链路状态异常，请恢复接口链路连接。若链路恢复后，会话仍异常，则请执行步骤 2 o 如果接口链路状态正常，则请执行步骤 2 2. 如果问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

85.2 MACSEC_MKA_PRINCIPAL_ACTOR

日志内容	The actor with CKN [STRING] became principal actor on interface [STRING].
日志含义	某个行动者被选举为主要行动者
参数解释	$1：CKN $2：接口名
日志等级	6 (Informational)
举例	MACSEC/6/MACSEC_MKA_PRINCIPAL_ACTOR: The actor with CKN 80A0EA0CB03D became principal actor on interface GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	接口上可能存在多个行动者，具有最高优先级的Key Server的行动者被选举为主要行动者，触发该日志
处理建议	无需处理

85.3 MACSEC_MKA_SAK_REFRESH

日志内容	The SAK has been refreshed on interface [STRING].
日志含义	接口上的SAK密钥更新
参数解释	$1：接口名
日志等级	6 (Informational)
举例	MACSEC/6/MACSEC_MKA_SAK_REFRESH: The SAK has been refreshed on interface GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	接口上的参与者派生出或接收到新的SAK时，触发该日志
处理建议	无需处理

85.4 MACSEC_MKA_SESSION_ESTABLISHED

日志内容	The MKA session has been established on interface [STRING].
日志含义	MKA会话成功建立
参数解释	$1：接口名
日志等级	5 (Notification)
举例	MACSEC/5/MACSEC_MKA_SESSION_ESTABLISHED: The MKA session has been established on interface GigabitEthernet1/0/1.
对系统的影响	两端设备将进行MACsec安全会话
日志产生原因	开启MACsec维护模式后，MKA会话成功建立
处理建议	无需处理

85.5 MACSEC_MKA_SESSION_REAUTH

日志内容	The MKA session with CKN [STRING] was re-authenticated on interface [STRING].
日志含义	接口上某MKA会话进行了重认证
参数解释	$1：CKN $2：接口名
日志等级	6 (Informational)
举例	MACSEC/6/MACSEC_MKA_SESSION_REAUTH: The MKA session with CKN 80A0EA0CB03D was re-authenticated on interface GigabitEthernet1/0/1.
对系统的影响	重认证过程中，MKA会话短暂断开，参与者接收到新的CAK，并使用它重新建立MKA会话
日志产生原因	客户端进行802.1X重认证时，触发该日志
处理建议	无需处理

85.6 MACSEC_MKA_SESSION_SECURED

日志内容	The MKA session with CKN [STRING] was secured on interface [STRING].
日志含义	接口上的MKA会话采用密文通信方式
参数解释	$1：CKN $2：接口名
日志等级	6 (Informational)
举例	MACSEC/6/MACSEC_MKA_SESSION_SECURED: The MKA session with CKN 80A020EA0CB03D was secured on interface GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	触发该日志的原因可能包括： • MKA 会话由明文通信切换为密文通信 • Key Server 和它对端的接口都支持 MACsec 功能，且两端至少有一个期望 MACsec 保护的情况下，两端协商出新的会话
处理建议	无需处理

85.7 MACSEC_MKA_SESSION_START

日志内容	The MKA session with CKN [STRING] started on interface [STRING].
日志含义	MKA会话协商开始
参数解释	$1：CKN $2：接口名
日志等级	6 (Informational)
举例	MACSEC/6/MACSEC_MKA_SESSION_START: The MKA session with CKN 80A020EA0CB03D started on interface GigabitEthernet1/0/1.
对系统的影响	MKA会话协商成功后，将建立MKA安全会话，两端参与者间采用加密通信
日志产生原因	触发该日志的原因可能包括： • 使能 MKA 功能后，有新的可用 CAK • 用户重建 MKA 会话 • 协商会话失败的接口收到新的 MKA 报文
处理建议	无需处理

85.8 MACSEC_MKA_SESSION_STOP

日志内容	The MKA session with CKN [STRING] stopped on interface [STRING].
日志含义	MKA会话终止
参数解释	$1：CKN $2：接口名
日志等级	5 (Notification)
举例	MACSEC/5/MACSEC_MKA_SESSION_STOP: The MKA session with CKN 80A020EA0CB03D stopped on interface GigabitEthernet1/0/1.
对系统的影响	两端参与者不再通过该MKA安全会话进行安全通信
日志产生原因	触发该日志的原因可能包括： • 用户删除或重建了接口的 MKA 会话 • MKA 会话所在链路故障
处理建议	1. 如果用户未删除会话，则请使用 **display mka session**命令查看会话是否存在： o 如果会话重建且已存在，则无需处理 o 如果会话不存在，则执行步骤 2 2. 在两端设备任意视图下执行 **display interface**命令查看配置了 MACsec功能的接口状态： o 如果接口链路状态异常，请恢复接口链路连接。链路正常后，若会话仍异常，则请执行步骤 3 o 如果接口链路状态正常，则请执行步骤 3 3. 请收集告警信息、日志信息和配置信息，并联系技术支持工程师

85.9 MACSEC_MKA_SESSION_UNESTABLISHED

日志内容	Interface [STRING] has not been blocked even though the MKA session has not been established.
日志含义	MACsec安全会话未建立，但端口处于unblock状态
参数解释	$1：接口名
日志等级	5 (Notification)
举例	MACSEC/5/MACSEC_MKA_SESSION_UNESTABLISHED: Interface GigabitEthernet1/0/1 has not been blocked even though the MKA session has not been established.
对系统的影响	
日志产生原因	开启MACsec维护模式后，端口处于unblock状态，对端配置不正确导致MKA会话始终未建立，则每隔30秒输出此日志
处理建议	• 请检查对端设备上 MACaec 相关配置是否正确 • 如果问题无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师

85.10 MACSEC_MKA_SESSION_UNSECURED

日志内容	The MKA session with CKN [STRING] was not secured on interface [STRING].
日志含义	接口上的MKA会话采用明文通信方式
参数解释	$1：CKN $2：接口名
日志等级	5 (Notification)
举例	MACSEC/5/MACSEC_MKA_SESSION_UNSECURED: The MKA session with CKN 80A020EA0CB03D was not secured on interface GigabitEthernet1/0/1.
对系统的影响	两端会话安全性降低
日志产生原因	输出该日志的触发条件可能包括： • MKA 会话由密文通信切换为明文通信 • Key Server 和它对端的接口未能都支持 MACsec 功能，或两端均未期望 MACsec 保护的情况下，两端协商出新的会话
处理建议	如果用户希望会话采用密文通信方式，则请先确认Key Server和它对端的接口都支持MACsec功能，再确认两个接口中至少有一个期望MACsec保护，只有两个条件都成立，会话才能采用密文通信方式

86 MBFD

本节介绍 MPLS BFD 模块输出的日志信息。

86.1 MBFD_TRACEROUTE_FAILURE

日志内容	[STRING] is failed. ([STRING].)
日志含义	周期性Traceroute检测出现错误
参数解释	$1：LSP信息 • 对于IPv4 LDP LSP，取值为LSP (LDP IPv4: *ipv4-address/mask-length*, nexthop: *nexthop-address*)。其中，*ipv4-address*为FEC的目的IPv4 地址前缀；*mask-length*为FEC目的IPv4 地址前缀的掩码长度；*nexthop-address*为LSP的下一跳地址 • 对于MPLS TE隧道，取值为TE tunnel (RSVP IPv4: *tunnel-name*)。其中，*tunnel-name*为MPLS TE隧道接口名称 $2：LSP失败原因，取值包括： • Malformed echo request received：收到的 echo request 报文内容错误 • One or more of the TLVs was not understood：报文中存在不支持的 TLV • Replying router has no mapping for the FEC：应答端不存在对应 FEC 的标签映射表项 • Downstream Mapping Mismatch：下游标签映射信息不匹配 • Upstream Interface Index Unknown：上游未填写出接口信息 • Label switched but no MPLS forwarding：标签交换节点上没有对应的转发信息 • Mapping for this FEC is not the given label：FEC 对应的转发标签与报文标签栈中的不一致 • No label entry：不存在报文标签栈中的标签对应的转发表项 • Protocol not associated with interface：FEC 对应的协议与报文标签转发表中的协议不一致 • Premature termination of ping due to label stack shrinking to a single label：只有单层标签导致 ping 异常终止
日志等级	3 (Error)
举例	MBFD/3/MBFD_TRACEROUTE_FAILURE: LSP (LDP IPv4: 22.22.2.2/32, nexthop: 20.20.20.2) is failed. (Replying router has no mapping for the FEC.) MBFD/5/MBFD_TRACEROUTE_FAILURE: TE tunnel (RSVP IPv4: Tunnel1) is failed. (No label entry.)
对系统的影响	LSP失败原因为Malformed echo request received或One or more of the TLVs was not understood时，表示周期性Traceroute检测功能本身存在问题，对系统和业务没有影响；LSP失败原因为其他值时，基于该LSP或TE隧道的流量可能会转发失败
日志产生原因	通过周期性Traceroute功能检测LSP或MPLS TE隧道时，如果收到带有不合法返回代码的应答，则打印本日志信息，说明周期性Traceroute检测功能本身存在问题，或LSP、MPLS TE隧道出现了故障
处理建议	LSP失败原因为Malformed echo request received或One or more of the TLVs was not understood时，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 LSP失败原因为其他值时，请检查LSP或者MPLS TE隧道经过节点上的隧道相关配置、转发表项信息是否准确。若配置和表项均正确，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

87 MBUF

本节介绍 MBUF 模块输出的日志信息。

87.1 MBUF_DATA_BLOCK_CREATE_FAIL

日志内容	Failed to create an MBUF data block because of insufficient memory. Failure count: [UINT32].
日志含义	申请MBUF数据块失败
参数解释	$1：失败次数
日志等级	2 (Critical)
举例	MBUF/2/MBUF_DATA_BLOCK_CREATE_FAIL: Failed to create an MBUF data block because of insufficient memory. Failure count: 128.
对系统的影响	会影响业务模块的运行
日志产生原因	业务模块运行时，向MBUF申请数据块，来存储运行数据。当申请MBUF数据块失败时，输出该日志。为避免该日志输出过于频繁，本次申请MBUF数据块失败距上次申请MBUF数据块失败间隔大于等于一分钟时，才会输出该日志
处理建议	1. 在Probe视图下执行 **display system internal kernel memory pool | include mbuf**命令查询已申请的MBUF数据块的数量 2. 在系统视图下执行 **display memory**命令查询系统内存总量 3. 将“已申请的 MBUF 数据块的数量”和“系统内存总量”比较，判断是否已申请的 MBUF 数据块过多导致申请失败 • 如果不是，则通过其他内存管理命令查询出占用内存较多的模块 • 如果是，则继续通过Probe视图下的 **display system internal mbuf socket statistics**命令查询Socket申请的MBUF数据块的数量，对比已申请的MBUF数据块的数量，判断是否某个进程缓存在Socket缓冲区中的MBUF数据块过多 o 如果是，则进一步分析进程不能及时释放 Socket 缓冲区中的 MBUF 数据块的原因 o 如果不是，则需要通过其他手段找出申请大量 MBUF 数据块的真正原因 4. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

88 MCS

本节介绍 MCS 模块输出的日志信息。

88.1 MCS_ENTRY_DRV_FAILED

日志内容	IGMP snooping entry refresh driver failed in [STRING].(SrcAddr=[STRING], GrpAddr=[STRING])
日志含义	二层组播转发表项下发芯片失败
参数解释	$1：VLAN或VSI信息，比如VLAN 10，或者VSI a $2：组播源地址 $3：组播组地址
日志等级	4(Notification)
举例	MCS/4/MCS_ENTRY_DRV_FAILED: IGMP snooping entry refresh driver failed in VLAN 10.(SrcAddr=1.1.1.1, GrpAddr=225.0.0.1)
对系统的影响	对系统无影响
日志产生原因	二层组播转发表项下发芯片失败
处理建议	1. 请在设备上执行 **display memory**命令查看系统内存占用率。 • 如果内存不足，请先解决内存问题，如果问题仍然不能解决，请执行步骤 2。 • 如果内存充足，则请执行步骤 2。 2. 请在设备上执行 **display l2-multicast ip forwarding**和 **display l2-multicast mac forwarding**命令查看设备上生成的二层组播转发表项。 • 如果设备上二层组播转发表项已达到设备允许的最大值，请清除无用的二层组播转发表项，释放资源。如果无用的IPv4 二层组播转发表项是通过侦听IGMP协议报文生成的动态生成的，请执行 **reset igmp-snooping group**命令删除；如果无用的二层组播转发表项是通过静态配置生成，请执行 **undo igmp-snooping static-group**命令删除。 • 如果设备上二层组播表项未达到设备允许的最大值，则请执行步骤 3。 3. 请收集告警信息和配置信息，并联系 H3C 技术支持工程师。

89 MCS6

本节介绍 MCS6 模块输出的日志信息。

89.1 MCS_ENTRY_DRV_FAILED

日志内容	MLD snooping entry refresh driver failed in [STRING].(SrcAddr=[STRING], GrpAddr=[STRING])
日志含义	二层组播转发表项下发芯片失败
参数解释	$1：VLAN或VSI信息，比如VLAN 10，或者VSI a $2：组播源地址 $3：组播组地址
日志等级	4(Notification)
举例	MCS6/4/MCS_ENTRY_DRV_FAILED: MLD snooping entry refresh driver failed in VLAN 10.(SrcAddr=10::1, GrpAddr=FF03::101)
对系统的影响	对系统无影响
日志产生原因	IPv6二层组播转发表项下发芯片失败
处理建议	1. 请在设备上执行 **display memory**命令查看系统内存占用率。 • 如果内存不足，请先解决内存问题，如果问题仍然不能解决，请执行步骤 2。 • 如果内存充足，则请执行步骤 2。 2. 请在设备上执行 **display ipv6 l2-multicast ip forwarding**和 **display ipv6 l2-multicast mac forwarding**命令查看设备上生成的IPv6 二层组播转发表项。 • 如果设备上IPv6 二层组播转发表项已达到设备允许的最大值，请清除无用的IPv6 二层组播转发表项，释放资源。如果无用的IPv6 二层组播转发表项是通过侦听MLD协议报文生成的动态生成的，请执行 **reset mld-snooping group**命令删除；如果无用的IPv6 二层组播转发表项是通过静态配置生成，请执行 **undo mld-snooping static-group**命令删除。 • 如果设备上 IPv6 二层组播表项未达到设备允许的最大值，则请执行步骤 3。 3. 请收集告警信息和配置信息，并联系技术支持

90 MDC

本节介绍 MDC（Multitenant Device Context，多租户设备环境）模块输出的日志信息。

90.1 MDC_CREATE

日志内容	MDC [UINT16] is created.
日志含义	MDC成功创建
参数解释	$1：MDC的编号
日志等级	5 (Notification)
举例	MDC/5/MDC_CREATE: MDC 2 is created.
对系统的影响	对系统无影响
日志产生原因	MDC成功创建
处理建议	无需处理

90.2 MDC_CREATE_ERR

日志内容	Failed to create MDC [UINT16] for not enough resources.
日志含义	因为资源不足，备用主控板上创建MDC失败
参数解释	$1：MDC的编号
日志等级	5 (Notification)
举例	MDC/5/MDC_CREATE_ERR: -Slot=1; Failed to create MDC 2 for not enough resources.
对系统的影响	设备主用和备用slot倒换后，会导致MDC无法运行
日志产生原因	备用主控板启动时会从主用主控板获取所有已创建的MDC的信息，并在备用主控板创建同样的MDC。如果备用主控板因为资源限制无法创建该MDC，则输出此日志信息。MDC进驻备用主控板失败，无法在该备用主控板上提供服务
处理建议	1. 使用 **display mdc resource**命令查询新插入的备用主控板的CPU、内存空间和磁盘空间 2. 增加备用主控板的内存或减少磁盘使用，以保证新 MDC 可创建 3. 使用 **undo mdc**命令删除该MDC，或者换一块资源足够的主控板作为备用主控板

90.3 MDC_DELETE

日志内容	MDC [UINT16] is deleted.
日志含义	成功删除MDC
参数解释	$1：MDC的编号
日志等级	5 (Notification)
举例	MDC/5/MDC_DELETE: MDC 2 is deleted.
对系统的影响	对系统无影响
日志产生原因	MDC成功删除
处理建议	无需处理

90.4 MDC_KERNEL_EVENT_TOOLONG

日志内容	[STRING] [UINT16] kernel event in sequence [STRING] function [STRING] failed to finish within [UINT32] minutes.
日志含义	MDC的某内核事件在长时间内未完成处理
参数解释	$1：MDC的编号 $2：内核事件的阶段 $3：内核事件阶段对应的函数的地址 $4：所用时间
日志等级	4 (Warning)
举例	MDC/4/MDC_KERNEL_EVENT_TOOLONG: slot=1; MDC 2 kernel event in sequence 0x4fe5 function 0xff245e failed to finish within 15 minutes.
对系统的影响	对系统无影响
日志产生原因	MDC的某内核事件在长时间内未完成处理
处理建议	**1.** 重启单板，尝试恢复 **2.** 请收集告警信息和配置信息，并联系技术支持工程师

90.5 MDC_LICENSE_EXPIRE

日志内容	The MDC feature's license will expire in [UINT32] days.
日志含义	MDC License将在指定天数后过期
参数解释	$1：天数，取值范围为1到30天
日志等级	5 (Notification)
举例	MDC/5/MDC_LICENSE_EXPIRE: The MDC feature’s license will expire in 5 days.
对系统的影响	对系统无影响
日志产生原因	MDC特性的授权即将过期
处理建议	请在授权到期前安装新的License

90.6 MDC_NO_FORMAL_LICENSE

日志内容	The feature MDC has no available formal license.
日志含义	当前主用主控板上未给MDC特性安装正式License
参数解释	无
日志等级	5 (Notification)
举例	MDC/5/MDC_NO_FORMAL_LICENSE: The feature MDC has no available formal license.
对系统的影响	对系统无影响
日志产生原因	备用主控板变为主用主控板了，但是新主用主控板没有安装MDC License。系统会给新主用主控板一个MDC试用期。试用期过期，如果用户还没有给新主用主控板安装License，则不能继续使用MDC特性
处理建议	请尽快安装正式MDC License

90.7 MDC_NO_LICENSE_EXIT

日志内容	The MDC feature is being disabled, because it has no license.
日志含义	因为缺乏授权，导致MDC功能无法使用
参数解释	无
日志等级	5 (Notification)
举例	MDC/5/MDC_NO_LICENSE_EXIT: The MDC feature is being disabled, because it has no license.
对系统的影响	MDC功能无法使用
日志产生原因	MDC特性被禁用，因为MDC License过期或者被卸载了
处理建议	请尽快安装正式MDC License

90.8 MDC_OFFLINE

日志内容	MDC [UINT16] is offline now.
日志含义	MDC停用了
参数解释	$1：MDC的编号
日志等级	5 (Notification)
举例	MDC/5/MDC_OFFLINE: MDC 2 is offline now.
对系统的影响	该MDC无法提供服务
日志产生原因	管理员执行**undo mdc start**命令停止运行指定MDC
处理建议	无需处理

90.9 MDC_ONLINE

日志内容	MDC [UINT16] is online now.
日志含义	MDC启用了
参数解释	$1：MDC的编号
日志等级	5 (Notification)
举例	MDC/5/MDC_ONLINE: MDC 2 is online now.
对系统的影响	对系统无影响
日志产生原因	管理员执行**mdc start**命令启动指定MDC
处理建议	无需处理

90.10 MDC_STATE_CHANGE

日志内容	Status of MDC [UINT16] changed to [STRING].
日志含义	MDC状态发生了变化
参数解释	$1：MDC的编号 $2：MDC的状态： ○ updating表示正在给MDC分配接口板，即对MDC执行 **location**命令 ○ stopping表示MDC正在停止，即MDC正在执行 **undo mdc start**命令 ○ inactive 表示 MDC 处于未启动状态 ○ starting表示MDC正在启动中，即对MDC正在执行 **mdc start**命令 ○ active 表示 MDC 正常运行
日志等级	5 (Notification)
举例	MDC/5/MDC_STATE_CHANGE: Status of MDC 2 changed to active.
对系统的影响	对系统无影响
日志产生原因	MDC在运行过程中状态发生了变化
处理建议	• 如果MDC处于inactive状态，可以执行 **mdc start**命令启动该MDC • 其它状态无需处理

91 MFIB

本节介绍组播转发模块输出的日志信息。

91.1 MFIB_IPV6L3MULTICAST_FAIL

日志内容	Failed to enable IPv6 Layer 3 multicast for VPN instance [STRING] because of insufficient resources. Failed to enable IPv6 Layer 3 multicast for the public network because of insufficient resources.
日志含义	驱动资源不足导致IPv6三层组播功能开启失败
参数解释	$1:VPN实例名，如果为公网侧则显示为the public network
日志等级	5 (Notification)
举例	MFIB/5/MFIB_IPV6L3MULTICAST_FAIL: Failed to enable IPv6 Layer 3 multicast for vpn-instance vpna because of insufficient resources.
对系统的影响	IPv6三层组播相关功能无法正常使用
日志产生原因	驱动资源不足
处理建议	• 请稍后重试 • 收集配置文件、日志信息和告警信息，并联系技术支持

91.2 MFIB_IPV6L3MULTICAST_FAIL_INT

日志内容	Failed to enable IPv6 Layer 3 multicast for interface [STRING] because of insufficient resources.
日志含义	驱动资源不足导致接口下IPv6三层组播功能开启失败
参数解释	$1:接口名
日志等级	5 (Notification)
举例	MFIB/5/MFIB_IPV6L3MULTICAST_FAIL_INT: Failed to enable IPv6 Layer 3 multicast for interface GigabitEthernet1/0/1 because of insufficient resources.
对系统的影响	接口下的IPv6三层组播功能无法正常使用
日志产生原因	驱动资源不足
处理建议	• 请稍后重试 • 收集配置文件、日志信息和告警信息，并联系技术支持

91.3 MFIB_IPV6L3MULTICAST_SUCCEED

日志内容	Enabled IPv6 Layer 3 multicast for VPN instance [STRING] successfully. Enabled IPv6 Layer 3 multicast for the public network successfully.
日志含义	IPv6三层组播功能使能恢复成功
参数解释	$1:VPN实例名，如果为公网侧则显示为the public network
日志等级	5 (Notification)
举例	MFIB/5/MFIB_IPV6L3MULTICAST_SUCCEED: Enabled IPv6 Layer 3 multicast for VPN instance vpna successfully.
对系统的影响	对系统无影响
日志产生原因	IPv6三层组播使能失败后，MFIB模块会以10秒为时间间隔，周期性将IPv6三层组播使能下驱动，如果驱动资源释放，使得驱动具有足够的资源使能IPv6三层组播，则IPv6三层组播使能下驱动成功
处理建议	无需处理

91.4 MFIB_IPV6L3MULTICAST_SUCCEED_INT

日志内容	Enabled IPv6 Layer 3 multicast for interface [STRING] successfully.
日志含义	接口下IPv6三层组播功能使能恢复成功
参数解释	$1:接口名
日志等级	5 (Notification)
举例	MFIB/5/MFIB_IPV6L3MULTICAST_SUCCEED_INT: -MDC=1; Enabled IPv6 Layer 3 multicast for interface GigabitEthernet1/0/1 successfully.
对系统的影响	对系统无影响
日志产生原因	IPv6三层组播使能失败后，MFIB模块会以10秒为时间间隔，周期性将IPv6三层组播使能下驱动。如果驱动资源释放，使得驱动具有足够的资源使能IPv6三层组播，则IPv6三层组播使能下驱动成功
处理建议	无需处理

91.5 MFIB_L3MULTICAST_FAIL

日志内容	Failed to enable Layer 3 multicast for VPN instance [STRING] because of insufficient resources. Failed to enable Layer 3 multicast for the public network because of insufficient resources.
日志含义	驱动资源不足导致IPv4三层组播功能开启失败
参数解释	$1: VPN实例名，如果为公网侧则显示为the public network
日志等级	5 (Notification)
举例	MFIB/5/MFIB_L3MULTICAST_FAIL: Failed to enable Layer 3 multicast for VPN instance vpna because of insufficient resources.
对系统的影响	IPv4三层组播相关功能无法正常使用
日志产生原因	驱动资源不足
处理建议	• 请稍后重试 • 收集配置文件、日志信息和告警信息，并联系技术支持

91.6 MFIB_L3MULTICAST_FAIL_INT

日志内容	Failed to enable Layer 3 multicast for interface [STRING] because of insufficient resources.
日志含义	驱动资源不足导致接口下IPv4三层组播功能开启失败
参数解释	$1: 接口名
日志等级	5 (Notification)
举例	MFIB/5/MFIB_L3MULTICAST_FAIL_INT: Failed to enable Layer 3 multicast for interface GigabitEthernet1/0/1 because of insufficient resources.
对系统的影响	接口下的IPv4组播功能无法正常使用
日志产生原因	驱动资源不足
处理建议	• 请稍后重试 • 收集配置文件、日志信息和告警信息，并联系技术支持

91.7 MFIB_L3MULTICAST_SUCCEED

日志内容	Enabled Layer 3 multicast for VPN instance [STRING] successfully. Enabled Layer 3 multicast for the public network successfully.
日志含义	IPv4三层组播功能使能恢复成功
参数解释	$1:VPN实例名，如果为公网侧则显示为the public network
日志等级	5 (Notification)
举例	MFIB/5/MFIB_L3MULTICAST_SUCCEED: -MDC=1; Enabled Layer 3 multicast for VPN instance vpna successfully.
对系统的影响	对系统无影响
日志产生原因	IPv4三层组播功能使能失败后，MFIB模块会以10秒为时间间隔，周期性将IPv4三层组播使能下驱动，如果驱动资源释放，使得驱动具有足够的资源使能IPv4三层组播，则IPv4三层组播使能下驱动成功
处理建议	无需处理

91.8 MFIB_L3MULTICAST_SUCCEED_INT

日志内容	Enabled Layer 3 multicast for interface [STRING] successfully.
日志含义	接口下IPv4三层组播功能使能恢复成功
参数解释	$1:接口名
日志等级	5 (Notification)
举例	MFIB/5/MFIB_L3MULTICAST_SUCCEED_INT: -MDC=1; Enabled Layer 3 multicast for interface GigabitEthernet1/0/1 successfully.
对系统的影响	对系统无影响
日志产生原因	三层IPv4组播功能使能失败后，MFIB模块会以10秒为时间间隔，周期性将IPv4三层组播使能下驱动。如果驱动资源释放，使得驱动具有足够的资源使能IPv4三层组播，则IPv4三层组播使能下驱动成功
处理建议	无需处理

91.9 MFIB_MEM_ALERT

日志内容	MFIB process received system memory alert [STRING] event.
日志含义	MFIB模块收到了系统发出的内存告警事件
参数解释	$1：内存告警事件类型
日志等级	5 (Notification)
举例	MFIB/5/MFIB_MEM_ALERT: MFIB process receive system memory alert start event.
对系统的影响	可能导致组播路由与转发相关功能无法正常使用
日志产生原因	内存资源不足
处理建议	1. 释放内存资源。例如，执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源 2. 执行 **display memory**命令查看内存使用情况： o 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，可以开启或者关闭进程对应的软件功能，来释放内存 o 如果内存占用率恢复到告警阈值以下，内存告警解除，MFIB 进程将恢复正常运行，无需额外处理 3. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

91.10 MFIB_MTI_NO_ENOUGH_RESOURCE

日志内容	Failed to create [STRING] because of insufficient resources.
日志含义	驱动资源不足，无法创建MTunnel隧道
参数解释	$1: MTunnel名称
日志等级	5 (Notification)
举例	MFIB/5/MFIB_MTI_NO_ENOUGH_RESOURCE: Failed to create MTunnel129 because of insufficient resources.
对系统的影响	MTunnel隧道创建失败，组播报文无法正常转发
日志产生原因	驱动资源不足
处理建议	删除暂时不用的组播隧道，释放组播隧道资源，可通过如下操作： • 在VXLAN视图下，使用 **undo group** *group-address* **source** *source-address*命令删除 • 在MVPN IPv4 地址族视图/MVPN IPv6 地址族视图下，使用 **undo default-group**命令删除

92 MGROUP

本节主要介绍与镜像组相关的日志消息。

92.1 MGROUP_APPLY_SAMPLER_FAIL

日志内容	Failed to apply the sampler for mirroring group [UINT16], because the sampler resources are insufficient.
日志含义	镜像组引用采样器失败
参数解释	$1：镜像组编号
日志等级	3 (Error)
举例	MGROUP/3/MGROUP_APPLY_SAMPLER_FAIL: Failed to apply the sampler for mirroring group 1, because the sampler resources are insufficient.
对系统的影响	无法对镜像报文进行采样
日志产生原因	采样器资源不足时，新镜像组引用采样器失败
处理建议	1. 通过 **display mirroring-group all**命令查看设备上所有镜像组引用的采样器，如果有不需要的，可以删除释放采样器资源 2. 执行以上操作后，若问题仍未解决，请收集配置文件、日志信息和告警信息，并联系技术支持

92.2 MGROUP_RESTORE_CPUCFG_FAIL

日志内容	Failed to restore configuration for mirroring CPU of [STRING] in mirroring group [UINT16], because [STRING].
日志含义	镜像组的源CPU配置恢复失败
参数解释	$1：单板所在的槽位号 $2：镜像组编号 $3：恢复源CPU配置失败的原因
日志等级	3 (Error)
举例	MGROUP/3/MGROUP_RESTORE_CPUCFG_FAIL: Failed to restore configuration for mirroring CPU of chassis 1 slot 2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
对系统的影响	源CPU方式的镜像功能无法正常使用
日志产生原因	当单板上的CPU用作镜像组的源CPU时，在单板拔出阶段，配置发生变化，单板再插入时，可能会引起镜像组源CPU的配置恢复失败
处理建议	排查配置恢复失败的原因，看是否是由于系统不支持变化的配置： • 如果是，请删除不支持的配置，重新配置镜像组的源 CPU • 如果不是，请收集配置文件、日志信息和告警信息，并联系技术支持

92.3 MGROUP_RESTORE_GROUP_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16], because [STRING]
日志含义	镜像组配置恢复失败
参数解释	$1：镜像组编号 $2：恢复镜像组配置失败的原因： o monitor resources are insufficient：镜像资源不足
日志等级	3 (Error)
举例	MGROUP/3/MGROUP_RESTORE_GROUP_FAIL: Failed to restore configuration for mirroring group 1, because monitor resources are insufficient.
对系统的影响	镜像功能无法正常使用
日志产生原因	设备启动后，因为镜像资源不足，导致镜像组的配置恢复失败
处理建议	1. 请删除不需要的镜像配置释放资源后，重新配置恢复失败的镜像组（流镜像和端口镜像使用相同的镜像资源。当设备整机重启时，优先恢复流镜像配置，再恢复端口镜像配置） 2. 执行以上操作后，若问题仍未解决，请收集配置文件、日志信息和告警信息，并联系技术支持

92.4 MGROUP_RESTORE_IFCFG_FAIL

日志内容	Failed to restore configuration for interface [STRING] in mirroring group [UINT16], because [STRING]
日志含义	镜像组的源端口配置恢复失败
参数解释	$1：接口名称 $2：镜像组编号 $3：恢复源端口配置失败的原因
日志等级	3 (Error)
举例	MGROUP/3/MGROUP_RESTORE_IFCFG_FAIL: Failed to restore configuration for interface Ethernet3/1/2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
对系统的影响	源端口方式的镜像功能无法正常使用
日志产生原因	当单板上的接口用作镜像组的源端口时，在单板拔出阶段，配置发生变化，单板再插入时，可能会引起镜像组源端口的配置恢复失败
处理建议	排查配置恢复失败的原因，看是否是由于系统不支持变化的配置： • 如果是，请删除不支持的配置，重新配置镜像组的源端口 • 如果不是，请收集配置文件、日志信息和告警信息，并联系技术支持

92.5 MGROUP_SYNC_CFG_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16] in [STRING], because [STRING]
日志含义	镜像组配置恢复失败
参数解释	$1：镜像组编号 $2：单板所在的槽位号 $3：恢复镜像组配置失败的原因
日志等级	3 (Error)
举例	MGROUP/3/MGROUP_SYNC_CFG_FAIL: Failed to restore configuration for mirroring group 1 in chassis 1 slot 2, because monitor resources are insufficient.
对系统的影响	镜像功能无法正常使用
日志产生原因	当向单板同步完整的镜像组配置时，由于单板资源不足，引起配置恢复失败
处理建议	1. 删除配置恢复失败的镜像组 2. 执行以上操作后，若问题仍未解决，请收集配置文件、日志信息和告警信息，并联系技术支持

93 MLAG

本节介绍 M-LAG 模块输出的日志信息。

93.1 MLAG_AUTORECOVERY_TIMEOUT

日志内容	The reload delay timer timed out. Please check configuration of the M-LAG system.
日志含义	M-LAG系统仅一台设备启动或M-LAG系统出现双主情况
参数解释	无
日志等级	4 (Warning)
举例	MLAG/4/MLAG_AUTORECOVERY_TIMEOUT: The reload delay timer timed out. Please check configuration of the M-LAG system.
对系统的影响	无
日志产生原因	M-LAG系统自动恢复定时器超时，M-LAG系统仅一台设备启动或M-LAG系统出现双主情况
处理建议	• 检查对端 M-LAG 设备是否正常启动 • 检查 peer-link 链路和 Keepalive 链路是否正常 • 检查自动恢复定时器配置值是否过小

93.2 MLAG_GLBCHECK_CONSISTENCY

日志内容	Finished global type [UINT16] configuration consistency check. No inconsistency exists.
日志含义	全局配置一致性检查结果一致
参数解释	$1：全局配置的类型，取值为： • 1：表示全局配置类型 1 • 2：表示全局配置类型 2
日志等级	6 (Informational)
举例	MLAG/6/MLAG_GLBCHECK_CONSISTENCY: Finished global type 1 configuration consistency check. No inconsistency exists.
对系统的影响	无
日志产生原因	M-LAG全局配置一致性检查结果一致
处理建议	无需处理

93.3 MLAG_GLBCHECK_INCONSISTENCY

日志内容	Detected global type [UINT16] configuration inconsistency.
日志含义	全局配置一致性检查结果不一致
参数解释	$1：全局配置的类型，取值为： • 1：表示全局配置类型 1 • 2：表示全局配置类型 2
日志等级	6 (Informational)
举例	MLAG/6/MLAG_GLBCHECK_INCONSISTENCY: Detected global type 1 configuration inconsistency.
对系统的影响	Type 1类型的全局配置不一致时，Secondary设备的所有DR口无法工作；Type 2类型的全局配置不一致时，无影响
日志产生原因	M-LAG全局配置一致性检查结果不一致
处理建议	• Type 1 类型的全局配置不一致，通过 **display m-lag consistency**命令查看两端设备配置信息，修改配置为一致 • ,Type 2 类型的全局配置不一致，建议两端设备配置为一致

93.4 MLAG_IFCHECK_CONSISTENCY

日志内容	Finished M-LAG interface [STRING] type [UINT16] configuration consistency check. No inconsistency exists.
日志含义	接口配置一致性接口检查结果一致
参数解释	$1：接口名称 $2：接口配置的类型，取值为： • 1：表示接口配置类型 1 • 2：表示接口配置类型 2
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFCHECK_CONSISTENCY: Finished M-LAG interface Bridge-Aggregation2 type 1 configuration consistency check. No inconsistency exists.
对系统的影响	无
日志产生原因	M-LAG接口配置一致性接口检查结果一致
处理建议	无需处理

93.5 MLAG_IFCHECK_INCONSISTENCY

日志内容	Detected type [UINT16] configuration inconsistency on interface [STRING].
日志含义	接口配置一致性检查不一致
参数解释	$1：接口配置的类型，取值为： • 1：表示接口配置类型 1 • 2：表示接口配置类型 2 $2：接口名称
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFCHECK_INCONSISTENCY: Detected type 1 configuration inconsistency on interface Bridge-Aggregation2.
对系统的影响	Type 1类型的接口配置不一致时，Secondary设备上当前的DR口无法工作；Type 2类型的接口配置不一致时，无影响
日志产生原因	M-LAG接口配置一致性检查不一致
处理建议	• Type 1 类型的接口配置不一致，通过 **display m-lag consistency**命令查看两端设备配置信息，修改配置为一致 • Type 2 类型的接口配置不一致，建议两端设备配置为一致

93.6 MLAG_IFEVT_MLAGIF_BIND

日志内容	Interface [STRING] was assigned to M-LAG group [UINT32].
日志含义	聚合接口加入分布式聚合组
参数解释	$1：二层聚合接口 $2：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_BIND: Interface Bridge-Aggregation1 was assigned to M-LAG group 1.
对系统的影响	无
日志产生原因	聚合接口加入M-LAG组，触发该日志的原因为用户设置
处理建议	无需处理

93.7 MLAG_IFEVT_MLAGIF_GLOBALDOWN

日志内容	The state of M-LAG interface [STRING] changed to globally down.
日志含义	分布式聚合接口变为全局DOWN状态
参数解释	$1：二层聚合接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_GLOBALDOWN: The state of M-LAG interface Bridge-Aggregation1 changed to globally down.
对系统的影响	当前接口无法转发业务流量
日志产生原因	M-LAG接口变为全局DOWN状态，触发该日志的原因为两台M-LAG设备相同M-LAG设备的成员端口都变为未选中状态，则为全局DOWN状态
处理建议	检查M-LAG设备的系统配置，系统优先级、系统MAC地址、系统编号是否已配置且一致

93.8 MLAG_IFEVT_MLAGIF_GLOBALUP

日志内容	The state of M-LAG interface [STRING] changed to globally up.
日志含义	分布式聚合接口变为全局UP状态
参数解释	$1：二层聚合接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_GLOBALUP: The state of M-LAG interface Bridge-Aggregation1 changed to globally up.
对系统的影响	
日志产生原因	M-LAG接口变为全局UP状态，触发该日志的原因为两台M-LAG设备相同M-LAG设备中第一次有成员端口变为被选中状态，则为全局UP状态
处理建议	无需处理

93.9 MLAG_IFEVT_MLAGIF_MAC_CHG

日志内容	Local M-LAG interface [STRING]'s system MAC address changed to [STRING]. Please ensure that the configuration is consistent with that of the peer M-LAG interface.
日志含义	M-LAG接口系统MAC地址配置发生变化
参数解释	$1：二层聚合接口 $2：系统MAC地址
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_MAC_CHG: Local M-LAG interface Bridge-Aggregation1's system MAC address changed to 2-2-2. Please ensure that the configuration is consistent with that of the peer M-LAG interface.
对系统的影响	无
日志产生原因	用户修改M-LAG接口系统MAC地址
处理建议	无需处理

93.10 MLAG_IFEVT_MLAGIF_NOSELECTED

日志内容	Local M-LAG interface [STRING] in M-LAG group [UINT32] does not have Selected member ports because [STRING].
日志含义	M-LAG接口对应的聚合组内无选中端口
参数解释	$1：二层聚合接口 $2：M-LAG组编号 $3：M-LAG设备DOWN的原因 • the aggregate interface went down. Please check the aggregate link status：由于 M-LAG 接口对应的聚合接口 DOWN 导致 M-LAG 接口 DOWN，请检查聚合接口链路状态 • no peer M-LAG interface was detected. Please check peer M-LAG interface configuration：由于未检测到对端 M-LAG 接口导致的 M-LAG 接口 DOWN，请检查对端 M-LAG 设备的配置情况 • of configuration consistency check failure. Please check the type 1 configuration of the M-LAG member devices for inconsistencies：由于配置一致性检查失败导致的 M-LAG 接口 DOWN，请检查 M-LAG 设备的 Type 1 配置情况 • it was removed from a M-LAG group. Please reconfigure the M-LAG interface settings as needed：由于聚合接口取消配置为 M-LAG 接口，导致 M-LAG 接口 DOWN，请根据需求重新配置 M-LAG 接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_NOSELECTED: Local M-LAG interface Bridge-Aggregation1 in M-LAG group 2 does not have Selected member ports because no peer M-LAG interface was detected. Please check peer M-LAG interface configuration.
对系统的影响	当前接口无法转发业务流量
日志产生原因	本端M-LAG接口对应的聚合组内无选中端口
处理建议	根据日志的显示信息检查聚合组成员端口配置或者线缆连接情况

93.11 MLAG_IFEVT_MLAGIF_PEERBIND

日志内容	An aggregate interface on the peer M-LAG device was assigned to M-LAG group [UINT32].
日志含义	对端M-LAG设备的聚合接口加入M-LAG组
参数解释	$1：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_PEERBIND: An aggregate interface on the peer M-LAG device was assigned to M-LAG group 1.
对系统的影响	无
日志产生原因	对端M-LAG设备的聚合接口加入M-LAG组，触发该日志的原因为用户设置
处理建议	无需处理

93.12 MLAG_IFEVT_MLAGIF_PEERUNBIND

日志内容	An aggregate interface on the peer M-LAG device was removed from M-LAG group [UINT32].
日志含义	对端M-LAG设备的聚合接口退出M-LAG组
参数解释	$1：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_PEERUNBIND: An aggregate interface on the peer M-LAG device was removed from M-LAG group 1.
对系统的影响	无
日志产生原因	对端M-LAG设备的聚合接口退出M-LAG组，触发该日志的原因为用户设置
处理建议	无需处理

93.13 MLAG_IFEVT_PEERIF_NOSELECTED

日志内容	Peer M-LAG interface in M-LAG group [UINT32] does not have Selected member ports.
日志含义	对端M-LAG接口对应的聚合组内无选中端口
参数解释	$1：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_PEERIF_NOSELECTED: Peer M-LAG interface in M-LAG group 10 does not have Selected member ports.
对系统的影响	当前接口无法转发业务流量
日志产生原因	对端M-LAG接口对应的聚合组内无选中端口
处理建议	检查对端聚合组成员端口配置或者线缆连接情况

93.14 MLAG_IFEVT_PEERIF_SELECTED

日志内容	Peer M-LAG interface in M-LAG group [UINT32] has Selected member ports.
日志含义	对端M-LAG接口对应的聚合组内存在选中端口
参数解释	$1：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_PEERIF_SELECTED: Peer M-LAG interface in M-LAG group 10 has Selected member ports.
对系统的影响	无
日志产生原因	对端M-LAG接口对应的聚合组内存在选中端口
处理建议	无需处理

93.15 MLAG_IFEVT_MLAGIF_PRIORITY_CHG

日志内容	M-LAG interface [STRING]'s system priority changed to [UINT16]. Please ensure that the configuration is consistent with that of the peer M-LAG interface.
日志含义	M-LAG接口的系统优先级发生变化
参数解释	$1：二层聚合接口 $2：新的系统优先级
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_PRIORITY_CHG: M-LAG interface Bridge-Aggregation1's system priority changed to 564. Please ensure that the configuration is consistent with that of the peer M-LAG interface.
对系统的影响	可能会导致设备的主备角色发生变化
日志产生原因	用户修改M-LAG接口的系统优先级
处理建议	无需处理

93.16 MLAG_IFEVT_MLAGIF_SELECTED

日志内容	Local M-LAG interface [STRING] in M-LAG group [UINT32] has Selected member ports.
日志含义	M-LAG接口对应的聚合组内存在选中端口
参数解释	$1：二层聚合接口 $2：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_SELECTED: Local M-LAG interface Bridge-Aggregation1 in M-LAG group 2 has Selected member ports.
对系统的影响	无
日志产生原因	M-LAG接口对应的聚合组内存在选中端口
处理建议	无需处理

93.17 MLAG_IFEVT_MLAGIF_UNBIND

日志内容	Interface [STRING] was removed from M-LAG group [UINT32].
日志含义	聚合接口退出M-LAG组
参数解释	$1：二层聚合接口 $2：M-LAG组编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_MLAGIF_UNBIND: Interface Bridge-Aggregation1 was removed from M-LAG group 1.
对系统的影响	可能导致业务流量被丢弃
日志产生原因	聚合接口退出M-LAG组，触发该日志的原因为用户设置
处理建议	无需处理

93.18 MLAG_IFEVT_PEERLINK_BIND

日志内容	Interface [STRING] was configured as peer-link interface [UINT16].
日志含义	聚合接口配置为peer-link接口
参数解释	$1：二层聚合接口 $2：peer-link接口编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_PEERLINK_BIND: Interface Bridge-Aggregation1 was configured as peer-link interface 1.
对系统的影响	无
日志产生原因	聚合接口配置为peer-link接口，触发该日志的原因为用户设置
处理建议	无需处理

93.19 MLAG_IFEVT_PEERLINK_DOWN

日志内容	IPP [STRING] went down because [STRING].
日志含义	peer-link接口变为DOWN
参数解释	$1：二层聚合接口 $2：peer-link接口DOWN的原因和处理建议 • the aggregate interface went down. Please check the aggregate link status：由于 peer-link 接口所在的聚合接口 DOWN 导致 peer-link 接口 DOWN，请检查聚合接口的链路状态 • the tunnel interface went down. Please check the tunnel link status：由于 IP 接口所在的 Tunnel 接口 DOWN 导致 peer-link 接口 DOWN，请检查 Tunnel 接口的链路状态 • no DRCPDUs were received. Please check the devices' DRCPDU transmission and reception status：由于接收不到有效 DRCP 报文导致的 peer-link 接口 DOWN，请检查两端 DRCP 报文收发状态 • the peer failed to receive DRCPDUs. Please check the devices' DRCPDU transmission and reception status：由于对端设备接收不到有效 DRCP 报文导致的 peer-link 接口 DOWN，请检查两端 DRCP 报文收发状态 • the peer-link role of the interface was removed. Please reconfigure an interface as the peer-link interface：由于接口取消配置为 peer-link 接口，导致 peer-link 接口 DOWN，请重新配置 peer-link 接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_PEERLINK_DOWN: IPP Bridge-Aggregation1 went down because the tunnel interface went down. Please check the tunnel link status.
对系统的影响	无法在DR设备之间转发业务流量和同步表项
日志产生原因	peer-link接口变为DOWN
处理建议	• 检查 M-LAG 设备的系统配置，系统优先级、系统 MAC 地址、系统编号、认证密码、序列号校验功能状态，是否已配置且一致 • 检查配置为 peer-link 接口的二层聚合接口状态

93.20 MLAG_IFEVT_PEERLINK_UNBIND

日志内容	Configuration for peer-link [UINT16] was removed from interface [STRING].
日志含义	删除peer-link接口
参数解释	$1：peer-link接口编号 $2：二层聚合接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_PEERLINK_UNBIND: Configuration for peer-link 1 was removed from interface Bridge-Aggregation1.
对系统的影响	无法在DR设备之间转发业务流量和同步表项
日志产生原因	删除peer-link接口，触发该日志的原因为用户设置
处理建议	无需处理

93.21 MLAG_IFEVT_PEERLINK_UP

日志内容	Peer-link interface [STRING] came up.
日志含义	peer-link接口变为UP状态
参数解释	$1：二层聚合接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_IFEVT_PEERLINK_UP: Peer-link interface Bridge-Aggregation1 came up.
对系统的影响	无
日志产生原因	peer-link接口变为UP状态，触发该日志的原因为M-LAG系统两端能正常收发DRCP协议报文
处理建议	无需处理

93.22 MLAG_PEERLINK_BLOCK

日志内容	The status of peer-link interface [STRING] changed to blocked.
日志含义	peer-link接口变为阻塞状态
参数解释	$1：二层聚合接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_PEERLINK_BLOCK: The status of peer-link interface Bridge-Aggregation20 changed to blocked.
对系统的影响	无法在DR设备之间转发业务流量和同步表项
日志产生原因	peer-link接口变为阻塞状态，该状态下peer-link接口仅能收发协议报文，不能收发数据报文。触发该日志的原因为当设备有角色且peer-link接口down时，peer-link接口变为阻塞状态
处理建议	• 检查 peer-link 链路连接线缆是否正常 • 检查 peer-link 链路两端配置是否一致

93.23 MLAG_PEERLINK_UNBLOCK

日志内容	The status of peer-link interface [STRING] changed to unblocked.
日志含义	peer-link接口变为非阻塞状态
参数解释	$1：二层聚合接口
日志等级	6 (Informational)
举例	MLAG/6/MLAG_PEERLINK_UNBLOCK: The status of peer-link interface Bridge-Aggregation20 changed to unblocked.
对系统的影响	无
日志产生原因	peer-link接口变为非阻塞状态，该状态下peer-link接口可以正常收发协议报文和数据报文。触发该日志的原因为当设备有角色且peer-link接口up时，peer-link接口变为非阻塞状态
处理建议	无需处理

93.24 MLAG_KEEPALIVEINTERVAL_MISMATCH

日志内容	Keepalive interval on the local M-LAG device is different from that on the neighbor.
日志含义	M-LAG系统两端配置的Keepalive报文发包间隔不一致
参数解释	无
日志等级	6 (Informational)
举例	MLAG/6/MLAG_KEEPALIVEINTERVAL_MISMATCH: Keepalive interval on the local M-LAG device is different from that on the neighbor.
对系统的影响	可能导致Keepalive会话震荡
日志产生原因	M-LAG系统两端的Keepalive报文发包间隔配置的不一致，会导致一端快速超时，出现误检测，触发该日志的原因为M-LAG系统两端配置的Keepalive报文发包间隔不一致
处理建议	将M-LAG系统两端的Keepalive报文发包间隔配置一致

93.25 MLAG_KEEPALIVELINK_DOWN

日志内容	Keepalive link went down because [STRING].
日志含义	Keepalive链路变为DOWN状态
参数解释	$1：Keepalive链路故障原因和处理建议 • keepalive IP address was not configured. Please configure keepalive IP address：由于未配置 Keepalive 报文的 IP 地址导致的 Keepalive 链路 DOWN，请先配置 Keepalive 报文的 IP 地址 • the device failed to send keepalive packets. Please check Layer 3 reachability to the peer：由于本端发送报文失败导致的 Keepalive 链路文 DOWN，请检查三层路由是否可达 • the local keepalive timeout timer expired. Please check the keepalive packet transmission and reception status at the two ends：由于本端接收报文超时导致的 Keepalive 链路 DOWN，请检查两端 Keepalive 报文收发状态 • the peer keepalive timeout timer expired. Please check the keepalive packet transmission and reception status at the two ends：由于对端接收报文超时导致的 Keepalive 链路 DOWN，请检查两端 Keepalive 报文收发状态
日志等级	6 (Informational)
举例	MLAG/6/MLAG_KEEPALIVELINK_DOWN: Keepalive link went down because the local keepalive timeout timer expired. Please check the keepalive packet transmission and reception status at the two ends.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	Keepalive链路变为DOWN状态
处理建议	• 检查设备角色 • 检查 M-LAG 设备的 Keepalive 配置，两端源 IP、目的 IP 是否匹配 • 检查所选取的三层链路状态

93.26 MLAG_KEEPALIVELINK_UP

日志内容	Keepalive link came up.
日志含义	Keepalive链路变为UP状态
参数解释	无
日志等级	6 (Informational)
举例	MLAG/6/MLAG_KEEPALIVELINK_UP: Keepalive link came up.
对系统的影响	无
日志产生原因	Keepalive链路变为UP状态，触发该日志的原因为M-LAG系统两端能正常收发Keepalive协议报文
处理建议	无需处理

93.27 MLAG_KEEPALIVEPACKETS_FAILED

日志内容	Failed to send keepalive packets to the CPU due to [STRING].
日志含义	
参数解释	$1：上送失败原因，目前仅支持insufficient device ACL resources，即设备ACL资源不足
日志等级	6 (Informational)
举例	MLAG/6/MLAG_KEEPALIVEPACKETS_FAILED: Failed to send keepalive packets to the CPU due to insufficient device ACL resources.
对系统的影响	可能会导致DR系统分裂
日志产生原因	由于设备ACL资源不足，导致无法将Keepalive报文上送CPU
处理建议	检查设备ACL资源占用情况，释放不必要资源，保证MLAG的Keepalive链路正常工作

93.28 MLAG_DEVICE_MADDOWN

日志内容	[STRING] will change to the M-LAG MAD DOWN state because [STRING].
日志含义	设备进行M-LAG MAD检测，会将部分接口置于M-LAG MAD状态
参数解释	$1：设备下发M-LAG MAD DOWN的接口范围 • All service interfaces not excluded from the M-LAG MAD DOWN action：设备上所有不是 M-LAG MAD 保留口的接口 • All service interfaces included in the M-LAG MAD DOWN action：设备上所有属于 M-LAG MAD include 的接口 • All new service interfaces not excluded from the M-LAG MAD DOWN ：设备上所有新加入且不是 M-LAG MAD 保留口的接口 • All new service interfaces included in the M-LAG MAD DOWN action：设备上所有新加入且属于 M-LAG MAD include 的接口 $2：设备下发M-LAG MAD DOWN的原因和处理建议 • the device is Initializing. Please set up the M-LAG system fisrt：设备正处于初始化状态，请先建立 M-LAG 系统 • the peer-link went down and the keepalive link remains up. Please check the peer-link interface settings on both ends of the peer-link：由于 peer-link 链路故障但 Keepalive 链路状态是 up 的，请检查 M-LAG 设备两端 peer-link 链路配置 • the peer-link came up. Please wait for the data restoration delay timer to expire：由于 peer-link 链路恢复工作，请等待延迟恢复定时器超时 • the peer-link and all M-LAG interfaces went down. Please first check the peer-link interface settings on both ends of the peer-link：由于 peer-link 链路和设备上所有 M-LAG 接口故障，设备无法正常工作，请先检查两端设备 peer-link 链路 配置
日志等级	4 (Warning)
举例	MLAG/4/MLAG_DEVICE_MADDOWN: All service interfaces not excluded from the MLAG MAD DOWN action will change to the M-LAG MAD DOWN state because the peer-link went down and the keepalive link remains up. Please check the peer-link interface settings on both ends of the peer-link.
对系统的影响	处于MAD DOWN状态的接口无法转发业务流量
日志产生原因	不同原因触发设备进行M-LAG MAD检测时，设备会根据触发原因和当前配置关闭相应业务接口
处理建议	检查peer-link链路两端配置

93.29 MLAG_DEVICE_MADRECOVERY

日志内容	All service interfaces on the device will be recovered from the M-LAG MAD DOWN state.
日志含义	处于M-LAG MAD DOWN状态的业务接口被开启
参数解释	无
日志等级	4 (Warning)
举例	MLAG/4/MLAG_DEVICE_MADRECOVERY: All service interfaces on the device will be recovered from the M-LAG MAD DOWN state.
对系统的影响	接口可以重新转发业务流量
日志产生原因	设备将会开启所有处于M-LAG MAD DOWN状态的业务接口
处理建议	无需处理

93.30 MLAG_SYSEVENT_DEVICEROLE_CHANGE

日志内容	Device role changed from [STRING] to [STRING] for [STRING].
日志含义	M-LAG设备角色变化
参数解释	$1：旧的设备角色，Primary、Secondary或None $2：新的设备角色，Primary、Secondary或None $3：角色变化原因： • M-LAG system initialization：M-LAG 系统初始化 • peer-link down and all M-LAG interfaces down：peer-link 链路故障时，所有 M-LAG 接口处于 down 状态 • peer-link and keepalive link down：peer-link 链路和 Keepalive 链路均故障 • peer-link calculation：本端设备角色通过 peer-link 链路计算 • peer-link down and role calculation based on keepalive link：peer-link 链路故障时，本端设备角色通过 Keepalive 链路计算
日志等级	6 (Informational)
举例	MLAG/6/MLAG_SYSEVENT_DEVICEROLE_CHANGE: Device role changed from Secondary to Primary for peer-link calculation.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	M-LAG设备角色变化及触发原因
处理建议	根据日志中角色变化原因排查故障

93.31 MLAG_SYSEVENT_MAC_CHANGE

日志内容	System MAC address changed from [STRING] to [STRING].
日志含义	M-LAG系统MAC变化
参数解释	$1：旧的系统MAC $2：新的系统MAC
日志等级	6 (Informational)
举例	MLAG/6/MLAG_SYSEVENT_MAC_CHANGE: System MAC address changed from 1-1-1 to 2-2-2.
对系统的影响	可能会导致设备角色发生变化
日志产生原因	M-LAG系统MAC变化，触发该日志的原因为用户设置
处理建议	无需处理

93.32 MLAG_SYSEVENT_MODE_CHANGE

日志内容	The device's working mode changed to [STRING].
日志含义	M-LAG设备工作模式变化
参数解释	$1：设备工作模式 • M-LAG system：M-LAG 系统 • standalone：独立工作
日志等级	6 (Informational)
举例	MLAG/6/MLAG_SYSEVENT_MODE_CHANGE: The device's working mode changed to standalone.
对系统的影响	可能会导致业务流量的转发路径发生变化
日志产生原因	M-LAG设备工作模式变化，触发原因为M-LAG系统分裂或者合并
处理建议	无需处理

93.33 MLAG_SYSEVENT_NUMBER_CHANGE

日志内容	System number changed from [STRING] to [STRING].
日志含义	M-LAG系统编号变化
参数解释	$1：旧的系统编号 $2：新的系统编号
日志等级	6 (Informational)
举例	MLAG/6/MLAG_SYSEVENT_NUMBER_CHANGE: System number changed from 1 to 2.
对系统的影响	可能会导致设备角色发生变化
日志产生原因	M-LAG系统编号变化，触发该日志的原因为用户设置
处理建议	无需处理

93.34 MLAG_SYSEVENT_PRIORITY_CHANGE

日志内容	System priority changed from [UINT16] to [UINT16].
日志含义	M-LAG系统优先级改变
参数解释	$1：旧的系统优先级 $2：新的系统优先级
日志等级	6 (Informational)
举例	MLAG/6/MLAG_SYSEVENT_PRIORITY_CHANGE: System priority changed from 123 to 564.
对系统的影响	可能会导致设备角色发生变化
日志产生原因	M-LAG系统优先级改变，触发该日志的原因为用户设置
处理建议	无需处理

93.35 MLAG_VMAC_INEFFECTIVE

日志内容	Failed to assign virtual MAC address [STRING] to interface [STRING]. Cause: [STRING].
日志含义	添加虚拟MAC地址失败
参数解释	$1：虚拟MAC地址 $2：接口名称，目前仅支持VLAN接口和LoopBack接口 $3：失败原因，目前仅包括硬件资源不足
日志等级	3 (Error)
举例	MLAG/3/MLAG_VMAC_INEFFECTIVE: Failed to assign virtual MAC address 0001-0001-0001 to interface Vlan-interface10. Cause: Insufficient hardware resources.
对系统的影响	接口的虚拟MAC地址配置失败
日志产生原因	在接口下配置MLAG虚拟IP地址和虚拟MAC地址时，由于硬件资源不足，导致添加虚拟MAC地址失败
处理建议	通过**display m-lag virtual-ip**命令查看M-LAG虚拟IP地址和MAC地址信息，然后通过**undo port m-lag [ipv6] virtual-ip [*ip-address*]**命令删除一些不需要的虚拟MAC地址，释放部分硬件资源

94 MLD

本节介绍 MLD 模块输出的日志信息。

94.1 MLD_GROUP_JOIN

日志内容	Interface receives an MLD Join message. (IfName=[STRING], IfIndex=[UINT32], Version=[STRING], SrcAddr=[STRING], GrpAddr=[STRING], HostAddr=[STRING], VPNName=[STRING])
日志含义	接收到组播MLDv1加入报文
参数解释	$1：接口名称 $2：接口索引 $3：MLD版本：MLDv1 $4：组播源地址 $5：组播组地址 $6：发送报文的主机地址 $7：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6(Notification)
举例	MLD/6/MLD_GROUP_JOIN: Interface receives an MLD Join message. (IfName=GigabitEthernet 1/0/1, IfIndex=257, Version=MLDv2, SrcAddr=10::1, GrpAddr=FF03::101, HostAddr=20::1, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	设备接收到组播MLDv1加入报文
处理建议	无需处理

94.2 MLD_GROUP_LEAVE

日志内容	Interface receives an MLD Leave message or corresponding group timer on this interface expires. (IfName=[STRING], IfIndex=[UINT32], SrcAddr=[STRING], GrpAddr=[STRING], VPNName=[STRING])
日志含义	设备接收到组播MLDv1离开报文
参数解释	$1：接口名称 $2：接口索引 $3：源地址 $4：组地址 $5：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6 (Notification)
举例	MLD/6/MLD_GROUP_LEAVE: Interface receives an MLD Leave message or corresponding group timer on this interface expires. (IfName=GigabitEthernet 1/0/1, IfIndex=257, SrcAddr=10::1, GrpAddr=FF03::101, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	设备接收到组播MLDv1成员离开报文
处理建议	无需处理

95 MOD

本节介绍 MOD 模块输出的日志信息。

95.1 MOD_ENABLE_FAIL

日志内容	Failed to enable MOD function. Reason: [STRING]
日志含义	开启MOD功能失败
参数解释	$1：失败原因 • The sampling function is not supported.：采样功能不支持 • The sampler has been used by another function.：采样器被其他功能引用
日志等级	4 (Warning)
举例	MOD/4/MOD_ENABLE_FAIL: Failed to enable MOD function. Reason: The sampling function is not supported.
对系统的影响	**reason-list**命令（MOD监控丢包原因）不生效
日志产生原因	请参见日志Reason字段
处理建议	通过**undo sampler**命令关闭MOD的采样功能

95.2 MOD_MODIFY_FAIL

日志内容	Failed to modify MOD parameters. Reason: [STRING]
日志含义	修改MOD参数失败
参数解释	$1：失败原因 • The sampling function is not supported.：采样功能不支持 • The sampler has been used by another function.：采样器被其他功能引用
日志等级	4 (Warning)
举例	MOD/4/MOD_MODIFY_FAIL: Failed to modify MOD parameters. Reason: The sampling function is not supported.
对系统的影响	修改MOD相关命令（如**device-id**、**collector**等）的参数后不生效
日志产生原因	请参见日志Reason字段
处理建议	通过**undo sampler**命令关闭MOD的采样功能

96 MPLS

本节介绍 MPLS 模块输出的日志信息。

96.1 MPLS_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for MPLS.
日志含义	MPLS硬件资源不足
参数解释	无
日志等级	4 (Warning)
举例	MPLS/4/MPLS_HARD_RESOURCE_NOENOUGH: No enough hardware resource for MPLS.
对系统的影响	无法建立新的LSP
日志产生原因	LSP数量过多等原因，导致MPLS硬件资源不足
处理建议	请检查是否生成了当前业务不需要的大量LSP。若是，则配置或调整标签分发协议的LSP触发策略、标签通告策略、标签接受策略，以过滤掉不需要的LSP

96.2 MPLS_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for MPLS are restored.
日志含义	MPLS硬件资源恢复
参数解释	无
日志等级	6 (Informational)
举例	MPLS/6/MPLS_HARD_RESOURCE_RESTORE: Hardware resources for MPLS are restored.
对系统的影响	对系统无影响
日志产生原因	MPLS从硬件资源不足恢复为具有足够的硬件资源
处理建议	无需处理

97 MRP

本节介绍 MRP 模块输出的日志信息。

97.1 IECMRP_INTER_MULTIPLE_MANAGERS

日志内容	The MIM detected another MIM (with MAC address [STRING]) in interconnection domain [STRING].
日志含义	MRP互联域中的MIM检测到另一个MIM
参数解释	$1：检测到另一MIM的MAC地址 $2：MRP互联域ID
日志等级	3 (Error)
举例	IECMRP/3/IECMRP_INTER_MULTIPLE_MANAGERS: The MIM detected another MIM (with MAC address 0000-0012-0034) in interconnection domain 3.
对系统的影响	MRP互联域中的MRP功能不能正常运行
日志产生原因	在同一MRP互联域中有多台设备被配置为了MIM
处理建议	检查同一MRP互联域中其他设备的配置，确保在同一MRP互联域中只有一台设备的角色为MIM

97.2 IECMRP_INTER_ROLE_FAIL

日志内容	The device cannot operate as an MIM in interconnection domain [STRING].
日志含义	在MRP互联域中，设备的节点角色被配置为MIM，但是不能作为MIM工作
参数解释	$1：MRP互联域ID
日志等级	3 (Error)
举例	IECMRP/3/IECMRP_INTER_ROLE_FAIL: The device cannot operate as an MIM in interconnection domain 3.
对系统的影响	设备不能作为MIM工作
日志产生原因	为MRP互联域指定的互联端口不支持Blocked状态时，该互联端口所在的设备不能在MRP互联域中作为MIM工作
处理建议	请根据设备的实际情况进行如下处理： • 如果设备上仅部分端口不支持 Blocked 状态，请重新为 MRP 互联域指定支持 Blocked 状态的互联端口 • 如果设备上的所有端口均不支持 Blocked 状态，请在 MRP 互联域中指定其他设备作为 MIM，保证该设备上存在端口支持 Blocked 状态

97.3 IECMRP_INTER_STATE_CHANGE

日志内容	The ring state for interconnection domain [STRING] has changed to [STRING].
日志含义	MRP互联域的换状态发生变化，仅MIM会输出本日志
参数解释	$1：MRP互联域ID $2：MRP冗余域的环状态，取值包括： • OPEN：开环状态 • CLOSE：闭环状态
日志等级	5 (Notification)
举例	IECMRP/5/IECMRP_INTER_STATE_CHANGE: The ring state for interconnection domain 3 has changed to OPEN.
对系统的影响	对系统无影响
日志产生原因	MRP互联域中发生了链路Down或恢复Up的事件
处理建议	无需处理

97.4 IECMRP_MRA_ROLE_CHANGE

日志内容	The role state for the MRA has changed from [STRING] to [STRING] in redundancy domain [STRING].
日志含义	MRA通过重新选举变化了在MRP冗余域中承担的节点角色
参数解释	$1：MRA的原节点角色，取值包括： • MRC：MRC 节点角色 • MRM：MRM 节点角色 $2：MRA变化后的节点角色，取值包括： • MRC：MRC 节点角色 • MRM：MRM 节点角色 $3：MRP冗余域ID
日志等级	5 (Notification)
举例	IECMRP/5/IECMRP_MRA_ROLE_CHANGE: The role state for the MRA has changed from MRC to MRM in redundancy domain 3.
对系统的影响	在MRP冗余域中，一台MRA通过选举转换为MRM，其余MRA均转换为MRC
日志产生原因	MRP功能启动后，所有MRA进行角色选举
处理建议	无需处理

97.5 IECMRP_MULTIPLE_MANAGERS

日志内容	The MRM detected another MRM (with MAC address [STRING]) in redundancy domain [STRING].
日志含义	MRP冗余域的MRM检测到另一个MRM
参数解释	$1：检测到另一MRM的MAC地址 $2：MRP冗余域ID
日志等级	3 (Error)
举例	IECMRP/3/IECMRP_MULTIPLE_MANAGERS: The MRM detected another MRM (with MAC address 0000-0012-0034) in redundancy domain 3.
对系统的影响	MRP冗余域中的MRP功能无法正常运行
日志产生原因	在同一MRP冗余域中有多台设备被配置为了MRM
处理建议	检查同一MRP冗余域中其他设备的配置，确保在同一MRP冗余域中只有一台设备的角色为MRM

97.6 IECMRP_REDUNANCY_ROLE_FAIL

日志内容	The device cannot operate as an MRM in redundancy domain [STRING].
日志含义	在MRP冗余域中，设备的节点角色被配置为MRM，但是不能作为MRM工作
参数解释	$1：MRP冗余域ID
日志等级	3 (Error)
举例	IECMRP/3/IECMRP_REDUNANCY_ROLE_FAIL: The device cannot operate as an MRM in redundancy domain 3.
对系统的影响	设备不能作为MRM工作
日志产生原因	为MRP冗余域指定的环端口不支持Blocked状态时，该环端口所在的设备不能在MRP冗余域中作为MRM工作
处理建议	请根据设备的实际情况进行如下处理： • 如果设备上仅部分端口不支持 Blocked 状态，请重新为 MRP 冗余域指定支持 Blocked 状态的环端口 • 如果设备上的所有端口均不支持 Blocked 状态，请在 MRP 冗余域中指定其他设备作为 MRM，保证该设备上存在支持 Blocked 状态的端口

97.7 IECMRP_REDUN_STATE_CHANGE

日志内容	The ring state for redundancy domain [STRING] has changed to [STRING].
日志含义	MRP冗余域的环状态发生变化，仅MRM会输出本日志
参数解释	$1：MRP冗余域ID $2：MRP冗余域的环状态，取值包括： • OPEN：开环状态 • CLOSE：闭环状态
日志等级	5 (Notification)
举例	IECMRP/5/IECMRP_REDUN_STATE_CHANGE: The ring state for redundancy domain 3 has changed to OPEN.
对系统的影响	对系统无影响
日志产生原因	MRP冗余域中存在链路Down或回复Up的时间
处理建议	无需处理

98 MTLK

本节介绍 Monitor Link 模块输出的日志信息。

98.1 MTLK_UPLINK_STATUS_CHANGE

日志内容	The uplink of monitor link group [UINT32] is [STRING].
日志含义	Monitor Link组的状态up或down
参数解释	$1：Monitor Link组ID $2：Monitor Link组状态 ○ down：故障 ○ up：正常
日志等级	6 (Informational)
举例	MTLK/6/MTLK_UPLINK_STATUS_CHANGE: The uplink of monitor link group 1 is up.
对系统的影响	Monitor Link组处于down状态时，该Monitor Link组所在链路无法转发流量
日志产生原因	• Monitor Link 组状态为 up 的上行接口个数低于上行接口阈值时，Monitor Link 组处于 down 状态 • Monitor Link 组状态为 up 的上行接口个数大于或等于上行接口阈值时，Monitor Link 组的状态恢复为 up
处理建议	检查故障链路

99 MTP

本节介绍 MTP 模块输出的日志信息。

99.1 MTP_PING_INFO

日志内容	Ping information, (Base: [STRING]), (Result: [STRING]).
日志含义	开启MTP功能后，设备向超时的邻居发起Ping操作的结果
参数解释	$1：Ping的基本信息，包括Ping的时间、目的IP地址、VRF索引、协议模块信息、发送Ping包的数量。协议模块信息包含模块名和实例名，若无实例名，则为空 $2：Ping的结果信息，包括发送Ping包成功数以及各Ping包结果信息。Ping包结果信息包含Ping包长度、Ping包发送顺序以及结果
日志等级	6 (Informational)
举例	MTP/6/MTP_PING_INFO: Ping information, (Base: Time = 09:39:18, Destination IP = 10.11.1.1, VrfIndex = 0, Protocol Module = BGP (default), Packet Number = 9), (Result: Success = 9, Length 100 ping 1 success, Length 100 ping 2 success, Length 100 ping 3 success, Length 1000 ping 4 success, Length 1000 ping 5 success, Length 1000 ping 6 success, Length 4000 ping 7 success, Length 4000 ping 8 success, Length 4000 ping 9 success).
对系统的影响	对系统无影响
日志产生原因	开启MTP功能后，当与邻居间的路由协议报文超时时，设备会向超时的邻居发起Ping操作并记录Ping结果
处理建议	可以通过以下方式进行处理： • 根据 Ping 结果信息，检查相应链路是否存在故障 • 执行 **display** *protocol* **troubleshooting**等路由协议模块的故障检测显示命令查看邻居断开的原因 • 执行 **display logbuffer**命令查看MTP的详细信息

99.2 MTP_TRACERT_INFO

日志内容	Tracert information, (Base: [STRING]), (Result: [STRING]).
日志含义	开启MTP功能后，设备向超时的邻居发起Tracert操作的结果
参数解释	$1：Tracert的基本信息，包括Tracert的时间、目的IP地址、VRF索引、最大跳数、每跳发送探测报文数、协议模块信息。协议模块信息包含模块名和实例名，若无实例名，则为空 $2：Tracert的结果信息，包括每一跳探测的回应IP地址、回应IP地址所属AS号（若不存在则不显示）以及探测成功的次数。若该跳探测无回应，则不显示该跳结果信息
日志等级	6 (Informational)
举例	MTP/6/MTP_TRACERT_INFO: Tracert information, (Base: Time = 10:39:18, Destination IP = 10.11.1.1, VrfIndex = 0, MaxHop = 30, Packet Number = 3, Protocol Module = BGP (default)), (Result: TTL 1 Response IP = 10.2.1.1 Success = 3, TTL 2 Response IP = 10.11.1.1 [AS 100] Success = 3).
对系统的影响	对系统无影响
日志产生原因	开启MTP功能后，当与邻居间的路由协议报文超时时，设备会向超时的邻居发起Tracert操作并记录Tracert结果
处理建议	可以通过以下方式进行处理： • 根据 Tracert 结果信息，检查相应链路是否存在故障 • 执行 **display** *protocol* **troubleshooting**等路由协议模块的故障检测显示命令查看邻居断开的原因 • 执行 **display logbuffer**命令查看MTP的详细信息

100 NA4

本节介绍 NA4（IPv4 NetAnalysis）模块输出的日志信息。

100.1 NA4_CLEARINFO_DRV

日志内容	Failed to clear the RoCEv2 flow statistics.
日志含义	清除NetAnalysis功能中RoCEv2流的统计信息失败
参数解释	无
日志等级	4 (Warning)
举例	NA4/4/NA4_CLEARINFO_DRV: Failed to clear the RoCEv2 flow statistics.
对系统的影响	无法先清除历史RoCEv2流的统计信息，再专门统计某段时间的RoCEv2流信息
日志产生原因	清除RoCEv2流的统计功能下发驱动失败
处理建议	**1.** 请稍后重新尝试 **2.** 收集配置文件、日志信息和告警信息，并联系技术支持

100.2 NA4_GETINFO_DRV

日志内容	Failed to obtain the RoCEv2 flow statistics.
日志含义	获取NetAnalysis功能中RoCEv2流的统计信息失败
参数解释	无
日志等级	4 (Warning)
举例	NA4/4/NA4_GETINFO_DRV: Failed to obtain the RoCEv2 flow statistics.
对系统的影响	无法及时获取RoCEv2流的统计信息，影响指定业务流的深度分析
日志产生原因	获取NetAnalysis功能中RoCEv2流的统计信息功能下发驱动失败
处理建议	**1.** 请稍后重新尝试 **2.** 收集配置文件、日志信息和告警信息，并联系技术支持

100.3 NA4_STATISTIC_DRV

日志内容	The operation conflicts with some existing configurations.
日志含义	该操作与已存在的配置冲突
参数解释	无
日志等级	4 (Warning)
举例	NA4/4/NA4_STATISTIC_DRV: The operation conflicts with some existing configurations.
对系统的影响	当前配置无法成功下发
日志产生原因	系统中存在与该操作冲突的配置
处理建议	请删除冲突配置

101 NAT

本节介绍 NAT 模块输出的日志信息。

101.1 NAT_ADDR_BIND_CONFLICT

日志内容	Failed to activate NAT configuration on interface [STRING], because global IP addresses already bound to another service card.
日志含义	无法激活接口上的NAT配置，因为NAT配置中的公网IP地址已经被其他业务板绑定
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	NAT/4/NAT_ADDR_BIND_CONFLICT: Failed to activate NAT configuration on interface GigabitEthernet1/0/2, because global IP addresses already bound to another service card.
对系统的影响	配置成功但实际不生效
日志产生原因	配置中的外网地址绑定指定业务板时发现其已经绑定到其他业务板上，则触发该日志
处理建议	1. 请执行 **display nat all**命令检查是否存在多个接口引用了同一个地址组或外网地址的配置。 o 如果存在，则这些接口必须指定同一块业务板进行NAT处理。请在需要修改配置的接口下执行 **undo nat service**命令取消指定的slot，再执行 **nat service**命令重新指定slot，确保上述接口下指定的slot相同。 o 如果不存在，请执行步骤 2。 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

101.2 NAT_FAILED_ADD_FLOW_RULE

日志内容	Failed to add flow-table due to: [STRING].
日志含义	添加流表失败
参数解释	$1：失败原因，取值包括： • Not enough resources are available to complete the operation：资源不足，无法完成添加流表的操作。资源不足包括硬件资源不足、内存不足等 • Operation failed：添加流表失败 • The item already exists：已存在相同的流表
日志等级	4 (Warning)
举例	NAT/4/NAT_FAILED_ADD_FLOW_RULE: Failed to add flow-table due to: Not enough resources are available to complete the operation.
对系统的影响	影响引流，可能导致正反向流量无法在同一个引擎上处理，引发流量不通
日志产生原因	添加流表失败，可能原因包括硬件资源不足、内存不足等

处理建议	失败原因为“Not enough resources are available to complete the operation”，处理步骤如下：
	1. 请使用 **display memory**命令查看内存资源是否充足。
	  ○ 如果内存资源不足，请关闭一些不必要的功能尝试解决此问题。
	  ○ 如果内存资源充足，请执行 2。
	2. 请增加能够处理 NAT 业务的接口板。
	3. 请通过 **undo nat flow-redirect**命令关闭NAT生成OpenFlow流表功能。
	4. 请通过 **session flow-redirect enable**命令开启会话引流功能。
	5. 请通过 **session flow-redirect hardware-fast-forwarding**命令开启会话引流的硬件快速转发功能。
	6. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。
	失败原因为“Operation failed”或“The item already exists”时，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

101.3 NAT_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
日志含义	创建或删除NAT会话
参数解释	$1：协议类型 $2：源IP地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IP地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：源DS-Lite Tunnel $17：目的DS-Lite Tunnel $18：创建会话的时间 $19：会话删除时间 $20：日志类型。取值包括1、2、3、6、8和254 $21：日志类型描述信息，包括： • Session created：NAT 会话创建日志。对应的日志类型取值为 8 • Active flow threshold：流量或时间阈值日志。对应的日志类型取值为 6 • Normal over：正常流结束，会话删除日志。对应的日志类型取值为 1 • Aged for timeout：会话老化删除日志。对应的日志类型取值为 2 • Aged for reset or config-change：通过配置删除会话日志。对应的日志类型取值为 3 • Other：其他原因删除会话日志，如由其他模块删除。对应的日志类型取值为 254
日志等级	6 (Informational)
举例	NAT/6/NAT_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=20.20.20.20;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session

	created;
对系统的影响	对系统无影响
日志产生原因	创建、删除NAT会话时会发送该日志 NAT会话过程中会定时发送该日志 NAT会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无需处理

101.4 NAT_SERVER_INVALID

日志内容	The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
日志含义	Easy IP方式的NAT内部服务器无法生效，因为与同一个接口下的其他NAT内部服务器使用了相同的公网信息
参数解释	无
日志等级	4 (Warning)
举例	NAT/4/NAT_SERVER_INVALID: The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
对系统的影响	Easy IP方式的NAT内部服务器配置无法生效
日志产生原因	Easy IP方式的NAT服务器配置生效时发现同一个接口下存在其他NAT服务器配置也包含相同的外网信息，则触发该日志
处理建议	1. 请执行 **display nat all**命令检查“NAT internal server information”下的配置信息。 2. 同一个接口下配置的NAT服务器，其协议类型、外网地址和外网端口号的组合必须是唯一的。请通过 **nat server**命令修改不符合此要求的内部服务器配置。 3. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

101.5 NAT_SERVICE_CARD_RECOVER_FAILURE

日志内容	形式一： Failed to recover the configuration of binding the service card on slot [UINT16] to interface [STRING], because [STRING]. 形式二： Failed to recover the configuration of binding the service card on chassis [UINT16] slot [UINT16] to interface [STRING], because [STRING].
日志含义	恢复接口绑定的业务板上的配置失败
参数解释	形式一： $1：slot编号 $2：接口名称 $3：指定接口绑定业务板配置恢复失败的原因 • NAT addresses already bound to another service card：NAT 地址已经绑定到其他业务板 • NAT service is not supported on this service card：指定业务板不支持 NAT 业务 • the hardware resources are not enough：硬件资源不足 • unknown error：未知错误 形式二： $1：chassis编号 $2：slot编号 $3：接口名称 $4：指定接口绑定业务板配置恢复失败的原因 • NAT addresses already bound to another service card：NAT 地址已经绑定到其他业务板 • NAT service is not supported on this service card：指定业务板不支持 NAT 业务 • the hardware resources are not enough：硬件资源不足 • unknown error：未知错误
日志等级	4 (Warning)
举例	NAT/4/NAT_SERVICE_CARD_RECOVER_FAILURE: Failed to recover the configuration of binding the service card on slot 3 to interface GigabitEthernet0/0/2, because NAT service is not supported on this service card.
对系统的影响	业务板无法处理NAT业务
日志产生原因	• NAT 地址已经绑定到其他业务板 • 指定业务板不支持 NAT 业务 • 硬件资源不足
处理建议	**1.** 如果提示业务板不支持 NAT 业务、硬件资源不足或者未知错误，请排查业务板的硬件问题请检查日志信息中“because”字段的取值。 o 如果取值为“NAT addresses already bound to another service card”，则使用 **display nat all**检查配置，并修改配置使得引用相同外网地址的接口绑定相同的业务板。 o 如果取值为“NAT service is not supported on this service card”、“the hardware resources are not enough”或“unknown error”，请排除业务板的硬件问题。

	2. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

102 ND

本节介绍 ND 模块输出的日志信息。

102.1 ND_COMMONPROXY_ENABLE_FAILED

日志内容	Failed to enable common ND proxy on interface [STRING].
日志含义	使能普通ND Proxy功能失败
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ND/4/ND_COMMONPROXY_ENABLE_FAILED: Failed to enable common ND proxy on interface Vlan-interface 1.
对系统的影响	可能会造成用户业务或者流量中断
日志产生原因	产生此日志的可能原因包括： • 接口上使能普通 ND Proxy 功能失败 • 主控板的接口上使能普通 ND Proxy 功能成功、非主控板的接口上使能普通 ND Proxy 功能失败，则在相应非主控板打印该日志信息
处理建议	**1.** 检查设备相应单板是否支持配置普通 ND Proxy 功能 **2.** 检查设备的硬件资源是否充足，删除不必要的配置 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.2 ND_CONFLICT

日志内容	[STRING] is inconsistent.
日志含义	配置与邻居路由器上不一致
参数解释	$1：配置类型 • M_FLAG：被管理地址配置标志位 • O_FLAG：其他信息配置标志位 • CUR_HOP_LIMIT：跳数限制 • REACHABLE TIME：保持邻居可达状态的时间 • NS INTERVAL：邻居请求消息间隔 • MTU：发布链路的 MTU • PREFIX VALID TIME：前缀的有效存活时间 • PREFIX PREFERRED TIME：前缀用于无状态地址配置的优选项的存活时间
日志等级	6 (Informational)
举例	ND/6/ND_CONFLICT: PREFIX VALID TIME is inconsistent.
对系统的影响	可能造成用户业务或者流量中断
日志产生原因	设备收到一个路由通告消息，导致与邻居路由器上的配置不一致
处理建议	检查设备配置，修改设备配置为与邻居路由器上的配置一致

102.3 ND_DUPADDR

日志内容	Duplicate address: [STRING] on the interface [STRING].
日志含义	接口IPv6地址冲突
参数解释	$1：将要分配的IPv6地址 $2：接口名称
日志等级	6 (Informational)
举例	ND/6/ND_DUPADDR: Duplicate address: 33::8 on the interface Vlan-interface9.
对系统的影响	无
日志产生原因	分配给该接口的IPv6地址已经被网络中其他设备使用
处理建议	根据网络规划和业务部署，重新给该接口分配一个新的IPv6地址

102.4 ND_ENTRY_ENOUGHRESOURCE

日志内容	Issued the software entry to the driver for IPv6 address [STRING] on VPN instance [STRING]. Issued the software entry to the driver for IPv6 address [STRING] on the public network.
日志含义	下发ND软件表项到驱动刷新硬件表项
参数解释	$1：IPv6地址 $2：VPN实例名。如果该ND属于公网，该字段不显示
日志等级	6 (Informational)
举例	ND/6/ND_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv6 address 10::1 on VPN instance vpn_1. ND/6/ND_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv6 address 10::2 on the public network.
对系统的影响	无
日志产生原因	通过**ipv6 nd consistency-check enable**命令开启ND表项一致性检查功能后，如果ND重刷硬件表项成功，则输出此日志
处理建议	无需处理

102.5 ND_ENTRY_INCONSISTENT

日志内容	Inconsistent software and hardware ND entries for IPv6 address [STRING] on VPN instance [STRING]. Inconsistent parameters: [STRING]. Inconsistent software and hardware ND entries for IPv6 address [STRING] on the public network. Inconsistent parameters: [STRING].
日志含义	ND软件表项与硬件表项不一致
参数解释	$1：IPv6地址 $2：VPN实例名。如果该ND属于公网，该字段不显示 $3：不一致的表项参数类型 o MAC address：MAC 地址 o output interface：ND 表项的出接口 o output port ：ND 表项的出端口 o outermost layer VLAN ID：第一层 VLAN 标签 o second outermost layer VLAN ID：第二层 VLAN 标签 o VSI index：VSI 索引 o link ID：VSI 出链路标识符
日志等级	6 (Informational)
举例	ND/6/ND_ENTRY_INCONSISTENT: Inconsistent software and hardware ND entries for IPv6 address 10::1 on VPN instance vpn_1. Inconsistent parameters: MAC address, output port, VSI index, and link ID. ND/6/ND_ENTRY_INCONSISTENT: Inconsistent software and hardware ND entries for IPv6 address 10::2 on the public network. Inconsistent parameters: MAC address, output port, VSI index, and link ID.
对系统的影响	可能造成业务流量不通等异常
日志产生原因	通过**ipv6 nd consistency-check enable**命令开启ND表项一致性检查功能后，如果设备检测到ND软件表项与硬件表项不一致（比如ND表项的出接口），则输出本日志
处理建议	无需处理，ND模块会主动根据ND软件表项刷新驱动硬件表项

102.6 ND_ENTRY_NORESOURCE

日志内容	Not enough hardware resources to issue the software entry to the driver for IPv6 address [STRING] on VPN instance [STRING]. Not enough hardware resources to issue the software entry to the driver for IPv6 address [STRING] on the public network.
日志含义	硬件资源不足时ND软件表项下发驱动
参数解释	$1：IPv6地址 $2：VPN实例名。如果该ND属于公网，该字段不显示
日志等级	6 (Informational)
举例	ND/6/ND_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv6 address 10::1 on VPN instance vpn_1. ND/6/ND_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv6 address 10::2 on the public network.
对系统的影响	无
日志产生原因	通过**ipv6 nd consistency-check enable**命令开启ND表项一致性检查功能后，当ND软件表项下发驱动时，驱动没有足够的ND硬件表项资源，则输出此日志
处理建议	无需处理，ND模块会主动根据ND软件表项刷新驱动硬件表项

102.7 ND_EVENTQUE_ALERT

日志内容	The current size of the EVENT queue has reached [UINT32]. Please check the network environment.
日志含义	当前ND事件队列长度超过4096
参数解释	$1: ND事件队列长度
日志等级	4 (Warning)
举例	ND/4/ND_EVENTQUE_ALERT: The current size of the EVENT queue has reached 4096. Please check the network environment.
对系统的影响	ND事件队列长度达到队列容量上限时会丢弃ND事件消息，影响正常业务
日志产生原因	当ND事件队列中ND事件消息的个数超过4096时，系统将每隔60秒输出一次日志信息进行提示
处理建议	1. 检查接口上收到的 ND 报文是否正常，如果收到异常的 ND 报文，则通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.8 ND_HARDWARE_REFRESH_NORESOURCE

日志内容	Failed to refresh the host route in FIB according to the ND entry because the device resources are insufficient. IPv6 address=[STRING]; VPN instance name=[STRING]; VPN instance index=[UINT16]; Interface=[STRING].
日志含义	设备资源不足导致转发表中的主机路由根据ND表项刷新失败
参数解释	$1：ND表项的IPv6地址 $2：ND表项的VPN实例名称。如果是公网内的日志信息，则显示为Public $3：ND表项的VPN实例索引。如果是公网内的日志信息，则显示为0 $4：ND表项所对应的出接口名称
日志等级	4 (Warning)
举例	ND/4/ND_HARDWARE_REFRESH_NORESOURCE: Failed to refresh the host route in FIB according to the ND entry because the device resources are insufficient. IPv6 address=1::1; VPN instance name=vpn1; VPN instance index=1; Interface=GigabitEthernet1/0/1.
对系统的影响	影响正常的报文转发，导致业务不通
日志产生原因	使用**ipv6 nd hardware log enable**命令开启ND表项下发硬件日志功能后，由于硬件资源不足导致转发表中的主机路由无法成功刷新
处理建议	**1.** 请检查设备资源使用情况，删除不必要的配置 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.9 ND_HARDWARE_SEND_NORESOURCE

日志内容	Failed to send the ND entry to the driver because the device resources are insufficient. IPv6 address=[STRING]; VPN instance name=[STRING]; VPN instance index=[UINT16]; Interface=[STRING].
日志含义	设备资源不足导致ND表项下发到硬件失败
参数解释	$1：ND表项的IPv6地址 $2：ND表项的VPN实例名称。如果是公网内的日志信息，则显示为Public $3：ND表项的VPN实例索引。如果是公网内的日志信息，则显示为0 $4：ND表项所对应的出接口名称
日志等级	4 (Warning)
举例	ND/4/ND_HARDWARE_SEND_NORESOURCE: Failed to send the ND entry to the driver because the device resources are insufficient. IPv6 address=1::1; VPN instance name=vpn1; VPN instance index=1; Interface=GigabitEthernet1/0/1.
对系统的影响	影响正常的报文转发，导致业务不通
日志产生原因	使用**ipv6 nd hardware log enable**命令开启ND表项下发硬件日志功能后，由于硬件资源不足导致ND表项无法成功下发到硬件
处理建议	**1.** 请检查设备资源使用情况，删除不必要的配置 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.10 ND_HOST_IP_CONFLICT

日志内容	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface [STRING].
日志含义	接口收到主机ND报文中的源IPv6地址与其他接口连接的主机的IPv6地址冲突
参数解释	$1：IPv6地址 $2：接口名称 $3：接口名称
日志等级	4 (Warning)
举例	ND/4/ND_HOST_IP_CONFLICT: The host 2::2 connected to interface GigabitEthernet1/0/1 cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface GigabitEthernet1/0/1.
对系统的影响	可能会造成用户业务或者流量中断
日志产生原因	产生此日志的可能原因包括： • 本设备下连接的不同主机配置了相同的 IPv6 地址 • 网络中存在伪造源 IPv6 地址的 ND 攻击
处理建议	**1.** 根据日志信息，检查对应接口下连接的主机配置，调整冲突主机的 IPv6 地址 **2.** 检查发送该 ND 报文的主机的合法性，如果该主机非法，则需要断开该主机网络 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.11 ND_LIPCQUE_ALERT

日志内容	The number of ND entries in the ND_LIPC queue has reached [UINT32]. Please check the network environment.
日志含义	在队列中等待主控板向其他板同步的ND表项的个数达到队列容量的50%或80%
参数解释	$1：在队列中等待主控板向其他板同步的ND表项的个数
日志等级	4 (Warning)
举例	ND/4/ND_LIPCQUE_ALERT: The number of ND entries in the ND_LIPC queue has reached 65. Please check the network environment.
对系统的影响	在队列中等待主控板向其他板同步的ND表项个数达到队列容量的上限时会丢弃ND表项，可能导致部分正常的ND报文被丢弃，造成流量转发不通
日志产生原因	在队列中等待主控板向其他板同步的ND表项的个数达到队列容量的50%或80%时会触发告警，系统将每隔60秒输出一次日志信息进行提示，可能原因包括： • 网络中可能存在环路 • 网络中可能存在 ND 攻击
处理建议	**1.** 配置 STP，检查网络中是否存在环路 **2.** 通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.12 ND_LOCALPROXY_ENABLE_FAILED

日志内容	Failed to enable local ND proxy on interface [STRING].
日志含义	使能本地ND Proxy功能失败
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	ND/4/ND_LOCALPROXY_ENABLE_FAILED: Failed to enable local ND proxy on interface Vlan-interface 1.
对系统的影响	可能会造成用户业务或者流量中断
日志产生原因	产生此日志的可能原因包括： • 接口上使能本地 ND Proxy 功能失败 • 主控板的接口上使能本地 ND Proxy 功能成功、非主控板的接口上使能本地 ND Proxy 功能失败，则在对应的接口板上打印该日志信息
处理建议	**1.** 检查设备相应单板是否支持配置本地 ND Proxy 功能 **2.** 检查设备的硬件资源是否充足，删除不必要的配置 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.13 ND_PKTQUE_ALERT

日志内容	The current size of the ND_PKT queue has reached [UINT32]. Please check the network environment.
日志含义	当前ND报文队列长度超过4096
参数解释	$1: ND报文队列长度
日志等级	4 (Warning)
举例	ND/4/ND_PKTQUE_ALERT: The current size of the ND_PKT queue has reached 4096. Please check the network environment.
对系统的影响	当上送CPU的ND报文队列长度达到队列容量上限时会丢弃ND报文，造成流量转发不通
日志产生原因	当上送CPU的ND报文队列长度超过4096时，系统将每隔60秒输出一次日志信息进行提示
处理建议	**1.** 检查接口上收到的 ND 报文是否正常，如果收到异常的 ND 报文，则通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.14 ND_MAC_CHECK

日志内容	Packet received on interface [STRING] was dropped because source MAC [STRING] was inconsistent with link-layer address [STRING].
日志含义	ND报文因源MAC地址和以太网数据帧首部的源MAC地址不一致而被丢弃
参数解释	$1：接收ND报文的接口名称 $2：ND报文中的源MAC地址 $3：ND报文的链路层源MAC地址
日志等级	6 (Informational)
举例	ND/6/ND_MAC_CHECK: Packet received on interface Ethernet2/0/2 was dropped because source MAC 0002-0002-0001 was inconsistent with link-layer address 0002-0002-0002.
对系统的影响	无
日志产生原因	执行**ipv6 nd mac-check enable**命令开启ND协议报文源MAC地址一致性检查功能，并执行**ipv6 nd check log enable**命令开启ND日志信息功能后，接收到的ND协议报文中的源MAC地址和源链路层选项地址中的MAC地址不一致
处理建议	1. 检查链路层源 MAC 地址对应主机的合法性，如果该主机非法，则需要断开该主机网络 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.15 ND_NETWORKROUTE_DUPLICATE

日志内容	Prefix [STRING] of the IPv6 ND network route matches different ports: [STRING] and [STRING].
日志含义	根据不同ND表项生成的网段路由冲突
参数解释	$1：IPv6地址前缀 $2：接口名称 $3：接口名称
日志等级	5 (Notification)
举例	ND/5/ND_NETWORKROUTE_DUPLICATE: Prefix 120::/70 of the IPv6 ND network route matches different ports: GigabitEthernet1/0/1 and GigabitEthernet1/0/2.
对系统的影响	可能造成流量转发不同，影响正常业务
日志产生原因	使用**ipv6 nd route-direct prefix convert-length**命令配置匹配指定IPv6前缀的ND表项生成网段路由的前缀长度后，如果根据不同的ND表项（与邻居相连的二层端口不同、但是与邻居相连的接口所属的VLAN相同）生成相同的网段路由，则输出本日志
处理建议	1. 据网络规划和业务部署，修改指定接口的网络配置 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.16 ND_RAGUARD_DROP

日志内容	Dropped RA messages with the source IPv6 address [STRING] on interface [STRING]. [STRING] messages dropped in total on the interface.
日志含义	RA报文被丢弃
参数解释	$1：被丢弃报文的源IPv6地址 $2：丢弃报文的端口名 $3：该端口已丢弃的报文总数
日志等级	4 (Warning)
举例	ND/4/ND_RAGUARD_DROP: Dropped RA messages with the source IPv6 address FE80::20 on interface GigabitEthernet1/0/1. 20 RA messages dropped in total on the interface.
对系统的影响	网络中可能存在RA报文欺骗攻击，影响设备正常运行
日志产生原因	RA Guard检测到非法RA报文，网络中可能存在RA报文欺骗攻击
处理建议	**1.** 检查发送该 RA 报文的设备是否合法，如果该设备非法，则需要断开该设备的网络 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.17 ND_RATE_EXCEEDED

日志内容	The ND packet rate ([UINT32] pps) exceeded the rate limit ([UINT32] pps) on interface [STRING] in most recent [UINT32] seconds.
日志含义	ND报文速率超过了接口限速速率
参数解释	$1：ND报文速率 $2：ND报文限速速率 $3：接口名称 $4：间隔时间
日志等级	4 (Warning)
举例	ND/4/ND_RATE_EXCEEDED: The ND packet rate (100 pps) exceeded the rate limit (80 pps) on interface GigabitEthernet1/0/1 in most recent 10 seconds.
对系统的影响	接口上接收ND报文的速率超过了ND限速速率时会被丢弃，可能影响正常的ND学习与应答，造成流量转发不通
日志产生原因	在此前的一段时间内，接口上接收ND报文速率超过了接口的ND报文限速值
处理建议	**1.** 检查接口上收到的 ND 报文是否正常 o 如果收到的ND报文均合理，则执行 **ipv6 nd rate-limit**命令将指定接口上ND报文限速速率的数值调大 o 如果检查到收到异常的 ND 报文，请执行步骤 2 **2.** 通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.18 ND_RATELIMIT_NOTSUPPORT

日志内容	形式一： ND packet rate limit is not support on slot [INT32]. 形式二： ND packet rate limit is not support on chassis [INT32] slot [INT32].
日志含义	不支持ND报文限速功能
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	6 (Informational)
举例	ND/6/ND_RATELIMIT_NOTSUPPORT: ND packet rate limit is not support on slot 2.
对系统的影响	无
日志产生原因	形式一： 指定的slot上不支持ND报文限速功能 形式二： 指定chassis内slot不支持ND报文限速功能
处理建议	无需处理

102.19 ND_SET_PORT_TRUST_NORESOURCE

日志内容	Not enough resources to complete the operation.
日志含义	资源不足，下发端口规则失败
参数解释	无
日志等级	6 (Informational)
举例	ND/6/ND_SET_PORT_TRUST_NORESOURCE: Not enough resources to complete the operation.
对系统的影响	驱动资源不足，影响业务正常运行
日志产生原因	下发端口规则过程中驱动资源不足
处理建议	**1.** 释放设备驱动资源，重新下发 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.20 ND_SET_VLAN_REDIRECT_NORESOURCE

日志内容	Not enough resources to complete the operation.
日志含义	资源不足，下发VLAN规则失败
参数解释	无
日志等级	6 (Informational)
举例	ND/6/ND_SET_VLAN_REDIRECT_NORESOURCE: Not enough resources to complete the operation.
对系统的影响	驱动资源不足，影响业务正常运行
日志产生原因	下发VLAN规则过程中驱动资源不足
处理建议	**1.** 释放设备驱动资源，重新下发 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.21 ND_SNOOPING_LEARN_ALARM

日志内容	The total number of ND snooping entries learned in all VLANs reached or exceeded the alarm threshold.
日志含义	所有VLAN学习的ND Snooping表项总数达到或超过告警阈值
参数解释	无
日志等级	4 (Warning)
举例	ND/4/ND_SNOOPING_LEARN_ALARM: The total number of ND snooping entries learned in all VLANs reached or exceeded the alarm threshold.
对系统的影响	设备可能无法再学习到新的ND Snooping表项，影响业务正常运行
日志产生原因	所有VLAN学习的ND Snooping表项总数达到或超过告警阈值，网络中可能存在ND报文攻击
处理建议	**1.** 通过抓包的方式检查网络中是否存在 ND 攻击，查找攻击源 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.22 ND_SNOOPING_LEARN_ALARM_RECOVER

日志内容	The total number of ND snooping entries learned in all VLANs dropped below the alarm threshold.
日志含义	所有VLAN学习的ND Snooping表项总数降低到告警阈值以下
参数解释	无
日志等级	4 (Warning)
举例	ND/4/ND_SNOOPING_LEARN_ALARM_RECOVER: The total number of ND snooping entries learned in all VLANs dropped below the alarm threshold.
对系统的影响	无
日志产生原因	所有VLAN学习的总的ND Snooping表项数降低到告警阈值以下
处理建议	无需处理

102.23 ND_SOURCE_IP

日志内容	An attack from IP [STRING] was detected on interface [STRING].
日志含义	检测到源IPv6地址固定的ND攻击
参数解释	$1：收到的ND攻击报文中的源IPv6地址 $2：收到源IPv6地址固定的ND报文的接口名称
日志等级	6 (Information)
举例	ND/6/ND_SOURCE_IP: An attack from IP 1001::1 was detected on interface GE1/0/1.
对系统的影响	设备处理大量源IPv6地址固定的ND报文会造成CPU繁忙，影响正常的业务处理
日志产生原因	在固定的时间（5秒）内，某个接口收到的同一源IPv6地址的ND报文个数超过检测阈值
处理建议	1. 执行 **display ipv6 nd source-ip**命令，查看检测到的源IPv6 地址固定的ND攻击检测表项，根据网络规划和业务部署，确认表项中该地址是否为用户信任的IPv6地址 o 如果是，则执行 **ipv6 nd source-ip exclude-ip**命令配置该地址为ND攻击检测的保护IPv6 地址 o 如果不是，则通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 2. 若问题仍未解决，请收集配置文件和日志信息，并联系技术支持

102.24 ND_SOURCE_MAC

日志内容	An attack from MAC [STRING] was detected on interface [STRING].
日志含义	检测到源MAC地址固定的ND攻击
参数解释	$1：收到的ND攻击报文中的源MAC地址 $2：收到源MAC地址固定的ND报文的接口名称
日志等级	6 (Information)
举例	ND/6/ND_SOURCE_MAC: An attack from MAC 0001-0001-0001 was detected on interface GE1/0/1.
对系统的影响	设备处理大量源MAC地址固定的ND报文会造成CPU繁忙，影响正常的业务处理
日志产生原因	在固定的时间（5秒）内，某个接口收到的同一源MAC地址的ND报文个数超过检测阈值
处理建议	1. 执行 **display ipv6 nd source-mac**命令，查看检测到的源MAC地址固定的ND攻击检测表项，根据网络规划和业务部署，确认表项中该地址是否为用户信任的MAC地址 o 如果是，则执行 **ipv6 nd source-mac exclude-mac**命令配置该地址为ND攻击检测的保护MAC地址 o 如果不是，则通过抓包的方式检查网络中是否存在 ND 报文攻击，查找攻击源 2. 若问题仍未解决，请收集配置文件和日志信息，并联系技术支持

102.25 ND_SUPPR_ALARM_CLEAR

日志内容	The number of ND suppression entries dropped below the threshold. Threshold=[UINT32], Number of ND suppression entries=[UINT32])
日志含义	ND泛洪抑制表项的数量降到了阈值以下
参数解释	$1：ND泛洪抑制表项的阈值 $2：ND泛洪抑制表项的数量
日志等级	5 (Notification)
举例	ND/5/ND_SUPPR_ALARM_CLEAR: The number of ND suppression entries dropped below the threshold. Threshold=100; Number of ND Suppression entries=59.
对系统的影响	无
日志产生原因	ND泛洪抑制表项的数量恢复到阈值的60%之下
处理建议	无需处理

102.26 ND_SUPPR_THRESHOLD_EXCEED

日志内容	The number of ND suppression entries exceeded the threshold. Threshold=[UINT32]; Number of ND suppression entries=[UINT32].
日志含义	ND泛洪抑制表项的数量超过了阈值
参数解释	$1：ND泛洪抑制表项的阈值

	$2：ND泛洪抑制表项的数量
日志等级	4 (Warning)
举例	ND/4/ND_SUPPR_THRESHOLD_EXCEED: The number of ND suppression entries exceeded the threshold. Threshold=100; Number of ND suppression entries=80.
对系统的影响	不能学习到新的ND泛洪抑制表项，可能导致设备泛洪ND报文，增加网络中组播报文的数量，影响设备运行的性能
日志产生原因	ND泛洪抑制表项的数量大于阈值的80%
处理建议	**1.** 执行 **display ipv6 nd suppression xconnect-group**命令，查看ND泛洪抑制表项 **2.** 根据网络规划和业务部署，检查设备上的 ND 泛洪抑制表项是否是用户必需的 o 如果 ND 泛洪抑制表项是用户必需的，请执行步骤 3 o 如果ND泛洪抑制表项不是用户必需的，执行 **reset ipv6 nd suppression xconnect-group**命令清除ND泛洪抑制表项 **3.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.27 ND_USER_DUPLICATE_IPV6ADDR

日志内容	Detected a user IPv6 address conflict. New user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] and old user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] were using the same IPv6 address [IPV6ADDR].
日志含义	检测到终端用户间IPv6地址冲突
参数解释	$1：新用户的MAC地址 $2：新用户所在的外层VLAN $3：新用户所在的内层VLAN $4：连接新用户的接口名称 $5：旧用户的MAC地址 $6：旧用户所在的外层VLAN $7：旧用户所在的内层VLAN $8：连接旧用户的接口名称 $9：终端用户的IPv6地址
日志等级	6 (Informational)
举例	ND/6/ND_USER_DUPLICATE_IPV6ADDR: Detected a user IPv6 address conflict. New user (MAC 0010-2100-01e1, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 and old user (MAC 0120-1e00-0102, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 were using the same IPv6 address 10::1.
对系统的影响	网络中可能存在冲突的IPv6地址，可能会造成用户业务或者流量中断等故障
日志产生原因	使用**ipv6 nd user-ip-conflict record enable**命令开启ND记录终端用户间IPv6地址冲突功能后，如果设备检测到冲突，则输出本日志
处理建议	**1.** 排查所有终端用户的 IPv6 地址，调整冲突用户的 IPv6 地址，解决 IPv6 地址冲突问题 **2.** 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.28 ND_USER_MOVE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) moved to another interface. Before user move: interface [STRING], SVLAN [STRING], CVLAN [STRING]. After user move: interface [STRING], SVLAN [STRING], CVLAN [STRING].
日志含义	检测到用户进行了端口迁移
参数解释	$1：迁移用户的IPv6地址 $2：迁移用户的MAC地址 $3：迁移前接口名称 $4：迁移前用户所在的外层VLAN $5：迁移前用户所在的内层VLAN $6：迁移后接口名称 $7：迁移后用户所在的外层VLAN $8：迁移后用户所在的内层VLAN
日志等级	6 (Informational)
举例	ND/6/ND_USER_MOVE: Detected a user (IPv6 address 10::1, MAC address 0010-2100-01e1) moved to another interface. Before user move: interface GigabitEthernet1/0/1, SVLAN 100, CVLAN 20. After user move: interface GigabitEthernet1/0/2, SVLAN 100, CVLAN 10.
对系统的影响	可能造成用户业务中断。当发生大量用户迁移操作时，可能会降低设备性能
日志产生原因	使用**ipv6 nd user-move record enable**命令开启ND记录终端用户端口迁移功能后，终端用户在接口间迁移，则输出本日志
处理建议	1. 使用 **display ipv6 nd user-move record命令** 查看终端用户端口迁移表项信息，确认迁移是否合理 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

102.29 ND_USER_OFFLINE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) was offline from interface [STRING].
日志含义	检测到终端用户下线
参数解释	$1：下线用户的IPv6地址 $2：下线用户的MAC地址 $3：连接下线用户的接口名称
日志等级	6 (Informational)
举例	ND/6/ND_USER_OFFLINE: Detected a user (IPv6 address 10::1, MAC address 0010-2100-01e1) was offline from interface GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	使用**ipv6 nd online-offline-log enable**命令开启ND输出终端用户上下线日志功能后，如果设备检测到有终端用户下线，则输出本日志
处理建议	无需处理

102.30 ND_USER_ONLINE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) was online on interface [STRING].
日志含义	检测到终端用户上线
参数解释	$1：上线用户的IPv6地址 $2：上线用户的MAC地址 $3：连接上线用户的接口名称
日志等级	6 (Informational)
举例	ND/6/ND_USER_ONLINE: Detected a user (IPv6 address 10::1, MAC address 0010-2100-01e1) was online on interface GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	使用**ipv6 nd online-offline-log enable**命令开启ND输出终端用户上下线日志功能后，如果设备检测到有终端用户上线，则输出本日志
处理建议	1. 根据日志信息，检查上线的用户是否是合法用户，如果该用户非法，则需要断开与该用户的网络连接 2. 若问题仍未解决，请收集配置文件、日志信息、告警信息，并联系技术支持人员

103 NETCONF

本节介绍 NETCONF 模块输出的日志信息。

103.1 CLI

日志内容	User ([STRING], [STRING][STRING]) performed an CLI operation: [STRING] operation result=[STRING][STRING]
日志含义	用户下发CLI操作后，操作的执行结果
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 CON0 $3：NETCONF会话的编号（Web和RESTful类型会话无此字段） $4：NETCONF请求中的message-id（Web和RESTful类型会话无此字段） $5：CLI的执行成功，取值为Succeeded；CLI的执行失败，取值为Failed $6：CLI执行失败的原因（仅已知失败原因的情况显示该信息）
日志等级	6 (Informational)
举例	XMLSOAP/6/CLI: -MDC=1; User (test, 169.254.5.222, session ID=1) performed an CLI operation:message ID=101, operation result=Succeeded.
对系统的影响	与CLI请求包含的命令行内容有关
日志产生原因	用户执行CLI操作
处理建议	无需处理

103.2 EDIT-CONFIG

日志内容	User ([STRING], [STRING], session ID [UINT]) performed an edit-config operation: message ID=[STRING], operation result=[STRING].
日志含义	用户下发edit-config操作后，操作的执行结果
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 console0 $3：NETCONF会话的编号，没有则不显示 $4：NETCONF请求中的message-id，没有则不显示 $5：操作执行结果，成功时取值为Succeeded，失败时取值为Failed
日志等级	6 (Informational)
举例	XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.56.1, session ID 1) performed an edit-config operation: message ID=101, operation result=Succeeded.
对系统的影响	与edit-config请求操作的表项有关
日志产生原因	用户执行edit-config操作
处理建议	• 操作执行成功时，无需处理 • 操作执行失败时，请检查 edit-config 操作是否与设备当前配置冲突；或者收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

日志内容	User ([STRING], [STRING][STRING])[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. No attributes. 或 User ([STRING], [STRING],[STRING]),[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. Attributes: [STRING].
日志含义	用户下发NETCONF操作后，该操作中的每个请求行操作及操作结果
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 console0 $3：NETCONF会话的编号，没有则不显示 $4：NETCONF请求中的message-id，没有则不显示 $5：NETCONF行操作名称 $6：模块和表名称 $7：索引信息。仅下发索引时显示，用括号包围；如果日志中包含多个索引，则索引之间用逗号分隔 $8：NETCONF行操作的处理结果，NETCONF行操作执行成功时，取值为Succeeded；执行失败时，取值为Failed $9：属性列信息。仅配置属性列时显示该信息
日志等级	6 (Informational)
举例	XMLSOAP/6/EDIT-CONFIG: -MDC=1; User (test, 192.168.200.220, session ID 1), message ID=101, operation=merge DHCP/DHCPServerPoolStatic (PoolIndex=1, Ipv4Address=1.1.1.1), result=Failed. Attributes: CID="aaaaa", HType=1.
对系统的影响	与edit-config请求操作的表项有关
日志产生原因	按NETCONF行操作输出日志，用户下发一次NETCONF操作，设备输出该操作中每个请求行操作的日志 仅action和set操作支持输出该日志
处理建议	无需处理

103.3 EDIT_CONFIG_CLI

日志内容	User ([STRING], [STRING], session ID [UINT16]), message ID=[UINT16], row index=[UINT16], command=[STRING]. [STRING]
日志含义	用户下发edit-config操作后，该操作对应的命令行
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 console0 $3：NETCONF会话的编号，没有则不显示 $4：NETCONF请求报文中的message-id，没有则不显示 $5：NETCONF报文中的行索引 $6：NETCONF报文被转化后的命令行 $7：NETCONF行操作下发失败时的错误提示“Configuration failed.”，下发成功则不显示
日志等级	6 (Informational)
举例	XMLSOAP/6/EDIT_CONFIG_CLI: User (test, 192.168.100.20, session ID 1), message ID=100, row index=1, command=port trunk pvid vlan 100.
对系统的影响	无
日志产生原因	用户下发一次NETCONF操作请求后，设备将该NETCONF请求报文转化为对应的命令行，并通过日志记录该命令行以及执行结果 仅action和edit-config操作支持输出该日志
处理建议	无需处理

103.4 NETCONF_CONFIG_LOG

日志内容	User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation=[STRING]. The operation results in the following configuration changes: [STRING]
日志含义	用户下发edit-config操作后，导致命令配置的变化
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 CON0 $3：NETCONF会话的编号 $4：NETCONF请求中的message-id $5：edit-config操作的配置选项，取值包括：merge、create、replace、remove、delete $6：本次操作导致的配置变化
日志等级	6 (Informational)
举例	XMLAGENT/6/NETCONF_CONFIG_LOG: -MDC=1; User (test, 192.168.100.20, session ID 1) performed an edit-config operation: message ID=6, operation=merge. The operation results in the following configuration changes: +# +interface Vlan-interface6
对系统的影响	无
日志产生原因	客户端与设备协商“urn:h3c:params:netconf:capability:h3c-netconf2cli-sysloglog:1.0”能力后，通过edit-config操作给设备下发配置，设备记录配置的变化
处理建议	无

103.5 NETCONF_MSG_DEL

日志内容	A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
日志含义	NETCONF请求报文被丢弃
参数解释	无
日志等级	7 (Debug)
举例	NETCONF/7/NETCONF_MSG_DEL: A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
对系统的影响	无
日志产生原因	来自NETCONF over SSH客户端或XML视图的NETCONF请求报文由于其大小超过设备支持的上限而被丢弃
处理建议	1. 减小发往设备的单个 NETCONF 请求报文的大小，例如删除报文中的空格、换行、制表符等占位字符 2. 如果报文仍然过大，可以拆分 NETCONF 请求并分别封装后再发送给设备，建议收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

103.6 THREAD

日志内容	Maximum number of NETCONF threads already reached.
日志含义	NETCONF线程数达到上限
参数解释	无
日志等级	3 (Error)
举例	XMLCFG/3/THREAD: -MDC=1; Maximum number of NETCONF threads already reached.
对系统的影响	无法再接受新的NETCONF SSH会话 无法再接受新的NETCONF SOAP和RESTful请求 WEB功能不可用
日志产生原因	NETCONF线程数达到上限
处理建议	NETCONF线程数达到上限，请稍后重试

104 NQA

本节介绍 NQA 模块输出的日志信息。

104.1 NQA_ENTRY_PROBE_RESULT

日志内容	Reaction entry [STRING] of NQA entry admin-name [STRING] operation-tag [STRING]: [STRING].
日志含义	NQA测试组的探测结果
参数解释	$1：阈值告警组编号 $2：NQA测试组的管理员名称 $3：测试操作的标签 $4：探测结果，取值为： • Probe-pass：表示探测成功 • Probe-fail：表示探测失败
日志等级	6 (Informational)
举例	NQA/6/NQA_ENTRY_PROBE_RESULT: Reaction entry 1 of NQA entry admin-name 1 operation-tag 1: Probe-pass.
对系统的影响	对系统无影响
日志产生原因	• 配置错误。探测失败阈值告警组配置的阈值太小 • 网络质量劣化，导致探测失败
处理建议	1. 执行 **display current-configuration | include probe-fail**命令查看探测失败阈值告警组配置。可根据维护经验和期望的网络状态，使用命令 **reaction checked-element probe-fail**命令修改探测失败阈值告警组配置的阈值 2. 登录 NQA server 端，如果 NQA server 运行异常，请修复或重启 NQA server 3. 在设备和 NQA server 上分别执行 Ping 操作查看网络丢包和时延，如果丢包和时延超过期望范围，请定位丢包和时延过大问题 4. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

104.2 NQA_LOG_UNREACHABLE

日志内容	Server [STRING] unreachable.
日志含义	NQA服务器路由不可达
参数解释	$1：NQA服务器的IP地址
日志等级	6 (Informational)
举例	NQA/6/NQA_LOG_UNREACHABLE: Server 192.168.30.117 unreachable.
对系统的影响	对系统无影响
日志产生原因	NQA客户端检测到NQA服务器路由不可达
处理建议	1. 根据日志信息中携带的IP地址，确认NQA服务器的IP地址是否正确，如果配置错误，请在NQA测试视图下，执行 **destination**命令重新配置NQA服务器的IP地址 2. 执行 **display ip routing-table**命令查看是否有去往NQA服务器的路由，如果没有去往NQA服务器的路由，可执行 **ip route-static**命令用来配置静态路由，或者通过动态路由协议生成一条路由 3. 执行 **display interface**命令查看去往NQA服务器路由出接口的状态，如果接口状态为down，请先解决接口故障问题 4. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

104.3 NQA_START_FAILURE

日志内容	NQA entry ([STRING]-[STRING]): [STRING]
日志含义	NQA测试下发驱动执行时失败
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签 $3：NQA测试下发驱动执行时失败，失败的原因包括： • Operation failed due to configuration conflicts：配置冲突导致下发驱动失败 • Operation failed because the driver was not ready to perform the operation：驱动未准备就绪导致下发驱动失败 • Operation not supported：驱动不支持该操作 • Not enough resources to complete the operation：资源不足导致下发驱动失败 • Operation failed due to an unknown error：其他情况导致下发驱动操作失败
日志等级	6 (Informational)
举例	NQA/6/NQA_START_FAILURE: NQA entry (1-1): Operation failed due to configuration conflicts.
对系统的影响	对系统无影响
日志产生原因	• 配置冲突导致下发驱动失败 • 驱动未准备就绪导致下发驱动失败 • 驱动不支持该操作 • 资源不足导致下发驱动失败 • 其他情况导致下发驱动操作失败
处理建议	• 如果NQA测试下发驱动执行时的失败原因为Operation failed due to configuration conflicts，请进入NQA测试组视图，执行 **display this**命令，查看NQA测试组的配置，请参照NQA配置指导要求配置后，重新启动测试 • 如果 NQA 测试下发驱动执行时的失败原因为其它取值，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

104.4 NQA_TWAMP_LIGHT_PACKET_INVALID

日志内容	NQA TWAMP Light test session [UINT32] index [UINT32]: The number of packets captured for statistics collection is invalid.
日志含义	NQA TWAMP Light在统计周期内统计到的探测报文数无效
参数解释	$1：测试会话ID $2：统计数据的序列号
日志等级	6 (Informational)
举例	NQA/6/NQA_TWAMP_LIGHT_PACKET_INVALID: NQA TWAMP Light test session 1 index 7: The number of packets captured for statistics collection is invalid.
对系统的影响	对系统无影响
日志产生原因	配置的统计周期小于探测报文的发送周期，导致统计的探测报文数异常，本次探测统计结果不计入统计计数
处理建议	请先TWAMP-light-sender视图下使用**stop**命令停止该TWAMP-light测试。然后重新使用**start**命令启动TWAMP-light测试，**start**命令中要求：**monitor-time**参数的取值>**statistics-interval**参数的取值>**tx-interval**参数的取值

104.5 NQA_TWAMP_LIGHT_REACTION

日志内容	NQA TWAMP Light test session [UINT32] reaction entry [UINT32]: Detected continual violation of the [STRING] [STRING] threshold for a threshold violation monitor time of [UINT32] ms.
日志含义	监测到NQA TWAMP-light测试的探测结果持续大于等于阈值告警的上限阈值或者从大于阈值告警的下限阈值恢复到小于等于该下限阈值
参数解释	$1：测试会话的ID $2：阈值告警组编号 $3：阈值告警类型，取值包括： o two-way delay：双向时延阈值告警 o two-way loss：双向丢包率阈值告警 o two-way jitter：双向抖动阈值告警 $4：阈值动作，取值包括： o upper：大于等于阈值告警的上限阈值 o lower：小于等于阈值告警的下限阈值 $5：日志告警周期
日志等级	6 (Informational)
举例	NQA/6/NQA_TWAMP_LIGHT_REACTION: NQA TWAMP Light test session 1 reaction entry 1: Detected continual violation of the two-way loss upper threshold for a threshold violation monitor time of 2000 ms.
对系统的影响	对系统无影响
日志产生原因	监测NQA TWAMP-light测试的探测结果，从测试统计的第一个结果大于等于阈值告警的上限阈值或者从大于阈值告警的下限阈值恢复到小于等于该下限阈值开始计时，若在监控时间内测试结果持续不变，打印该日志
处理建议	无需处理

104.6 NQA_TWAMP_LIGHT_START_FAILURE

日志内容	形式一： NQA TWAMP Light test session [UINT32]: Failed to start the test session. Reason: Invalid configuration. 形式二： NQA TWAMP Light test session [UINT32]: Failed to start the test session. Reason: Not enough resources.
日志含义	TWAMP-light Responder端启动TWAMP LIGHT测试失败
参数解释	$1：测试会话的ID
日志等级	6 (Informational)
举例	NQAS/6/NQA_TWAMP_LIGHT_START_FAILURE: NQA TWAMP Light test session 1: Failed to start the test session. Reason: Invalid configuration.
对系统的影响	对系统无影响
日志产生原因	启动TWAMP-light Responder端的测试会话失败，失败原因可能为： • Invalid configuration：非法配置 • Not enough resources：资源不足
处理建议	• 如果失败原因为Invalid configuration，则表示 **test-session**命令TWAMP-light Responder端缺少参数必配项，请根据当前网络环境判断参数的必配项，重新配置 **test-session**命令 • 如果失败原因为Not enough resources，请尝试释放内存来解决问题。例如：执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源 • 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

105 NSS

本节介绍 NSS（Session-based NetStream，基于会话的 NetStream）模块输出的日志信息。

105.1 NSS_ENABLE_FAIL

日志内容	Failed to apply the command **session-based netstream enable** to the driver. Reason: [STRING].
日志含义	基于会话的NetStream功能下发驱动失败
参数解释	$1：失败原因 • The operation is not supported：操作不支持 • The operation conflicts with existing configurations：与已存在的配置冲突
日志等级	4 (Warning)
举例	NSS/4/NSS_ENABLE_FAIL: Failed to apply the command **session-based netstream enable** to the driver. Reason: The operation is not supported.
对系统的影响	基于会话的NetStream功能无法正常使用
日志产生原因	**session-based netstream enable**命令下发驱动失败
处理建议	1. 检查 FPGA 子卡是否在位，并重新下发命令 2. 检查设备上是否配置了 NetStream 或 sFlow（基于会话的 NetStream、NetStream 和 sFlow 三者间存在冲突，同一时间设备仅支持运行其中一种功能）

105.2 NSS_SESSION_TIMEOUT_FAIL

日志内容	Failed to apply the command **session-based netstream session-timeout** to the driver. Reason: [STRING].
日志含义	会话不活跃老化时间功能下发驱动失败
参数解释	$1：失败原因 The operation is not supported：操作不支持
日志等级	4 (Warning)
举例	NSS/4/NSS_SESSION_TIMEOUT_FAIL: Failed to apply the command **session-based netstream session-timeout** to the driver. Reason: The operation is not supported.
对系统的影响	无法配置会话不活跃的老化时间
日志产生原因	**session-based netstream session-timeout**命令下发驱动失败
处理建议	检查FPGA子卡是否在位，并重新下发命令

106 NTP

本节介绍 NTP 模块输出的日志信息。

106.1 NTP_CLOCK_CHANGE

日志内容	System clock changed from [STRING] to [STRING], the NTP server's IP address is [STRING].
日志含义	设备和NTP服务器进行时间同步成功
参数解释	$1：起始时间 $2：同步后时间 $3：IP地址
日志等级	5 (Notification)
举例	NTP/5/NTP_CLOCK_CHANGE: System clock changed from 02:12:58 12/28/2012 to 02:29:12 12/28/2012, the NTP server's IP address is 192.168.30.116.
对系统的影响	对系统无影响
日志产生原因	NTP客户端的时间已经和NTP服务器同步
处理建议	无需处理

106.2 NTP_LEAP_CHANGE

日志内容	System Leap Indicator changed from [UINT32] to [UINT32] after clock update.
日志含义	设备发生闰秒跳变
参数解释	$1：起始闰秒标识，取值可能为： • 01：表示一天中的最后一分钟有 61 秒 • 10：表示一天中的最后一分钟有 59 秒 $2：当前闰秒标识，取值可能为： • 01：表示一天中的最后一分钟有 61 秒 • 10：表示一天中的最后一分钟有 59 秒
日志等级	5 (Notification)
举例	NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 00 to 01 after clock update.
对系统的影响	设备会在打印该日志的当天最后一分钟时间跳变1秒钟
日志产生原因	• NTP 闰秒标识是一个二位码，预报当天最近的分钟里要被插入的闰秒秒数 • 比特值在闰秒秒数插入当天 23:59 前或次日 00:00 后设置。因此秒数会比插入当天的时间提前或推后 1 秒 • 系统的闰秒标识发生变化
处理建议	请根据国际时间组织（国际计量局，BIPM）定期公布的TAI和UTC时间的偏差值来判断在打印该日志的当天是否有必要进行闰秒跳变： • 如果需要闰秒跳变，且跳变的值是正确的，则无需处理 • 如果不需要闰秒跳变，则等待下一次时间同步。如果下一次时间同步后，设备的系统时间和国际标准时间相同，则无需处理；如果下一次时间同步后，设备的系统时间和国际标准时间不同，则继续检查时钟源是否也发生了闰秒跳变。如果时钟源发生了错误的闰秒跳变，请重新校准时钟源的时间

106.3 NTP_SOURCE_CHANGE

日志内容	NTP server's IP address changed from [STRING] to [STRING].
日志含义	NTP时钟源发生了变化
参数解释	$1：起始时钟源的IP地址 $2：新时钟源的IP地址
日志等级	5 (Notification)
举例	NTP/5/NTP_SOURCE_CHANGE: NTP server's IP address changed from 1.1.1.1 to 1.1.1.2.
对系统的影响	对系统无影响
日志产生原因	设备选择的NTP时钟源发生了变化

处理建议	• 正常处理流程，无需处理
	• 您也可以进一步定位时钟源切换的原因，例如：
	  ○ Ping 原时钟源的 IP 地址，查看原时钟源是否路由可达。如果路由不可达，先解决路由问题
	  ○ 登录原时钟源，查看原时钟源上的时钟是否精准。如果不精准，需要调整原时钟源上的时间
	  ○ 登录原时钟源，查看原时钟源上的 NTP 配置是否正确。如果不正确，请参照 NTP 配置手册进行修改

106.4 NTP_SOURCE_LOST

日志内容	Lost synchronization with NTP server with IP address [STRING].
日志含义	设备和时钟源失去同步
参数解释	$1：IP 地址
日志等级	5 (Notification)
举例	NTP/5/NTP_SOURCE_LOST: Lost synchronization with NTP server with IP address 1.1.1.1.
对系统的影响	可能会影响设备时钟的准确度
日志产生原因	NTP交互中的时钟源处于未同步状态或不可达，而这个时候又没有其它候选同步源时，设备生成此日志
处理建议	1. Ping 原时钟源的 IP 地址，查看原时钟源是否路由可达。如果路由不可达，先解决路由问题 2. 登录原时钟源，查看原时钟源上的时钟是否精准。如果不精准，需要调整原时钟源上的时间 3. 登录原时钟源，查看原时钟源上的 NTP 配置是否正确。如果不正确，请参照 NTP 配置手册进行修改 4. 根据采用的时钟同步模式选用对应的命令行配置新的时钟源

106.5 NTP_STRATUM_CHANGE

日志内容	System stratum changed from [UINT32] to [UINT32] after clock update.
日志含义	设备的NTP时钟层级发生了变化
参数解释	$1：起始层 $2：当前层
日志等级	5 (Notification)
举例	NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 6 to 5 after clock update.
对系统的影响	可能会影响设备和下游设备之间的时钟同步
日志产生原因	设备时钟层数发生变化的原因，可能为： • 时钟源自身层级变化，例如系统刚开始选择到时钟源 • 同步过程中发生同步时钟源切换，时钟源变化导致时钟层级发生了变化 实际网络中，通常将从权威时钟（如原子时钟）获得时间同步的NTP服务器的层数设置为1，并将其作为主时间服务器同步网络中其他设备的时钟。网络中的设备与主时间服务器的NTP距离，即NTP同步链上NTP服务器的数目，决定了设备上时钟的层数。例如网络拓扑为：原子时钟—>Device A—>Device B—>Device C，则Device A的时钟层级为1，Device B的时钟层级为2，Device C的时钟层级为3
处理建议	1. 确认时钟源是否发生变化。执行 **display ntp-service status**查看字段Reference clock ID（表示时钟源地址）的取值： o 如果 Reference clock ID 字段的取值和网络规划中的主时钟源地址一致，则执行步骤 2；如果 Reference clock ID 字段的取值和网络规划中的主时钟源地址不一致，则说明发生了时钟源切换，时钟源的切换导致时钟层数的变化，无需处理 o 如果 Reference clock ID 的取值为 none，则表示时钟源丢失。请更换时钟源或者修复故障的时钟源 2. 确认是否是时钟源本身层级变化导致本设备的时钟层数变化。登录时钟源，查看时钟源的时钟层数。如果时钟源的时钟层数和网络规划不一致，请修改时钟源的时钟层数（如果时钟源为H3C设备，执行 **display ntp-service sessions**命令，stra字段的取值即为时钟源的时钟层数，在系统视图下执行 **ntp-service refclock-master**命令修改时钟源的时钟层级） 3. 确认是否是时钟源本身层级变化导致本设备的时钟层数变化。在设备上执行 **display ntp-service sessions**命令，stra字段的取值即为时钟源的时钟层数。如果时钟源的时钟层数和网络规划不一致，请登录时钟源并修改时钟源的时钟层数（如果时钟源为H3C设备，在系统视图下执行 **ntp-service refclock-master** 命令可修改时钟源的时钟层数）

107 OAP

本节介绍 OAP 模块输出的日志信息。

107.1 OAP_CLIENT_DEREG

日志内容	OAP client [UINT32] on interface [STRING] deregistered.
日志含义	OAP client已注销
参数解释	$1：OAP clien ID $2：接口名称
日志等级	5 (Notification)
举例	OAP/5/OAP_CLIENT_DEREG: OAP client 1 on interface GigabitEthernet1/0/24 deregistered.
对系统的影响	OAP client不能和设备通信
日志产生原因	接口上承载的OAP client已注销
处理建议	检查OAP client的登录信息

107.2 OAP_CLIENT_TIMEOUT

日志内容	OAP client [UINT32] on interface [STRING] timed out.
日志含义	OAP client超时
参数解释	$1：OAP clien ID $2：接口名称
日志等级	4 (Warning)
举例	OAP/4/OAP_CLIENT_TIMEOUT: OAP client 1 on interface GigabitEthernet1/0/24 timed out.
对系统的影响	可能会影响OAP client和设备的通信
日志产生原因	接口上承载的OAP client超时
处理建议	检查故障链路

108 OBJP

本节介绍 OBJP（对象策略）模块输出的日志信息。

108.1 OBJP_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] object-policy [STRING]. The resources are insufficient.
日志含义	硬件资源不足导致某对象策略加速失败
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4 (Warning)
举例	OBJP/4/OBJP_ACCELERATE_NO_RES: Failed to accelerate IPv6 object-policy a. The resources are insufficient.
对系统的影响	新增加加速失败的规则不生效，但是不影响之前加速成功的规则
日志产生原因	因硬件资源不足，系统加速对象策略失败
处理建议	删除一些规则或者关闭其他对象策略的加速功能，释放硬件资源

108.2 OBJP_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] object-policy [STRING]. Object-policy acceleration is not supported.
日志含义	某对象策略暂不支持加速导致加速失败
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4 (Warning)
举例	OBJP/4/OBJP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 object-policy a. Object-policy acceleration is not supported.
对系统的影响	加速失败的对象策略匹配报文速度较慢，影响转发效率
日志产生原因	因系统不支持对象策略加速而导致对象策略加速失败
处理建议	无需处理

108.3 OBJP_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] object-policy [STRING].
日志含义	系统故障导致某对象策略加速失败
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4 (Warning)
举例	OBJP/4/OBJP_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 object-policy a.
对系统的影响	新增加加速失败的规则不生效，但是不影响之前加速成功的规则
日志产生原因	因系统故障导致对象策略加速失败
处理建议	无需处理

109 OFP

本节介绍 OpenFlow 模块输出的日志信息。

109.1 OFP_ACTIVE

日志内容	Activate openflow instance [UINT16]
日志含义	激活OpenFlow实例
参数解释	$1：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_ACTIVE: Activate openflow instance 1.
对系统的影响	无
日志产生原因	收到激活OpenFlow实例的命令
处理建议	无需处理

109.2 OFP_ACTIVE_FAILED

日志内容	Failed to activate instance [UINT16].
日志含义	OpenFlow实例激活失败
参数解释	$1：实例ID
日志等级	4 (Warning)
举例	OFP/4/OFP_ACTIVE_FAILED: Failed to activate instance 1.
对系统的影响	Openflow实例无法使用
日志产生原因	激活OpenFlow实例失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.3 OFP_CONNECT

日志内容	Openflow instance [UINT16], controller [CHAR] is connected.
日志含义	OpenFlow实例与控制器建立了连接
参数解释	$1：实例ID $2：控制器ID
日志等级	5 (Notification)
举例	OFP/5/OFP_CONNECT: Openflow instance 1, controller 0 is connected.
对系统的影响	无
日志产生原因	OpenFlow实例与控制器建立了连接
处理建议	无需处理

109.4 OFP_DISCONNECT

日志内容	Openflow instance [UINT16], controller [STRING] is disconnected.disconnected reason:[STRING].
日志含义	OpenFlow实例与控制器断开了连接
参数解释	$1：实例ID $2：控制器ID $3：连接断开的原因，取值包括： o Undo commands executed o Echo timeout o Hello failed o Receiving Hello packet timed out o Receiving message failed o Epoll error o VRF deleted o VRF global port down o Failed to recycle the buffer o AP down
日志等级	5 (Notification)
举例	OFP/5/OFP_DISCONNECT: Openflow instance 1, controller 1 is disconnected.disconnected reason:Echo timeout.
对系统的影响	无
日志产生原因	OpenFlow实例与控制器的连接断开，断开原因参见reason字段
处理建议	建议收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.5 OFP_FAIL_OPEN

日志内容	Openflow instance [UINT16] is in fail [STRING] mode.
日志含义	OpenFlow实例进入连接中断模式
参数解释	$1：实例ID $2：连接中断模式，显示为secure或standalone
日志等级	5 (Notification)
举例	OFP/5/OFP_FAIL_OPEN: Openflow instance 1 is in fail secure mode.
对系统的影响	无
日志产生原因	实例激活后无法连接控制器，或者从所有控制器断开
处理建议	无需处理

109.6 OFP_FAIL_OPEN_FAILED

日志内容	OpenFlow instance [UINT16]: [STRING] fail-open mode configuration failed and the secure mode is restored.
日志含义	OpenFlow实例的连接中断模式配置失败，回退为缺省模式Secure
参数解释	$1：实例ID $2：连接中断模式，取值包括smart和standalone
日志等级	4 (Warning)
举例	OFP/4/OFP_FAIL_OPEN_FAILED: OpenFlow instance 1: standalone fail-open mode configuration failed and the secure mode is restored.
对系统的影响	OpenFlow实例的连接中断模式配置失败
日志产生原因	由于系统资源不足等原因，OpenFlow实例的连接中断模式配置失败（相关命令为**`fail-open mode`**），将回退为缺省模式Secure
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.7 OFP_FLOW_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
日志含义	OpenFlow实例添加流表项
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：XID $5：流表项cookie $6：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD: Openflow instance 1 controller 0: add flow entry 1, xid 0x1, cookie 0x0, table id 0.
对系统的影响	无
日志产生原因	收到修改流表信息（增加操作）并通过报文检查。即将添加流表项
处理建议	无需处理

109.8 OFP_FLOW_ADD_ARP_FAILED

日志内容	Failed to add OpenFlow ARP entry: IPAddr=[STRING], OutIfIndex=[UINT32], MACAddr=[STRING].
日志含义	OpenFlow ARP表项添加失败
参数解释	$1：ARP表项的IP地址 $2：ARP表项对应的出接口的索引 $3：ARP表项的MAC地址
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD_ARP_FAILED: Failed to add OpenFlow ARP entry: IPAddr=102.0.1.1, OutIfIndex=605, MACAddr=0002-0300-0002.
对系统的影响	无
日志产生原因	OpenFlow ARP表项添加失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.9 OFP_FLOW_ADD_BUSY

日志内容	The device is busy adding a large number of OpenFlow messages. Please do not reboot the active MPU.
日志含义	设备正忙于添加大量OpenFlow消息，建议不要重启主用主控板
参数解释	无
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD_BUSY: The device is busy adding a large number of OpenFlow messages. Please do not reboot the active MPU.
对系统的影响	无
日志产生原因	设备正忙于添加大量OpenFlow消息
处理建议	看到这条日志之后，建议避免重启主用主控板，否则可能导致备用主控板重启两次

109.10 OFP_FLOW_ADD_BUSY_RECOVER

日志内容	Finished adding a large number of OpenFlow messages.
日志含义	大量OpenFlow消息已完成添加
参数解释	无
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD_BUSY_RECOVER: Finished adding a large number of OpenFlow messages.
对系统的影响	无
日志产生原因	控制器向设备下发的大量OpenFlow消息已完成添加，设备不再处于忙状态
处理建议	无需处理

109.11 OFP_FLOW_ADD_DUP

日志内容	Openflow instance [UINT16] controller [CHAR]: add duplicate flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
日志含义	OpenFlow实例添加重复的流表项
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：XID $5：Cookie $6：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD_DUP: Openflow instance 1 controller 0: add duplicate flow entry 1, xid 0x1, cookie 0x1, table id 0.
对系统的影响	无
日志产生原因	表项重复添加
处理建议	无需处理

109.12 OFP_FLOW_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32],table id [CHAR],because of insufficient resources.
日志含义	由于资源不足，OpenFlow实例添加流表项失败
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：流表ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry 641,table id 0,because of insufficient resources.
对系统的影响	该流表项流量转发功能不可用
日志产生原因	由于资源不足，添加流表项失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32], table id [CHAR].
日志含义	OpenFlow实例添加流表项失败
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：流表ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry 1, table id 0.
对系统的影响	该流表项流量转发功能不可用
日志产生原因	添加流表项失败
处理建议	无需处理

109.13 OFP_FLOW_ADD_ND_FAILED

日志内容	Failed to add OpenFlow ND entry: IPv6Addr=[STRING], OutIfIndex=[UINT32], MACAddr=[STRING].
日志含义	OpenFlow ND表项添加失败
参数解释	$1：ND表项的IPv6地址 $2：ND表项对应的出接口的索引 $3：ND表项的MAC地址
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD_ND_FAILED: Failed to add OpenFlow ND entry: IPv6Addr=1:1::1:1, OutIfIndex=5, MACAddr=1-1-1.
对系统的影响	无
日志产生原因	OpenFlow ND表项添加失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.14 OFP_FLOW_ADD_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: add table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
日志含义	OpenFlow实例添加Table Miss流表项
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_ADD_TABLE_MISS: Openflow instance 1 controller 0: add table miss flow entry, xid 0x1, cookie 0x0, table id 0.
对系统的影响	无
日志产生原因	收到修改流表信息（增加操作）并通过报文检查。即将添加miss规则
处理建议	无需处理

109.15 OFP_FLOW_ADD_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add table miss flow entry, table id [CHAR].
日志含义	OpenFlow实例添加Table Miss流表项失败
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_ADD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to add table miss flow entry, table id 0.
对系统的影响	该Miss表项功能不可用
日志产生原因	添加miss规则失败
处理建议	无需处理

109.16 OFP_FLOW_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
日志含义	OpenFlow实例删除流表项
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_DEL: Openflow instance 1 controller 0: delete flow entry, xid 0x1, cookie 0x0, table id 0.
对系统的影响	无
日志产生原因	收到修改流表信息（删除操作）并通过报文检查。即将删除对应的流表项
处理建议	无需处理

109.17 OFP_FLOW_DEL_L2VPN_DISABLE

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because L2VPN was disabled.
日志含义	L2VPN功能关闭导致多个流表项被删除
参数解释	$1：删除的表项个数 $2：流表ID $3：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_DEL_L2VPN_DISABLE: 2 flow entries in table 1 of instance 1 were deleted because L2VPN was disabled.
对系统的影响	无
日志产生原因	L2VPN功能关闭导致多个流表项被删除
处理建议	无需处理

109.18 OFP_FLOW_DEL_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: delete table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
日志含义	OpenFlow实例删除Table Miss流表项
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_DEL_TABLE_MISS: Openflow instance 1 controller 0: delete table miss flow entry, xid 0x1, cookie 0x0, table id 0.
对系统的影响	无
日志产生原因	收到修改流表信息（删除操作）并通过报文检查。即将删除对应的miss规则
处理建议	无需处理

109.19 OFP_FLOW_DEL_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to delete table miss flow entry, table id [STRING].
日志含义	OpenFlow实例删除Table Miss流表项失败
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_DEL_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to delete table miss flow entry, table id 0.
对系统的影响	旧miss规则依旧生效
日志产生原因	删除miss规则失败
处理建议	无需处理

109.20 OFP_FLOW_DEL_VSIIF_DEL

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because the Vsi-interface in VSI [STRING] was deleted.
日志含义	由于VSI下的VSI虚接口被删除，导致相关流表项被删除
参数解释	$1：删除的表项个数 $2：流表ID $3：实例ID $4：VSI的名称
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_DEL_VSIIF_DEL: 5 flow entries in table 1 of instance 1 were deleted because the Vsi-interface in VSI VSI-OFP was deleted.
对系统的影响	无
日志产生原因	VSI下的VSI虚接口被删除
处理建议	无需处理

109.21 OFP_FLOW_DEL_VXLAN_DEL

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because a tunnel (ifindex [UINT32]) in VXLAN [UINT32] was deleted.
日志含义	VXLAN隧道被删除，导致多个流表项被删除
参数解释	$1：删除的表项个数 $2：流表ID $3：实例ID $4：Tunnel接口索引 $5：VXLAN ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_DEL_VXLAN_DEL: 2 flow entries in table 1 of instance 1 were deleted because a tunnel (ifindex 141) in VXLAN 1 was deleted.
对系统的影响	无
日志产生原因	VXLAN隧道被删除
处理建议	无需处理

109.22 OFP_FLOW_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
日志含义	OpenFlow实例修改流表项
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_MOD: Openflow instance 1 controller 0: modify flow entry, xid 0x1, cookie 0x0, table id 0.
对系统的影响	无
日志产生原因	收到修改流表信息（修改操作）并通过报文检查。即将修改对应的流表项
处理建议	无需处理

109.23 OFP_FLOW_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify flow entry, table id [CHAR].
日志含义	OpenFlow实例修改流表项失败
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_MOD_FAILED: Openflow instance 1 controller 0: failed to modify flow entry, table id 0.
对系统的影响	旧流表项依旧生效
日志产生原因	修改流表项失败
处理建议	控制器重试修改操作或直接删除流表项

109.24 OFP_FLOW_MOD_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: modify table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
日志含义	OpenFlow实例修改Table Miss流表项
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_MOD_TABLE_MISS: Openflow instance 1 controller 0: modify table miss flow entry, xid 0x1, cookie 0x0, table id 0.
对系统的影响	无
日志产生原因	收到修改流表信息（修改操作）并通过报文检查。即将修改对应的miss规则
处理建议	无需处理

109.25 OFP_FLOW_MOD_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify table miss flow entry, table id [CHAR].
日志含义	OpenFlow实例修改Table Miss流表项失败
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_MOD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to modify table miss flow entry, table id 0.
对系统的影响	旧miss规则依旧生效
日志产生原因	修改miss规则失败
处理建议	控制器重试修改操作或直接删除miss规则

109.26 OFP_FLOW_RMV_GROUP

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
日志含义	group_mod消息导致流表项被删除
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance 1 was deleted with a group_mod message.
对系统的影响	无
日志产生原因	Group删除导致的表项删除
处理建议	无需处理

109.27 OFP_FLOW_RMV_HARDTIME

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an hard-time expiration.
日志含义	Hard-time超时导致流表项被删除
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_RMV_HARDTIME: The flow entry 1 in table 0 of instance 1 was deleted because of an hard-time expiration.
对系统的影响	无
日志产生原因	Hard-time超时导致的表项删除
处理建议	无需处理

109.28 OFP_FLOW_RMV_IDLETIME

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
日志含义	Idle-time超时导致流表项被删除
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_RMV_IDLETIME: The flow entry 1 in table 0 of instance 1 was deleted because of an idle-time expiration.
对系统的影响	无
日志产生原因	Idle-time超时导致的表项删除
处理建议	无需处理

109.29 OFP_FLOW_RMV_METER

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
日志含义	meter_mod消息导致流表项被删除
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance1 was deleted with a meter_mod message.
对系统的影响	无
日志产生原因	Meter删除导致的表项删除
处理建议	无需处理

109.30 OFP_FLOW_UPDATE_FAILED

日志内容	OpenFlow instance [UINT16] table [CHAR]: failed to update or synchronize flow entry [UINT32].
日志含义	OpenFlow实例更新或同步流表项失败
参数解释	$1：实例ID $2：流表ID $3：流表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_FLOW_UPDATE_FAILED: OpenFlow instance 1 table 0: failed to update or synchronize flow entry 10000.
对系统的影响	更新或同步失败的表项丢失
日志产生原因	主备倒换时，新主用主控板更新流表项失败 设备插入新接口板时，接口板同步主控板的流表项失败 IRF中主从设备倒换时，新主设备更新流表项失败 IRF中加入新成员设备时，成员设备同步主设备的流表项失败
处理建议	删除下发失败的流表项

109.31 OFP_GROUP_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add group [STRING], xid 0x[HEX].
日志含义	OpenFlow实例添加Group表项
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5 (Notification)
举例	OFP/5/OFP_GROUP_ADD: Openflow instance 1 controller 0: add group 1, xid 0x1.
对系统的影响	无
日志产生原因	收到修改group表信息（增加操作）并通过报文检查。即将添加group表项
处理建议	无需处理

109.32 OFP_GROUP_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add group [STRING].
日志含义	OpenFlow实例添加Group表项失败
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_GROUP_ADD_FAILED: Openflow Instance 1 controller 0: failed to add group 1.
对系统的影响	该流表项流量转发功能不可用
日志产生原因	添加group表项失败
处理建议	无需处理

109.33 OFP_GROUP_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete group [STRING], xid [HEX].
日志含义	OpenFlow实例删除Group表项
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5 (Notification)
举例	OFP/5/OFP_GROUP_DEL: Openflow instance 1 controller 0: delete group 1, xid 0x1.
对系统的影响	无
日志产生原因	收到修改group表信息（删除操作）并通过报文检查。即将删除对应group表项
处理建议	无需处理

109.34 OFP_GROUP_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify group [STRING], xid 0x[HEX].
日志含义	OpenFlow实例修改Group表项
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5 (Notification)
举例	OFP/5/OFP_GROUP_MOD: Openflow instance 1 controller 0: modify group 1, xid 0x1.
对系统的影响	无
日志产生原因	收到修改group表信息（修改操作）并通过报文检查。即将修改对应group表项
处理建议	无需处理

109.35 OFP_GROUP_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify group [STRING].
日志含义	OpenFlow实例修改Group表项失败
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_GROUP_MOD_FAILED: Openflow instance 1 controller 0: failed to modify group 1.
对系统的影响	旧group表项依旧生效
日志产生原因	修改group表项失败
处理建议	控制器重试修改操作或直接删除group表项

109.36 OFP_GROUP_REFRESH_FAILED

日志内容	Openflow instance [STRING]:Failed to refresh group [STRING].
日志含义	OpenFlow实例刷新Group表项失败
参数解释	$1：实例ID $2：Group表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_GROUP_REFRESH_FAILED: Openflow instance 1:Failed to refresh group 1.
对系统的影响	无
日志产生原因	控制器成功下发Group表项到设备后，设备因为拔出/插入接口板或删除/重新创建接口，需要刷新该Group表项中某些bucket的接口信息，但是由于硬件资源不足或设备异常，刷新Group表项失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.37 OFP_GROUP_ROLLBACK_FAILED

日志内容	Openflow instance [STRING]:Failed to roll back group [STRING].
日志含义	OpenFlow实例回退Group表项失败
参数解释	$1：实例ID $2：Group表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_GROUP_ROLLBACK_FAILED: Openflow instance 1:Failed to roll back group 1.
对系统的影响	无
日志产生原因	控制器修改设备的Group表项失败时，设备需要将该Group表项回退到修改前状态，但是由于硬件资源不足或设备异常，回退Group表项失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.38 OFP_METER_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add meter [STRING], xid 0x[HEX].
日志含义	OpenFlow实例添加Meter表项
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5 (Notification)
举例	OFP/5/OFP_METER_ADD: Openflow instance 1 controller 0: add meter 1, xid 0x1.
对系统的影响	无
日志产生原因	收到修改meter表信息（增加操作）并通过报文检查。即将添加meter表项
处理建议	无需处理

109.39 OFP_METER_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add meter [STRING].
日志含义	OpenFlow实例添加Meter表项失败
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_METER_ADD_FAILED: Openflow Instance 1 controller 0: failed to add meter 1.
对系统的影响	无
日志产生原因	添加meter表项失败
处理建议	无需处理

109.40 OFP_METER_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete meter [STRING], xid 0x[HEX].
日志含义	OpenFlow实例删除Meter表项
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5 (Notification)
举例	OFP/5/OFP_METER_DEL: Openflow instance 1 controller 0: delete meter 1, xid 0x1.
对系统的影响	无
日志产生原因	收到修改meter表信息（删除操作）并通过报文检查。即将删除指定的meter表项
处理建议	无需处理

109.41 OFP_METER_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify meter [STRING], xid 0x[HEX].
日志含义	OpenFlow实例修改Meter表项
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5 (Notification)
举例	OFP/5/OFP_METER_MOD: Openflow Instance 1 controller 0: modify meter 1, xid 0x1.
对系统的影响	无
日志产生原因	收到修改meter表信息（修改操作）并通过报文检查。即将修改指定的meter表项
处理建议	无需处理

109.42 OFP_METER_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify meter [STRING].
日志含义	OpenFlow实例修改Meter表项失败
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4 (Warning)
举例	OFP/4/OFP_METER_MOD_FAILED: Openflow instance 1 controller 0: failed to modify meter 1.
对系统的影响	旧流表项依旧生效
日志产生原因	修改meter表项失败
处理建议	控制器重试修改操作或直接删除meter表项

109.43 OFP_MISS_RMV_GROUP

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
日志含义	group_mod消息导致Table Miss表项被删除
参数解释	$1：流表ID $2：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_MISS_RMV_GROUP: The table-miss flow entry in table 0 of instance 1 was deleted with a group_mod message.
对系统的影响	无
日志产生原因	Group删除导致的table-miss表项删除
处理建议	无需处理

109.44 OFP_MISS_RMV_HARDTIME

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an hard-time expiration.
日志含义	Hard-time超时导致Table Miss表项被删除
参数解释	$1：流表ID $2：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_MISS_RMV_HARDTIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an hard-time expiration.
对系统的影响	无
日志产生原因	Hard-time超时导致的table-miss表项删除
处理建议	无需处理

109.45 OFP_MISS_RMV_IDLETIME

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
日志含义	Idle-time超时导致Table Miss表项被删除
参数解释	$1：流表ID $2：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_MISS_RMV_IDLETIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an idle-time expiration.
对系统的影响	无
日志产生原因	Idle-time超时导致的table-miss表项删除
处理建议	无需处理

109.46 OFP_MISS_RMV_METER

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
日志含义	meter_mod消息导致Table Miss表项被删除
参数解释	$1：流表ID $2：实例ID
日志等级	5 (Notification)
举例	OFP/5/OFP_MISS_RMV_METER: The table-miss flow entry in table 0 of instance 1 was deleted with a meter_mod message.
对系统的影响	无
日志产生原因	Meter删除导致的table-miss表项删除
处理建议	无需处理

109.47 OFP_SMARTGROUP_BIND

日志内容	Bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项绑定到Program Group表项
参数解释	$1：Target ID $2：Program ID $3：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	5 (Notification)
举例	OFP/5/OFP_SMARTGROUP_BIND: Bind target 1 to program 2 by flow ID map 7.
对系统的影响	无
日志产生原因	收到控制器消息，准备将指定Target ID和Flow ID的Target Group表项与指定Program ID和Flow ID的Program Group表项进行绑定。其中，Flow ID由Flow ID Map提供 本日志对应的操作中，同一Target Group表项只能绑定到一个Program Group表项 上述举例中的日志信息表示设备执行了如下操作： • 将 Target ID 为 1、Flow ID 为 0 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 0 的 Program Group 表项 • 将 Target ID 为 1、Flow ID 为 1 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 1 的 Program Group 表项 • 将 Target ID 为 1、Flow ID 为 2 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 2 的 Program Group 表项
处理建议	无需处理

109.48 OFP_SMARTGROUP_BIND_FAILED

日志内容	Failed to bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项绑定到Program Group表项时失败
参数解释	$1：Target ID $2：Program ID $3：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	4 (Warning)
举例	OFP/4/OFP_SMARTGROUP_BIND_FAILED: Failed to bind target 1 to program 2 by flow ID map 7.
对系统的影响	Program Group表项未能获得Target Group表项的动作桶
日志产生原因	对Target Group表项的绑定操作失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

109.49 OFP_SMARTGROUP_NEW_BIND

日志内容	Bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项绑定到Program Group表项
参数解释	$1：Target ID $2：Program ID $3：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	5 (Notification)
举例	OFP/5/OFP_SMARTGROUP_NEW_BIND: Bind target 1 to program 2 by flow ID map 7.
对系统的影响	无
日志产生原因	收到控制器消息，准备将指定Target ID和Flow ID的Target Group表项绑定到指定Program ID和Flow ID的Program Group表项。其中，Flow ID由Flow ID Map提供 上述举例中的日志信息表示设备执行了如下操作： • 将 Target ID 为 1、Flow ID 为 0 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 0 的 Program Group 表项 • 将 Target ID 为 1、Flow ID 为 1 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 1 的 Program Group 表项 • 将 Target ID 为 1、Flow ID 为 2 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 2 的 Program Group 表项
处理建议	无需处理

109.50 OFP_SMARTGROUP_NEW_BIND_FAILED

日志内容	Failed to bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项绑定到Program Group表项时失败
参数解释	$1：Target ID $2：Program ID $3：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	4 (Warning)
举例	OFP/4/OFP_SMARTGROUP_NEW_BIND_FAILED: Failed to bind target 1 to program 2 by flow ID map 7.
对系统的影响	Program Group表项未能获得Target Group表项的动作桶
日志产生原因	对Target Group表项的绑定操作失败
处理建议	请联系技术支持人员

109.51 OFP_SMARTGROUP_REBIND

日志内容	Unbind target [UINT32] from program [UINT32] and bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项与Program Group表项解除绑定，再绑定到新的Program Group表项
参数解释	$1：Target ID $2：Program ID $3：Target ID $4：Program ID $5：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	5 (Notification)
举例	OFP/5/OFP_SMARTGROUP_REBIND: Unbind target 1 from program 1 and bind target 1 to program 2 by flow ID map 7.
对系统的影响	Target Group表项的动作桶被转移到新的Program Group表项，可实现业务流切换
日志产生原因	收到控制器消息，准备将指定Target ID和Flow ID的Target Group表项与指定Program ID和Flow ID的Program Group表项解除绑定，并将这些Target Group表项绑定到新的Program Group表项。其中，Flow ID由Flow ID Map提供 上述举例中的日志信息表示设备执行了如下操作： • 将 Target ID 为 1、Flow ID 为 0 的 Target Group 表项与 Program ID 为 1、Flow ID 为 0 的 Program Group 表项解除绑定，再绑定到 Program ID 为 2、Flow ID 为 0 的 Program Group 表项 • 将 Target ID 为 1、Flow ID 为 1 的 Target Group 表项与 Program ID 为 1、Flow ID 为 1 的 Program Group 表项解除绑定，再绑定到 Program ID 为 2、Flow ID 为 1 的 Program Group 表项 • 将 Target ID 为 1、Flow ID 为 2 的 Target Group 表项与 Program ID 为 1、Flow ID 为 2 的 Program Group 表项解除绑定，再绑定到 Program ID 为 2、Flow ID 为 2 的 Program Group 表项
处理建议	无需处理

109.52 OFP_SMARTGROUP_REBIND_FAILED

日志内容	Failed to unbind target [UINT32] from program [UINT32] and bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项与Program Group表项解除绑定、再绑定到新的Program Group表项的操作失败
参数解释	$1：Target ID $2：Program ID $3：Target ID $4：Program ID $5：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	4 (Warning)
举例	OFP/4/OFP_SMARTGROUP_REBIND_FAILED: Failed to unbind target 1 from program 1 and bind target 1 to program 2 by flow ID map 7.
对系统的影响	可能出现业务流切换失败现象
日志产生原因	对Target Group表项的重新绑定操作失败
处理建议	请联系技术支持人员

109.53 OFP_SMARTGROUP_UNBIND

日志内容	Unbind target [UINT32] from program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项与Program Group表项解除绑定
参数解释	$1：Target ID $2：Program ID $3：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	5 (Notification)
举例	OFP/5/OFP_SMARTGROUP_UNBIND: Unbind target 1 from program 2 by flow ID map 7.
对系统的影响	Program Group表项被解除Target Group表项的动作桶后，不再进行转发动作
日志产生原因	收到控制器消息，准备将指定Target ID和Flow ID的Target Group表项与指定Program ID和Flow ID的Program Group表项解除绑定。其中，Flow ID由Flow ID Map提供
处理建议	无需处理

109.54 OFP_SMARTGROUP_UNBIND_FAILED

日志内容	Failed to unbind target [UINT32] from program [UINT32] by flow ID map [UINT32].
日志含义	根据Flow ID Map将Target Group表项与Program Group表项解除绑定时失败
参数解释	$1：Target ID $2：Program ID $3：Flow ID Map，代表一到多个Flow ID • 本参数以十进制数显示，其对应二进制值的各bit从右到左分别代表Flow ID 0～Flow ID 31，bit值为 1 表示取该位对应的Flow ID。例如，Flow ID Map值 7 对应的二进制数 00000000 00000000 00000000 00000**111**表示取Flow ID 0、Flow ID 1、Flow ID 2 • 取值为 0 时，表示所有 Flow ID
日志等级	4 (Warning)
举例	OFP/4/OFP_SMARTGROUP_UNBIND_FAILED: Failed to unbind target 1 from program 2 by flow ID map 7.
对系统的影响	Program Group表项仍保持Target Group表项的动作桶
日志产生原因	对Target Group表项的解除绑定操作失败
处理建议	请联系技术支持人员

109.55 OFP_TTP_GROUP_DEL_DENY

日志内容	Openflow instance [STRING] controller [CHAR]: Failed to delete TTP group [STRING], XID [HEX]. Reason: The TTP group is used by another TTP group.
日志含义	由于被其他TTP Group表项引用，TTP Group表项删除失败
参数解释	$1：实例ID $2：控制器ID $3：TTP（Table Type Pattern） Group表项ID $4：XID（Transaction ID，交互ID）
日志等级	4 (Warning)
举例	OFP/4/OFP_TTP_GROUP_DEL_DENY: Openflow instance 1 controller 0: Failed to delete TTP group 1, XID 0x1. Reason: The TTP group is used by another TTP group.
对系统的影响	TTP Group表项删除失败
日志产生原因	被其他TTP Group表项引用的TTP Group表项不允许被删除
处理建议	请控制器先删除引用TTP Group表项的其他TTP Group表项，再重试删除操作

109.56 PORT_MOD

日志内容	Port modified. InstanceID =[UINT16], IfIndex =[UINT32], PortDown=[STRING], NoRecv=[STRING], NoFwd=[STRING], NoPktIn=[STRING], Speed=[STRING], Duplex=[STRING].
日志含义	OpenFlow实例中的接口已修改
参数解释	$1：实例ID $2：接口索引 $3：接口状态是否设置为down。NoChange表示不改变接口状态，True表示设置接口down，False表示设置接口up $4：设置接口不接收报文。NoChange表示不改变接口设置，True表示设置接口不接收报文，False表示设置接口接收报文 $5：设置接口不发送报文。NoChange表示不改变接口设置，True表示设置接口不发送报文，False表示设置接口发送报文 $6：设置接口上的报文不上送控制器。NoChange表示不改变接口设置，True表示设置接口的报文不上送控制器，False表示设置接口的报文上送控制器 $7：设置的接口速率。取值包括Auto、Error、10M、100M、1G、10G等。其中Error表示设置的速率不支持。如果取值为空，表示没有设置该参数 $8：设置的接口双工模式。取值包括Full、Half、Auto和Error。其中Error表示设置的双工模式不支持。如果取值为空，表示没有设置该参数
日志等级	5 (Notification)
举例	OFP/5/PORT_MOD: Port modified. InstanceID =1, IfIndex =2, PortDown=True, NoRecv=NoChange, NoFwd=NoChange, NoPktIn=NoChange, Speed=, Duplex=.
对系统的影响	无
日志产生原因	控制器修改了OpenFlow实例中的接口
处理建议	无需处理

109.57 OFP_RADARDETECTION

日志内容	inIfIndex = [UINT32], packageId = [UINT16], innerTTL = [CHAR], outerTTL = [CHAR].
日志含义	报文的索引、标记和Time To Live信息
参数解释	$1：报文入接口索引 $2：报文标记 $3：报文内层IP头的Time To Live取值 $4：报文外层IP头的Time To Live取值
日志等级	5 (Notification)
举例	OFP/5/OFP_RADARDETECTION: inIfIndex = 1, packageId = 1, innerTTL = 128, outerTTL = 128.
对系统的影响	无
日志产生原因	收到用于雷达探测或VM仿真功能的报文
处理建议	无需处理

110 ONVIF

本节介绍 ONVIF（Open Network Video Interface Forum，开放型网络视频接口论坛）模块输出的日志信息。

110.1 ONVIF_ENDPOINT_CHANGE

日志内容	Detected the change of an endpoint: MAC address=[STRING], IP address=[STRING], VLAN=[UINT16], interface=[STRING].
日志含义	ONVIF检测到终端的参数发生了变化
参数解释	$1：终端的MAC地址 $2：变化后，终端的IP地址 $3：变化后，终端所属的VLAN $4：变化后，终端上线的接口
日志等级	6 (Informational)
举例	ONVIF/6/ONVIF_ENDPOINT_CHANGE: Detected the change of an endpoint: MAC address=12c2-d4ed-0200, IP address=192.168.254.24, VLAN=1, interface=GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	ONVIF检测到终端的以下某个或多个参数发生了变化： • 终端的 IP 地址 • 终端所属的 VLAN • 终端上线的接口
处理建议	无需处理

110.2 ONVIF_ENDPOINT_OFFLINE

日志内容	Detected the disassociation of an endpoint: MAC address=[STRING], IP address=[STRING], VLAN=[UINT16], interface=[STRING].
日志含义	ONVIF检测到终端下线
参数解释	$1：终端的MAC地址 $2：终端的IP地址 $3：终端所属的VLAN $4：终端上线的接口
日志等级	6 (Informational)
举例	ONVIF/6/ONVIF_ENDPOINT_OFFLINE: Detected the disassociation of an endpoint: MAC address=12c2-d4ed-0200, IP address=192.168.254.24, VLAN=1, interface=GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	• ONVIF 检测到终端下线
处理建议	• 如果是管理员主动操作让终端下线（例如断开设备和终端的连线、重启终端等），则无需处理 • 如果是非管理员主动操作导致的终端下线，请按照以下步骤处理： a. 检查终端供电是否正常，请确保终端供电正常 b. 检查终端是否故障。如果终端故障，请先修复终端 c. 检查终端和设备的链接是否畅通，可以尝试重新插拔网线、更换网线、更换对接接口来修复故障

110.3 ONVIF_ENDPOINT_ONLINE

日志内容	Detected the association of an endpoint: MAC address=[STRING], IP address=[STRING], VLAN ID=[UINT16], interface=[STRING].
日志含义	ONVIF检测到终端上线
参数解释	$1：终端的MAC地址 $2：终端的IP地址 $3：终端所属的VLAN $4：终端上线的接口
日志等级	6 (Informational)
举例	ONVIF/6/ONVIF_ENDPOINT_ONLINE: Detected the association of an endpoint: MAC address=b4a3-8267-bc03, IP address=192.168.254.24, VLAN ID=1, interface=GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	ONVIF检测到终端上线
处理建议	无需处理

111 OPENSRC（FreeRADIUS）

本节介绍 OPENSRC 模块输出的开源软件 FreeRADIUS 日志信息。

111.1 HUP事件

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
日志含义	接收到HUP信号
参数解释	$1：时间（月 日） $2：时刻（时:分:秒） $3：FreeRADIUS进程ID $4：HUP事件说明 • Received HUP sign：收到 HUP 信号 • Module: Reloaded module "files"：重新加载模块配置文件 • HUP - Files loaded by a module have changed. ：收到 HUP 信号，完成配置文件加载 • Ignoring HUP (less than 5s since last one) ：收到此 HUP 信号间隔小于 5 秒，忽略
日志等级	6 (Informational)
举例	OPENSRC/6/SYSLOG: Jan 1 01:14:04 radiusd[427]: Received HUP sign
对系统的影响	对系统无影响
日志产生原因	可能的原有有： • 系统接收到 HUP 信号，重新加载用户配置信息（用户名、用户密码、授权 VLAN、授权 ACL 及用户有效期）用于认证处理 • 系统收到此 HUP 信号间隔小于 5 秒，将其忽略
处理建议	请根据HUP事件的详细说明选择相应的处理方式： • 如果收到此HUP信号间隔小于5秒，且希望5秒内配置的新用户生效，请执行激活命令 **radius-server activate** • 其它情况无需处理

111.2 进程重启

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
日志含义	进程重启
参数解释	$1：日期（月 日） $2：时间（时:分:秒） $3：FreeRADIUS进程ID $4：进程重启事件说明 • Signalled to terminate：收到终结进程信号 • Exiting normally：进程关闭 • Debugger not attached：进程对应的调试信息开关处于关闭状态 • Loaded virtual server <default>：加载虚拟服务器 • Loaded virtual server inner-tunnel：加载虚拟服务器内部通道 • Loaded virtual server default：加载虚拟服务器默认配置 • Ready to process requests：准备开始处理认证报文
日志等级	6 (Informational)
举例	OPENSRC/6/SYSLOG: Jan 1 02:00:02 radiusd[427]: Signalled to terminate
对系统的影响	FreeRADIUS进程终结，停止提供RADIUS server服务
日志产生原因	当前的FreeRADIUS进程终结，并重新启动
处理建议	系统正常运行时产生的信息，无需处理

111.3 进程启动

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
日志含义	进程启动
参数解释	$1：日期（月 日） $2：时间（时:分:秒） $3：FreeRADIUS进程ID $4：进程启动事件说明 • 11 Check item "FreeRADIUS-Response-Delay" found in filter list for realm "DEFAULT".：在指定文件中检查默认过滤项 FreeRADIUS-Response-Delay • 11 Check item "FreeRADIUS-Response-Delay-USec" found in filter list for realm "DEFAULT".：在指定文件中检查默认过滤项 FreeRADIUS-Response-Delay-USec • Ignoring "sql" (see raddb/mods-available/README.rst) ：忽略 SQL 处理 • Ignoring "ldap" (see raddb/mods-available/README.rst) ：忽略 LDAP 处理
日志等级	4 (Warning)
举例	OPENSRC/4/SYSLOG: Jan 1 02:00:03 radiusd[460]: [//etc/raddb/mods-config/attr_filter/access_reject]:11 Check item "FreeRADIUS-Response-Delay" found in filter list for realm "DEFAULT".
对系统的影响	FreeRADIUS进程正在启动，暂时无法提供RADIUS server服务
日志产生原因	FreeRADIUS进程启动时，系统加载默认检查项
处理建议	系统正常运行时产生的信息，无需处理

111.4 用户认证

日志内容	[DATE] [TIME] radiusd[UINT32]: ([UINT32]) [STRING]: [[STRING]] (from client [IPADDR] port [UINT32] cli [MAC])
日志含义	用户认证成功
参数解释	$1：日期（月 日） $2：时间（时:分:秒） $3：FreeRADIUS进程ID $4：日志编号 $5：认证结果 • Login OK：认证成功或共享密钥配置不一致 • **Lo**gin incorrect (pap: Cleartext password does not match "known good" password)：PAP认证密码错误 • Login incorrect (chap: Password comparison failed: password is incorrect)：CHAP认证密码错误 • Login incorrect (No Auth-Type found: rejecting the user via Post-Auth-Type = Reject)：PAP 认证用户名不匹配或 802.1X 用户配置的认证类型为 EAP • Login incorrect (chap: &control:Cleartext-Password is required for authentication)：CHAP 认证用户名不匹配 • Invalid user (expiration: Account expired at 'Jan 1 2013 02:19:00 UTC')：用户存在，但已经失效 $6：用户名 $7：RADIUS客户端IP地址 $8：RADIUS客户端端口号 $9：用户MAC地址
日志等级	5 (Notification)
举例	OPENSRC/5/SYSLOG: Jan 1 02:06:15 radiusd[460]: (0) Login OK: [test] (from client 7.7.7.7 port 33591297 cli 00-00-00-00-00-02)
对系统的影响	对系统无影响
日志产生原因	用户认证成功

处理建议	请根据认证结果的详细说明选择相应的处理方式：
	• 认证成功或共享密钥配置不一致：
	  ○ 如果用户认证成功，则不需要处理
	  ○ 如果用户认证失败，请检查RADIUS客户端和RADIUS服务器端的共享密钥是否一致。客户端共享密钥通过 **primary authentication**命令配置；服务器端共享密钥通过 **radius-server client ip**命令配置
	• PAP 认证密码错误：用户重新输入正确的密码
	• CHAP 认证密码错误：用户重新输入正确的密码
	• PAP 认证用户名不匹配或 802.1X 用户配置的认证类型为 EAP：
	  ○ 若是非法用户，则不需要处理
	  ○ 若是新增用户，则需要添加本地用户（通过 **local-user**命令）
	  ○ 检查配置的认证类型是否准确。例如，对于 802.1X用户可以通过 **display dot1x**查看认证类型，并通过 **dot1x authentication-method**命令修改认证

	方式
	• CHAP 认证用户名不匹配：
	  ○ 若是非法用户，则不需要处理
	  ○ 若是新增用户，则需要添加对应的本地用户（通过 **local-user**命令）
	• 用户存在，但已经失效
	  ○ 若是用户账户正常失效，则不需要处理
	  ○ 若需要延长用户有效期，则需要修改该本地用户的生效截至日期（通过 **validity-datetime**命令）

日志内容	[DATE] [TIME] radiusd[UINT32]: ([UINT32]) Login incorrect (No Auth-Type found: rejecting the user via Post-Auth-Type = Reject): [[STRING]] (from client [IPADDR] port [UINT32])
日志含义	不支持的Login类型的用户认证请求
参数解释	$1：日期（月 日） $2：时间（时:分:秒） $3：FreeRADIUS进程ID $4：日志编号 $5：用户名 $6：RADIUS客户端IP地址 $7：RADIUS客户端端口号
日志等级	5 (Notification)
举例	OPENSRC/5/SYSLOG: Jan 1 02:21:20 radiusd[460]: (16) Login incorrect (No Auth-Type found: rejecting the user via Post-Auth-Type = Reject): [ddd] (from client 7.7.7.7 port 0)
对系统的影响	对系统无影响
日志产生原因	系统拒绝了不支持的Login类型的用户认证请求
处理建议	系统正常运行时产生的信息，无需处理

日志内容	[DATE] [TIME] radiusd[UINT32]: Ignoring request to auth address * port 1812 bound to server default from unknown client [IPADDR] port [UINT32] proto udp
日志含义	不处理来自未知RADIUS客户端的认证请求报文
参数解释	$1：日期（月 日） $2：时间（时:分:秒） $3：FreeRADIUS进程ID $4：RADIUS客户端IP地址 $5：RADIUS客户端端口号
日志等级	3 (Error)
举例	OPENSRC/3/SYSLOG: Jan 1 02:31:05 radiusd[548]: Ignoring request to auth address * port 1812 bound to server default from unknown client 7.7.7.7 port 11969 proto udp
对系统的影响	可能有非法客户端接入，需要进一步排查
日志产生原因	未知的RADIUS客户端IP地址和端口号，不处理认证请求报文
处理建议	• 若是非法客户端，则不需要处理 • 若是新增客户端，则通过 **radius-server client**命令新增对应的RADIUS客户端配置

112 OPTMOD

本节介绍 OPTMOD 模块输出的日志信息。

112.1 BIAS_HIGH

日志内容	[STRING]: Bias current is high.
日志含义	光模块的偏置电流超过偏置电流高告警门限
参数解释	$1：端口名称
日志等级	2 (Critical)
举例	OPTMOD/2/BIAS_HIGH: GigabitEthernet1/0/1: Bias current is high.
对系统的影响	光模块无法正常工作
日志产生原因	光模块的偏置电流超过偏置电流高告警门限时，打印该日志
处理建议	1. **使用display transceive diagnosis i**nterface命令查看当前偏置电流值是否已经超过偏置电流高告警门限 2. 使用display transceive alarm interface命令多次查看当前是否确实存在偏置电流高告警 3. 如果确实存在偏置电流高告警，则表明光模块存在问题，请更换光模块

112.2 BIAS_LOW

日志内容	[STRING]: Bias current is low.
日志含义	光模块的偏置电流低于偏置电流低告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/BIAS_LOW: GigabitEthernet1/0/1: Bias current is low.
对系统的影响	光模块无法正常工作
日志产生原因	光模块的偏置电流低于偏置电流低告警门限时，打印该日志
处理建议	1. 确认 端口状态是否为shutdown，如果状态为shutdown，请端口状态恢复为up 2. 使用display transceive diagnosis interface命令查看当前偏置电流值是否已经超过偏置电流低告警门限 3. 使用display transceive alarm interface命令多次查看当前是否确实有偏置电流低告警 4. 如果低于偏置电流低告警门限，光模块或者单板存在故障，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.3 BIAS_NORMAL

日志内容	[STRING]: Bias current is normal.
日志含义	光模块的偏置电流恢复至正常范围
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/BIAS_NORMAL: GigabitEthernet1/0/1: Bias current is normal.
对系统的影响	对系统无影响
日志产生原因	光模块的偏置电流恢复至正常范围时，打印该日志
处理建议	无需处理

112.4 CFG_ERR

日志内容	[STRING]: Transceiver type and port configuration mismatched.
日志含义	光模块类型与端口配置不匹配
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/CFG_ERR: GigabitEthernet1/0/1: Transceiver type and port configuration mismatched.
对系统的影响	光模块可能无法正常工作
日志产生原因	光模块类型与端口配置不匹配时，打印该日志
处理建议	1. 判断光模块是否可以正常工作，如果光模块可以正常工作，则无需处理 2. 如果光模块不能正常工作，则可能是端口不支持或软件不支持导致的，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.5 CHKSUM_ERR

日志内容	[STRING]: Transceiver information checksum error.
日志含义	光模块寄存器信息校验失败
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/CHKSUM_ERR: GigabitEthernet1/0/1: Transceiver information checksum error.
对系统的影响	一般对系统无影响
日志产生原因	光模块寄存器信息校验失败时，打印该日志
处理建议	1. 判断光模块是否可以正常工作，如果光模块可以正常工作，则无需处理 2. 如果光模块不能正常工作，请重新插拔光模块 3. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.6 FIBER_SFP MODULE_INVALID

日志内容	[STRING]: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in [UINT32] days. Please replace it with a compatible one as soon as possible.
日志含义	光模块与接口卡不匹配
参数解释	$1：端口名称 $2：光模块失效天数
日志等级	4 (Warning)
举例	OPTMOD/4/FIBER_SFPMODULE_INVALID: GigabitEthernet1/0/1: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in 3 days. Please replace it with a compatible one as soon as possible.
对系统的影响	光模块无法正常工作
日志产生原因	光模块与接口卡不匹配时，打印该日志
处理建议	更换光模块

112.7 FIBER_SFPMODULE_NOWINVALID

日志内容	[STRING]: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
日志含义	不支持光模块
参数解释	$1：端口名称
日志等级	4 (Warning)
举例	OPTMOD/4/FIBER_SFPMODULE_NOWINVALID: GigabitEthernet1/0/1: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
对系统的影响	无法确保的光模块能够在设备上正常工作
日志产生原因	不支持光模块时，打印该日志
处理建议	更换光模块

112.8 IO_ERR

日志内容	[STRING]: The transceiver information I/O failed.
日志含义	设备读取光模块寄存器信息失败
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/IO_ERR: GigabitEthernet1/0/1: The transceiver information I/O failed.
对系统的影响	光模块无法正常工作
日志产生原因	设备读取光模块寄存器信息失败时，打印该日志
处理建议	**1.** 判断端口是否工作正常，如果端口不能正常工作，请先确认端口问题并解决 **2.** 确认单板上其他光模块是否多次出现此故障，如果是，则说明单板可能存在器件故障，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 **3.** 执行 display transceive diagnosis interface或者 display transceive alarm interface 命令，如果都显示为fail，则表示光模块故障，请更换光模块

112.9 MOD_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
日志含义	光模块故障被清除
参数解释	$1：端口名称 $2：故障类型
日志等级	3 (Error)
举例	OPTMOD/3/MOD_ALM_OFF: GigabitEthernet1/0/1: Module_not_ready was removed.
对系统的影响	对系统无影响
日志产生原因	光模块故障被清除时，打印该日志
处理建议	无需处理

112.10 MOD_ALM_ON

日志内容	[STRING]: [STRING] was detected.
日志含义	检测到光模块故障
参数解释	$1：端口名称 $2：故障类型
日志等级	3 (Error)
举例	OPTMOD/3/MOD_ALM_ON: GigabitEthernet1/0/1: Module_not_ready was detected.
对系统的影响	光模块可能无法正常工作
日志产生原因	检测到光模块故障时，打印该日志
处理建议	根据不同的故障类型，产生故障的原因可能是光模块本身的问题，也可能是端口、链路问题，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.11 MODULE_IN

日志内容	[STRING]: The transceiver is [STRING].
日志含义	一块光模块插入某端口
参数解释	$1：端口名称 $2：光模块类型
日志等级	4 (Warning)
举例	OPTMOD/4/MODULE_IN: GigabitEthernet1/0/1: The transceiver is 1000_BASE_T_AN_SFP.
对系统的影响	对系统无影响
日志产生原因	当一块光模块插入某端口时，打印该日志
处理建议	无需处理

112.12 MODULE_OUT

日志内容	[STRING]: Transceiver absent.
日志含义	光模块被拔出
参数解释	$1：端口名称
日志等级	4 (Warning)
举例	OPTMOD/4/MODULE_OUT: GigabitEthernet1/0/1: Transceiver absent.
对系统的影响	光模块不可用
日志产生原因	光模块被拔出时，打印该日志
处理建议	无需处理

112.13 OPTICAL_ALARM_CLEAR

日志内容	Transceiver alarm cleared. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	光模块重要故障恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	OPTMOD/2/OPTICAL_ALARM_CLEAR: Transceiver alarm cleared. (PhysicalIndex=9, PhysicalName=transceiver, RelativeResource=(transceivertype:SFP,interface:1/1/1,channel:2), ErrorCode=600023, Reason=Transceiver matches the port type.)
对系统的影响	对系统无影响
日志产生原因	光模块重要故障恢复
处理建议	无需处理

表112-1 OPTICAL_ALARM_CLEAR 故障码和故障原因描述表

故障码	故障原因描述
600023	Transceiver matches the port type.
600022	Transceiver matches the port configuration.
600001	OPTMOD initialization failure fixed on $1. $1：接口索引（框/槽/子卡/接口） Initialization failure of the DDR used for the transceiver cleared.

112.14 OPTICAL_ALARM_OCCUR

日志内容	Transceiver alarm occurred. (PhysicalIndex=[UINT], PhysicalName=[STRING], RelativeResource=([STRING]), ErrorCode=[STRING], Reason=[STRING])
日志含义	光模块重要故障产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	2 (Critical)
举例	OPTMOD/2/OPTICAL_ALARM_OCCUR: Transceiver alarm occurred. (PhysicalIndex=9, PhysicalName=transceiver, RelativeResource=(transceivertype:SFP,interface:1/1/1,channel:2), ErrorCode=600023, Reason=Transceiver does not match the port type.)
对系统的影响	光模块上的业务可能会受到影响
日志产生原因	光模块重要故障产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表112-2 OPTICAL_ALARM_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
600023	Transceiver does not match the port type.
600022	Transceiver does not match the port configuration.
600001	OPTMOD initialization failed on $1. $1：接口索引（框/槽/子卡/接口） DDR used for the transceiver failed initialization.

112.15 OPTICAL_WARNING_CLEAR

日志内容	Transceiver warning alarm cleared. (PhysicalIndex=$1, PhysicalName=$2, RelativeResource=$3, ErrorCode=$4, Reason=$5)
日志含义	光模块告警恢复
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	OPTMOD/4/OPTICAL_WARNING_CLEAR: Transceiver warning alarm occurred. (PhysicalIndex=9, PhysicalName= 1000_BASE_T_AN_SFP, RelativeResource= (transceivertype:SFP,interface: GigabitEthernet1/0/1,channel:2), ErrorCode=0600021, Reason= Transceiver information checksum error removed.)
对系统的影响	对系统无影响
日志产生原因	光模块告警恢复
处理建议	无需处理

表112-3 OPTICAL_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
0600021	Transceiver information checksum error removed.
0600020	Transceiver information read/write error fixed.
0600019	Transceiver Rx_not_ready error occurred.
0600018	Transceiver Tx_not_ready error removed.
0600017	Transceiver module_not_ready error removed.
0600014	Transceiver temperature increased to the normal range: CurrentValue = $1 degree centigrade, Threshold =$2 degree centigrade. $1:当前光模块温度值 $2:光模块设置低温告警阈值
0600013	Transceiver temperature decreased to the normal range:CurrentValue = $1 degree centigrade, Threshold =$2 degree centigrade. $1:当前光模块温度值 $2:光模块设置高温告警阈值
0600011	Transceiver voltage increased to the normal range: CurrentValue = $1 V, Threshold =$2 V. $1:当前供电电压值 $2:供电电压低阈值
0600010	Transceiver voltage decreased to the normal range: CurrentValue = $1 V, Threshold =$2 V. $1:当前供电电压值

故障码	故障原因描述
	$2:供电电压高阈值
0600009	Transceiver bias current increased to the normal range:CurrentValue = $1 mA, Threshold =$2 mA. $1:当前发送偏置电流值 $2:发送偏置电流低阈值
0600008	Transceiver bias current decreased to the normal range:CurrentValue = $1 mA, Threshold =$2 mA. $1:当前发送偏置电流值 $2:发送偏置电流高阈值
0600007	Transceiver Rx power increased to the normal range: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际接收光功率 $2:光模块接收光功率低门限值
0600006	Transceiver Rx power decreased to the normal range: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际接收光功率 $2:光模块接收光功率高门限值
0600005	Transceiver Tx power increased to the normal range: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际发送光功率 $2:光模块发送光功率低门限值
0600004	Transceiver Tx power decreased to the normal range: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际发送光功率 $2:光模块发送光功率高门限值
0600002	Transceiver module inserted in $1. $1 接口索引（框/槽/子卡/接口） Transceiver inserted.

112.16 OPTICAL_WARNING_OCCUR

日志内容	Transceiver warning alarm occurred. (PhysicalIndex=$1 PhysicalName=$2 RelativeResource=$3, ErrorCode=$4 Reason=$5
日志含义	光模块告警产生
参数解释	$1：实体索引 $2：实体名称 $3：故障位置信息 $4：故障码 $5：故障原因描述，详情请参见故障码和故障原因描述表
日志等级	4 (Warning)
举例	OPTMOD/4/OPTICAL_WARNING_OCCUR: Transceiver warning alarm occurred. (PhysicalIndex=9, PhysicalName= 1000_BASE_T_AN_SFP, RelativeResource= (transceivertype:SFP,interface: GigabitEthernet1/0/1,channel:2), ErrorCode=0600021, Reason= Transceiver information checksum error.)
对系统的影响	光模块上的业务可能会受到影响
日志产生原因	光模块告警产生时，打印该日志，详情请参见故障原因描述
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

表112-4 OPTICAL_WARNING_OCCUR 故障码和故障原因描述表

故障码	故障原因描述
0600021	Transceiver information checksum error.
0600020	Failed to read/write transceiver information.
0600019	Transceiver Rx_not_ready error occurred.
0600018	Transceiver Tx_not_ready error occurred.
0600017	Transceiver module_not_ready error occurred.
0600014	Transceiver temperature is too low: CurrentValue = $1 degree centigrade, Threshold =$2 degree centigrade. $1:当前光模块温度值 $2:光模块设置低温告警阈值
0600013	Transceiver temperature is too high: CurrentValue = $1 degree centigrade, Threshold =$2 degree centigrade. $1:当前光模块温度值 $2:光模块设置高温告警阈值
0600011	Transceiver voltage is too low:CurrentValue = $1 V, Threshold =$2 V. $1:当前供电电压值 $2:供电电压低阈值
0600010	Transceiver voltage is too high:CurrentValue = $1 V, Threshold =$2 V. $1:当前供电电压值 $2:供电电压高阈值

故障码	故障原因描述
0600009	Transceiver bias current is too low: CurrentValue = $1 mA, Threshold =$2 mA. $1:当前发送偏置电流值 $2:发送偏置电流低阈值
0600008	Transceiver bias current is too high: CurrentValue = $1 mA, Threshold =$2 mA. $1:当前发送偏置电流值 $2:发送偏置电流高阈值
0600007	Transceiver Rx power is too low: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际接收光功率 $2:光模块接收光功率低门限值
0600006	Transceiver Rx power is too high: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际接收光功率 $2:光模块接收光功率高门限值
0600005	Transceiver Tx power is too low: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际发送光功率值 $2:光模块发送光功率低门限值
0600004	Transceiver Tx power is too high: CurrentValue = $1 dBm, Threshold = $2 dBm. $1:光模块当前实际发送光功率 $2:光模块发送光功率高门限值
0600002	Transceiver module removed from $1. $1 接口索引（框/槽/子卡/接口） Transceiver removed.

112.17 OPTMOD_COUNTERFEIT_MODULE

日志内容	The following transceiver you are using is suspected to be a counterfeit/pirated/unauthorized H3C transceiver, which might cause compatibility problems and expose your device to security threats. Please contact H3C for further detection and verification promptly. [STRING]: Transceiver type [STRING], SN [STRING].
日志含义	您正在使用的如下光模块，被怀疑是伪造、盗版或未经授权的H3C光模块，这可能会导致兼容性问题并使您的设备面临安全威胁。请及时联系H3C进行进一步的检测和核实。
参数解释	$1：接口类型和编号 $2：接口模块型号 $3：光模块序列号
日志等级	3 (Error)
举例	OPTMOD/3/OPTMOD_COUNTERFEIT_MODULE: The following transceiver you are using is suspected to be a counterfeit/pirated/unauthorized H3C transceiver, which might cause compatibility problems and expose your device to security threats. Please contact H3C for further detection and verification promptly. GigabitEthernet1/0/1: Transceiver type 1000_BASE_SX_SFP, SN 2013AYU0711103. GigabitEthernet1/0/2: Transceiver type 1000_BASE_SX_SFP, SN 2013AYU0711103.
对系统的影响	光模块可能无法正常工作
日志产生原因	当检测到设备上可能存在伪造、盗版或未经授权的H3C光模块时，打印该日志。对于伪造、盗版或未经授权的H3C光模块，通过**display transceiver diagnosis**命令无法获取数据
处理建议	请购买并使用H3C原厂光模块

112.18 OPTMOD_FEC_CONFIGURATION_CLEAR

日志内容	[STRING]: The transceiver module does not support FEC mode setting and the FEC mode configuration has been cleared on the port.
日志含义	端口插入的光模块不支持FEC模式，端口下已有FEC模式配置已清除
参数解释	$1：端口名称
日志等级	5 (Notification)
举例	OPTMOD/5/OPTMOD_FEC_MODE_RESET: FourHundredGigE1/0/1: The transceiver module does not support FEC mode setting and the FEC mode configuration has been cleared on the port.
对系统的影响	对系统无影响
日志产生原因	端口下已有FEC模式配置，新插入的光模块不支持FEC模式时，打印该日志
处理建议	无需处理

112.19 OPTMOD_MODULE_CHECK

日志内容	An H3C transceiver is detected. Please go to the website www.h3c.com to verify its authenticity.
日志含义	检测到设备上存在H3C光模块，请前往H3C官网（www.h3c.com）进行条形码防伪查询
参数解释	无
日志等级	6 (Informational)
举例	OPTMOD/6/OPTMOD_MODULE_CHECK: An H3C transceiver is detected. Please go to the website www.h3c.com to verify its authenticity.
对系统的影响	对系统无影响
日志产生原因	检测到设备上存在H3C光模块时，会打印该日志。提醒用户到H3C官网（www.h3c.com）进行条形码防伪查询
处理建议	无需处理

112.20 PHONY_MODULE

日志内容	[STRING]: A non-H3C transceiver is detected. Please confirm the label of the transceiver. If there is an H3C Logo, it is suspected to be a counterfeit H3C transceiver. This transceiver is NOT sold by H3C. H3C therefore shall NOT guarantee the normal function of the device or assume the maintenance responsibility thereof!
日志含义	检测到非H3C生产的光模块。请确认光模块的标签，如果标签中有H3C标志，则怀疑是假冒的H3C光模块。这个光模块不是H3C售卖的。因此，H3C不能保证设备的正常功能，也不承担设备的维护责任！
参数解释	$1：端口名称
日志等级	4 (Warning)
举例	OPTMOD/4/PHONY_MODULE: GigabitEthernet1/0/1: A non-H3C transceiver is detected. Please confirm the label of the transceiver. If there is an H3C Logo, it is suspected to be a counterfeit H3C transceiver. This transceiver is NOT sold by H3C. H3C therefore shall NOT guarantee the normal function of the device or assume the maintenance responsibility thereof!
对系统的影响	光模块可能无法正常工作
日志产生原因	检测到非H3C生产的光模块时，打印该日志
处理建议	**1.** 请购买并使用 H3C 原厂光模块 **2.** 如果确认使用的是 H3C 光模块，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.21 RX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
日志含义	光模块RX故障被清除
参数解释	$1：端口名称 $2：RX故障类型
日志等级	3 (Error)
举例	OPTMOD/3/RX_ALM_OFF: GigabitEthernet1/0/1: RX_not_ready was removed.
对系统的影响	对系统无影响
日志产生原因	光模块RX故障被清除时，打印该日志
处理建议	无需处理

112.22 RX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
日志含义	检测到光模块RX故障
参数解释	$1：端口名称 $2：RX故障类型
日志等级	3 (Error)
举例	OPTMOD/3/RX_ALM_ON: GigabitEthernet1/0/1: RX_not_ready was detected.
对系统的影响	光模块可能无法正常工作
日志产生原因	检测到光模块RX故障时，打印该日志
处理建议	产生故障的原因可能是光模块本身的问题，也可能是端口、链路问题，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.23 RX_POW_HIGH

日志内容	[STRING]: RX power is high.
日志含义	光模块RX功率超过接收光功率高告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/RX_POW_HIGH: GigabitEthernet1/0/1: RX power is high.
对系统的影响	光模块可能无法正常工作
日志产生原因	光模块RX功率超过接收光功率高告警门限时，打印该日志
处理建议	**1.** 调整链路，增加光衰使光功率，使光模块收光功率满足正常的工作范围 **2.** 使用display transceive diagnosis interface命令查看功率是否已经超过接收光功率高告警门限 **3.** 使用display transceive alarm interface命令查看当前是否确实存在接收光功率高告警 **4.** 如果确实超过接收光功率高告警门限了，则表示光模块存在问题，请更换光模块

112.24 RX_POW_LOW

日志内容	[STRING]: RX power is low.
日志含义	光模块RX功率低于接收光功率低告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/RX_POW_LOW: GigabitEthernet1/0/1: RX power is low.
对系统的影响	光模块可能无法正常工作
日志产生原因	光模块RX功率低于接收光功率低告警门限时，打印该日志
处理建议	**1.** 调整链路，使光模块收光功率满足正常的工作范围 **2.** 使用display transceive diagnosis interface命令查看功率是否已经低于接收光功率低告警门限 **3.** 使用display transceive alarm interface命令查看当前是否确实存在接收光功率低告警 **4.** 如果确实低于接收光功率低告警门限了，则表示光模块存在问题，请更换光模块

112.25 RX_POW_NORMAL

日志内容	[STRING]: RX power is normal.
日志含义	光模块RX功率恢复至正常范围
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/RX_POW_NORMAL: GigabitEthernet1/0/1: RX power is normal.
对系统的影响	对系统无影响
日志产生原因	光模块RX功率恢复至正常范围时，打印该日志
处理建议	无需处理

112.26 TEMP_HIGH

日志内容	[STRING]: Temperature is high.
日志含义	光模块的温度超过温度高告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TEMP_HIGH: GigabitEthernet1/0/1: Temperature is high.
对系统的影响	温度过高会影响光模块正常工作
日志产生原因	光模块的温度超过温度高告警门限时，打印该日志
处理建议	**1.** 请检查机房现场环境温度是否过高，如果环境温度确实过高，请改善机房温度，保持设备环境正常通风 **2.** 检查设备风扇是否工作正常，如果风扇非正常工作，请安装风扇或更换故障风扇 **3.** 如果设备风扇正常，且环境温度正常，则表示光模块故障，请更换光模块

112.27 TEMP_LOW

日志内容	[STRING]: Temperature is low.
日志含义	光模块的温度低于温度低告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TEMP_LOW: GigabitEthernet1/0/1: Temperature is low.
对系统的影响	温度过低会影响光模块正常工作
日志产生原因	光模块的温度低于温度低告警门限时，打印该日志
处理建议	**1.** 请检查机房现场环境温度是否过低，如果环境温度确实过低，请改善机房温度 **2.** 如果环境温度正常，则表示光模块故障，请更换光模块

112.28 TEMP_NORMAL

日志内容	[STRING]: Temperature is normal.
日志含义	光模块温度恢复至正常范围
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TEMP_NORMAL: GigabitEthernet1/0/1: Temperature is normal.
对系统的影响	对系统无影响
日志产生原因	光模块温度恢复至正常范围时，打印该日志
处理建议	无需处理

112.29 TX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
日志含义	光模块TX故障被清除
参数解释	$1：端口名称 $2：TX故障类型
日志等级	3 (Error)
举例	OPTMOD/3/TX_ALM_OFF: GigabitEthernet1/0/1: TX_fault was removed.
对系统的影响	对系统无影响
日志产生原因	光模块TX故障被清除时，打印该日志
处理建议	无需处理

112.30 TX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
日志含义	检测到光模块TX故障
参数解释	$1：端口名称 $2：TX故障类型
日志等级	3 (Error)
举例	OPTMOD/3/TX_ALM_ON: GigabitEthernet1/0/1: TX_fault was detected.
对系统的影响	光模块可能无法正常工作
日志产生原因	检测到光模块TX故障时，打印该日志
处理建议	产生故障的原因可能是光模块本身的问题，也可能是端口、链路问题，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.31 TX_POW_HIGH

日志内容	[STRING]: TX power is high.
日志含义	光模块TX功率超过发送光功率高告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TX_POW_HIGH: GigabitEthernet1/0/1: TX power is high.
对系统的影响	光模块可能无法正常工作
日志产生原因	光模块TX功率超过发送光功率高告警门限时，打印该日志
处理建议	**1.** 调整链路，增加光衰使光功率，使光模块收光功率满足正常的工作范围 **2.** 使用display transceive diagnosis interface命令查看功率是否已经超过发送光功率高告警门限 **3.** 使用display transceive alarm interface命令查看当前是否确实存在发送光功率高告警 **4.** 如果确实超过发送光功率高告警门限了，则表示光模块存在问题，请更换光模块

112.32 TX_POW_LOW

日志内容	[STRING]: TX power is low.
日志含义	光模块TX功率低于发送光功率低告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TX_POW_LOW: GigabitEthernet1/0/1: TX power is low.
对系统的影响	光模块无法正常工作
日志产生原因	光模块TX功率低于发送光功率低告警门限时，打印该日志
处理建议	1. 确认端口状态是否为shutdown，如果状态为shutdown，请端口状态恢复为up 2. 使用display transceive diagnosis interface命令查看功率是否已经低于发送光功率低告警门限 3. 使用display transceive alarm interface命令查看当前是否确实存在发送光功率低告警 4. 如果确实低于发送光功率低告警门限了，则表示光模块存在问题，请更换光模块 5. 如果问题无法解决，有可能是单板问题（如关光、高速信号异常等），请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.33 TX_POW_NORMAL

日志内容	[STRING]: TX power is normal.
日志含义	光模块TX功率恢复至正常范围
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TX_POW_NORMAL: GigabitEthernet1/0/1: TX power is normal.
对系统的影响	对系统无影响
日志产生原因	光模块TX功率恢复至正常范围，打印该日志
处理建议	无需处理

112.34 TYPE_ERR

日志内容	[STRING]: The transceiver type is not supported by port hardware.
日志含义	端口硬件不支持光模块类型
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/TYPE_ERR: GigabitEthernet1/0/1: The transceiver type is not supported by port hardware.
对系统的影响	光模块无法正常工作
日志产生原因	端口硬件不支持光模块类型时，打印该日志
处理建议	1. 请更换光模块 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

112.35 VOLT_HIGH

日志内容	[STRING]: Voltage is high.
日志含义	光模块电压超过电压高告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/VOLT_HIGH: GigabitEthernet1/0/1: Voltage is high.
对系统的影响	光模块可能无法正常工作或者光模块被损坏
日志产生原因	光模块电压超过电压高告警门限时，打印该日志
处理建议	1. 判断端口是否工作正常，如果端口不能正常工作，请先确认端口问题并解决 2. 确认单板上其他光模块是否多次出现此故障，如果是，则说明单板可能存在器件故障，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 3. 使用display transceive diagnosis interface命令查看电压是否已经超过电压高告警门限 4. 使用display transceive alarm interface命令查看当前是否确实存在电压高告警 5. 如果确实超过电压高告警门限了，则表示光模块存在问题，请更换光模块

112.36 VOLT_LOW

日志内容	[STRING]: Voltage is low.
日志含义	光模块电压低于电压低告警门限
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/VOLT_LOW: GigabitEthernet1/0/1: Voltage is low.
对系统的影响	光模块可能无法正常工作
日志产生原因	光模块电压低于电压低告警门限时，打印该日志
处理建议	1. 判断端口是否工作正常，如果端口不能正常工作，请先确认端口问题并解决 2. 确认单板上其他光模块是否多次出现此故障，如果是，则说明单板可能存在器件故障，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 3. 使用display transceive diagnosis interface命令查看电压是否已经超过电压低告警门限 4. 使用display transceive alarm interface命令查看当前是否确实存在电压低告警 5. 如果确实低于电压低告警门限了，则表示光模块存在问题，请更换光模块

112.37 VOLT_NORMAL

日志内容	[STRING]: Voltage is normal.
日志含义	光模块电压恢复至正常范围
参数解释	$1：端口名称
日志等级	3 (Error)
举例	OPTMOD/3/VOLT_NORMAL: GigabitEthernet1/0/1: Voltage is normal!
对系统的影响	对系统无影响
日志产生原因	光模块电压恢复至正常范围时，打印该日志
处理建议	无需处理

113 OSPF

本节介绍 OSPF 模块输出的日志信息。

113.1 OSPF_DUP_RTRID_NBR

日志内容	OSPF [UINT16] Duplicate router ID [STRING] on interface [STRING], sourced from IP address [IPADDR].
日志含义	OSPF检测到直连邻居配置了相同的Router ID
参数解释	$1：OSPF进程ID $2：路由器ID $3：接口名称 $4：IP地址
日志等级	6 (Informational)
举例	OSPF/6/OSPF_DUP_RTRID_NBR: OSPF 1 Duplicate router ID 11.11.11.11 on interface GigabitEthernet0/0/3, sourced from IP address 11.2.2.2.
对系统的影响	Router LSA不断刷新，产生路由震荡
日志产生原因	两台直连设备配置了相同的路由器ID
处理建议	1. 请根据 OSPF 进程获取 Router ID 方式的不同，选择不同的处理步骤： ○ 如果OSPF进程使用的是全局Router ID，请使用 **router id**命令修改Router ID。 ○ 如果OSPF进程使用的是手工指定的Router ID，请使用 **ospf router-id**命令修改Router ID。 ○ 如果OSPF进程使用的是自动获取的Router ID，请使用 **ip address**命令修改Router ID对应的接口的IP地址。 2. 请使用 **reset ospf process**命令使新的路由器ID生效。

113.2 OSPF_IF_NETWORKTYPE_MISMATCH

日志内容	OSPF [UINT16] Network type is inconsistent. Local interface: [STRING], neighbor address: [IPADDR].
日志含义	本端OSPF接口和邻居OSPF接口的网络类型不一致
参数解释	$1：OSPF进程ID $2：接口名称 $3：邻居IP地址
日志等级	6 (Informational)
举例	OSPF/6/OSPF_IF_NETWORKTYPE_MISMATCH: OSPF 1 Network type is inconsistent. Local interface: GigabitEthernet0/0/1, neighbor address: 21.1.1.1.
对系统的影响	OSPF邻居关系建立失败。需要说明的是，如果双方一端为PTP，另一端为Broadcast，那么邻居关系可以达到Full状态，但无法计算出路由信息。
日志产生原因	两端OSPF接口的网络类型不一致
处理建议	1. 请进入日志信息中Local interface指示的接口视图下，然后执行 **ospf network-type**命令修改接口的网络类型，确保两端OSPF接口的网络类型一致。 2. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

113.3 OSPF_IP_CONFLICT_INTRA

日志内容	OSPF [UINT16] Received newer self-originated network-LSAs. Possible conflict of IP address [IPADDR] in area [STRING] on interface [STRING].
日志含义	OSPF收到更新的自己生成的Network LSA。可能是同一OSPF区域内两台设备的接口上配置了相同的IP地址导致的
参数解释	$1：OSPF进程ID $2：IP地址 $3：OSPF区域ID $4：接口名称
日志等级	6 (Informational)
举例	OSPF/6/OSPF_IP_CONFLICT_INTRA: OSPF 1 Received newer self-originated network-LSAs. Possible conflict of IP address 11.1.1.1 in area 0.0.0.1 on interface GigabitEthernet0/0/3.
对系统的影响	可能会对系统造成如下影响： • 设备 CPU 使用率较高 • OSPF 频繁地老化 LSA、重新生成 LSA • 设备路由频繁刷新、路由计算出错
日志产生原因	同一OSPF区域内两台设备的接口上可能配置了相同的主IP地址，其中至少一台设备是DR
处理建议	1. 请检查是否同时会生成 OSPF_RTRID_CONFLICT_INTRA，即是否存在同一 OSPF 区域内 Router ID 冲突的情况。 o 如果存在同一 OSPF 区域内 Router ID 冲突的情况，请根据 OSPF_RTRID_CONFLICT_INTRA 日志的处理建议解决 Router ID 冲突的问题。 o 如果不存在同一 OSPF 区域内 Router ID 冲突的情况，请执行步骤 2。 2. 查找日志信息中的接口信息，然后修改该接口的主 IP 地址，保证同一区域内设备接口使用不同的主 IP 地址。

113.4 OSPF_LAST_NBR_DOWN

日志内容	OSPF [UINT32] Last neighbor down event: Router ID: [STRING] Local address: [STRING] Remote address: [STRING] Reason: [STRING]
日志含义	OSPF邻居状态变为Down
参数解释	$1：OSPF进程ID $2：路由器ID $3：本地IP地址 $4：邻居IP地址 $5：OSPF邻居状态变为Down的原因，取值包括： • Ospf Interface Parameters Changed：OSPF 接口参数改变 • Reset ospf command was performed：重启 OSPF 进程 • Undo ospf command was performed：执行了 **undo ospf**命令 • Undo area command was performed：执行了 **undo area**命令 • Undo network：执行了 **undo network**命令 • Silent Interface：执行了 **silent interface**命令 • Ospf_iflchange：接口逻辑属性变化 • Ospf_ifachange：接口物理属性变化 • Ospf_ifvchange：接口 vlink 属性变化 • Vlink down：虚连接接口 down • Shamlink down：伪连接接口 down • DeadInterval timer expired：Dead 定时器超时 • Configuring stub area：Stub 区域配置变化 • Configuring nssa area：NSSA 区域配置变化 • Opaque-Capability changed：**opaque-capability enable**配置变化 • Out-of-Band Resynchronazition Capability changed：**enable out-of-band-resynchronization**配置变化 • BFD session down：BFD 会话 down • Database-filter or referenced ACL changed：对发送给指定邻居的 LSA 进行过滤的配置发生变化或者该配置引用的 ACL 规则改变 • shutdown：配置了 **shutdown process**命令
日志等级	6 (Informational)
举例	OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 2.2.2.2 Local address: 10.1.1.1 Remote address: 10.1.1.2 Reason: Dead Interval timer expired.
对系统的影响	可能导致业务中断
日志产生原因	• 邻接定时器超时 • 物理接口变化 • OSPF 联动的 BFD 会话 Down • OSPF 配置发生变化 • 邻居设备原因

处理建议	OSPF邻居down的原因为邻接定时器超时，处理建议如下： **1.** 请执行 **ping**命令，检查设备链路是否故障（包括传输设备故障）。 o 如果 ping 不通，请检查传输设备、链路情况、接口情况，通过调整硬件设备恢复业务。 o 如果能 ping 通，则请执行步骤 2。 **2.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。 OSPF邻居down的原因为物理接口变化，处理建议如下： **3.** 请执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令检查建立OSPF邻居关系的物理接口状态是否良好。 o 如果接口的物理状态为 DOWN，请检查传输设备是否正常，通过恢复物理接口状态来消除故障。 o 如果接口的物理状态为“Administratively DOWN”，说明该接口被人为执行 **shutdown**命令关闭，请在接口下执行 **undo shutdown**命令打开接口。 o 如果接口的物理状态为“UP”，则请执行步骤 2。 **4.** 请执行 **display ospf interface**命令查看接口在OSPF协议下状态是否为正常状态。 o 如果 OSPF 接口状态为 Down，请检查接口下是否配置了 IP 地址、IP 地址配置是否正确，通过对 IP 地址的检查来消除故障。 o 如果 OSPF 接口状态为 P-2-P、DR、BDR 或 DROther，则请执行步骤 3。 **5.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。 OSPF邻居down的原因为BFD会话down，处理建议如下： **6.** 请执行 **ping**命令，检查设备链路是否故障（包括传输设备故障）。 o 如果 ping 不通，请检查传输设备、链路情况、接口情况，通过调整硬件设备恢复业务。 o 如果能 ping 通，则请执行步骤 2。 **7.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。 OSPF邻居down的原因为配置变化，处理建议如下： **8.** 请使用 **display ospf interface**命令检查两端OSPF Area ID配置是否一致。 o 如果一致，请执行步骤 2。 o 如果不一致，请修改为一致。 **9.** 请在使用 **display ospf interface**命令检查本端和对端接口的网络类型是否一致。 o 如果不一致，请修改为一致。 o 如果一致，则请执行步骤 3。 **10.** 请每隔 10 秒钟使用 **display ospf statistics error**命令检查一次OSPF的错误统计信息，并持续 5 分钟。 o 如果 Bad authentication type 字段对应的计数值一直增长，表示建立邻居的两台设备配置的 OSPF 认证类型不一致，需要在两端设备上配置相同认证的类型。 o 如果 Hello-time mismatch 字段对应的计数值一直在增长，表示接口上的 Hello 定时器的值不一致，需要将两端接口的 Hello 定时器的值设置为一致。 o 如果 Dead-time mismatch 字段对应的计数值一直在增长，表示接口上的 Dead 定时器的值不一致，需要将两端接口的 Dead 定时器的值设置为一致。 o 如果 Ebit option mismatch 字段对应的计数值一直在增长，表示区域类型配置不一致（一端配置为普通区域，另一端配置为 Stub 或 NSSA 区域），需要将两端的区域类型设置为一致。 **11.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

113.5 OSPF_NBR_CHG

日志内容	OSPF [UINT32] Neighbor [STRING] ([STRING]) changed from [STRING] to [STRING].
日志含义	OSPF邻居状态发生变化
参数解释	$1：OSPF进程ID $2：邻居路由器ID $3：接口名称 $4：旧邻接状态 $5：新邻接状态
日志等级	5 (Notification)
举例	OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 12.1.1.2(GigabitEthernet10/1) changed from FULL to DOWN.
对系统的影响	OSPF邻居状态变化顺序从低到高为：Down->Init->2-Way->ExStart->Exchange->Loading->Full。如果邻居状态由较低状态变为较高状态，则属于正常运行信息，无需关注。如果邻居状态由较高状态变为较低状态，则可能导致业务中断
日志产生原因	以下原因可能会导致OSPF邻居状态从2-way或Full状态变为其他状态： • 链路故障，OSPF 报文被丢弃 • 接口的 DR 优先级配置不合理 • 两端配置的 OSPF MTU 值不同 • 邻接定时器超时 • OSPF 联动的 BFD 会话状态变为 Down

处理建议	1. 请执行 **display ospf peer**命令查看“State”字段，该字段的取值为邻居状态。如果邻居状态为Full，则属于正常运行信息，无需处理。否则，请执行步骤 2。
	2. 请执行 **display interface** *interface-type interface-number*命令查看连接邻居的接口的状态。
	  ○ 如果物理接口状态为 Up，请执行步骤 3。
	  ○ 如果物理接口状态为Down，请检查该接口下是否配置了 **shutdown**命令。如果配置了 **shutdown**命令，请执行 **undo shutdown**命令，然后执行步骤 3。如果没有配置 **shutdown**命令，请执行步骤 3。
	3. 检查能否 ping 通对端接口 IP 地址。
	  ○ 如果 ping 不通，请执行步骤 6。
	  ○ 如果可以 ping 通，请执行步骤 4。
	4. 请执行 **display ospf interface**命令查看“State”字段，该字段的取值为OSPF接口的状态。
	  ○ 如果与对端建立邻居关系的接口处于 Down 状态，请执行步骤 6。
	  ○ 如果与对端建立邻居关系的接口处于非 Down 状态，请执行步骤 5。
	5. 请执行 **display ospf interface verbose**命令检查本端设备与对端设备配置的参数是否一致，包括：Hello定时器、Dead定时器、Poll定时器、OSPF网络类型、认证。如果两端配置的参数一致，请执行步骤 6。如果两端配置的参数不一致，请通过如下命令修改配置，保证两端参数一致。
	  ○ **ospf timer hello**
	  ○ **ospf timer dead**
	  ○ **ospf timer poll**

	○ **`ospf network-type`** ○ **`ospf authentication-mode`** **6.** 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

113.6 OSPF_NBR_CHG_REASON

日志内容	OSPF [UINT32] Area [STRING] Router [STRING]([STRING]) CPU usage: [STRING], VPN name: [STRING], IfMTU: [UINT32], Neighbor address: [STRING], NbrID [STRING] changed from [STRING] to [STRING] at [STRING]. Last 4 hello packets received at: [STRING] Last 4 hello packets sent at: [STRING]
日志含义	OSPF邻居状态发生变化的原因
参数解释	$1：OSPF进程ID $2：区域ID $3：路由ID $4：接口简名 $5：CPU使用率 $6：VPN名称。仅OSPF多实例进程的邻居状态变化日志信息中会显示VPN名称 $7：接口MTU大小 $8：邻居的IP地址 $9：邻居的路由器ID $10：变化前的邻居状态 $11：变化后的邻居状态和状态变化原因 • to DOWN because OSPF interface parameters changed：OSPF 接口参数改变导致邻居关系断开 • to DOWN because the OSPF process was reset：重启 OSPF 进程导致邻居关系断开 • to DOWN because the OSPF process was deleted：删除 OSPF 进程导致邻居关系断开 • to DOWN because the OSPF area was deleted：删除 OSPF 区域导致邻居关系断开 • to DOWN because OSPF was disabled (Interface: *interface*, peer address: *address*)：关闭指定网段接口上的OSPF功能导致邻居关系断开 • to DOWN because OSPF packet receiving and sending are disabled (Interface: *interface*, peer address: *address*)：接口禁止收发OSPF报文导致邻居关系断开 • to DOWN because the interface address was deleted or OSPF was disabled on interface：删除接口地址或者在接口上关闭 OSPF 导致邻居关系断开 • to DOWN because the interface went down or MTU changed：接口 down 或者接口 MTU 改变导致邻居关系断开 • to DOWN because the virtual link was deleted or the route it relies on was deleted：虚连接删除或者其依赖的路由删除导致邻居关系断开 • to DOWN because to DOWN because the virtual link interface went down or the virtual link settings were deleted：虚连接接口 down 或者删除虚连接配置导致邻居关系断开 • to DOWN because the sham link was deleted or the route it relies on was deleted：删除伪连接或者其依赖的路由删除导致邻居关系断开 • to DOWN because the dead timer expired：Dead 定时器超时导致 OSPF 邻居关系断开

	• to DOWN because the stub configuration changed in area *area-id*：Stub区域配置变化导致邻居关系断开 • to DOWN because the NSSA configuration changed in area *area-id*：NSSA区域配置变化导致邻居关系断开 • to DOWN because the Opaque LSA capability configuration changed：Opaque LSA 发布接收能力配置改变导致邻居关系断开 • to DOWN because the out-of-band resynchronization capability configuration changed：OSPF 带外同步能力配置改变导致邻居关系断开 • to DOWN because BFD session went down：BFD 会话 Down 导致 OSPF 邻居关系断开 • to INIT because a 1-way hello packet was received：接收到 1-way 的 Hello 报文导致邻居状态变为 Init • to DOWN because database-filter configuration changed or database-filter ACL configuration changed：对发送给指定邻居的 LSA 进行过滤的配置发生变化或者该配置引用的 ACL 规则改变导致邻居关系断开 • to EXSTART because a BadLSReq event was triggered upon the request for a nonexistent LSA：由于收到的 LSR 报文请求的是本地并不存在的 LSA，触发了 BadLSReq 事件导致邻居状态变为 Exstart • to EXSTART because the LSA requested and then learned is the same as that in local：本端向对端请求更新一条 LSA，对端回复的 LSA 与本端 LSDB 中已有的 LSA 相同，导致邻居状态变为 Exstart • to EXSTART because the LSA requested and then learned is older than that in local：本端向对端请求更新一条 LSA，对端回复的 LSA 比本端 LSDB 中已有的 LSA 旧，导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a non-retransmitted DD packet from the Loading or Full peer during the DD retransmit interval：邻居状态到达 Loading 或 Full，但在 DD 重传时间间隔内收到了非请求重传的 DD 报文，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered by the change of the OSPF peer’s capability to link-local signaling attribute：接收到邻居发送的 DD 报文中的 L 位发生变化，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered by the OSPF peer’s multi-topology attribute change：邻居支持多拓扑属性发生变化，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a retransmitted DD packet from the Loading or Full peer after the DD retransmit interval expired：邻居状态到达 Loading 或 Full，在 DD 重传时间间隔超时后又收到了重传的 DD 报文，触发了 SeqNumberMismatch 事件导致邻居状态改为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered by the change of the OSPF peer’s capability to receive AS external LSA：接收到邻居发送的 DD 报文中的 E 位发生变化，触发了 SeqNumberMismatch 事件导致邻居状态改为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered by the master-slave relationship change：与邻居交互的主从关系发生改变，触发了 SeqNumberMismatch 事件导致邻居关系降为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of an unexpected initial DD packet after DD transmission started：开始通过 DD 报文交互 DB 摘要的时候，收到了初始 DD 包，触发了 SeqNumberMismatch 事件导致邻居关系降为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet with a wrong sequence number from the slave：Master 收到 Slave

	发送的序列号错误的DD报文，触发了SeqNumberMismatch事件导致邻居状态变为Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet with a wrong sequence number from the master：Slave 接收到 Master 发送的序列号错误的 DD 报文中，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing local opaque LSA without enabling the opaque capability：接收到的 DD 报文包含了 Type-9 LSA，但本地未使能 Opaque LSA 发布接收能力，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing area opaque LSA without enabling the opaque capability：接收到的 DD 报文包含了 Type-10 LSA，但本地未使能 Opaque LSA 发布接收能力，触发了 SeqNumberMismatch 事件导致邻居关系降为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing AS opaque LSA without enabling the opaque capability：接收到的 DD 报文包含了 Type-11 LSA，但本地未使能 Opaque LSA 发布接收能力，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing NSSA external LSA in a non-NSSA area：在非 NSSA 区域收到了含有 Type-7 LSA 的 DD 报文，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing invalid LSA：接收到的 DD 报文中含有无效 LSA，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart • to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing AS external LSA in the stub area or on the virtual link：在 Stub 区域或虚连接上接收到了包含 Type-5 LSA 的 DD 报文，触发了 SeqNumberMismatch 事件导致邻居状态变为 Exstart $12：邻居状态改变的时间 $13：邻居状态改变前接收的4个Hello报文的时间 $14：邻居状态改变前发送的4个Hello报文的时间

日志等级	5 (Notification)
举例	OSPF/5/OSPF_NBR_CHG_REASON: OSPF 1 Area 0.0.0.0 Router 2.2.2.2(GE1/0/1) CPU usage:3.80%, VPN name: a, IfMTU:1500, Neighbor address:10.1.1.2, NbrID:1.1.1.1 changed from Full to Down because OSPF interface parameters changed at 2019-09-01 15:20:57:034. Last 4 hello packets received at: 2019-09-01 15:19:46:225 2019-09-01 15:19:56:224 2019-09-01 15:20:06:225 2019-09-01 15:20:16:225 Last 4 hello packets sent at: 2019-09-01 15:20:22:033 2019-09-01 15:20:32:033 2019-09-01 15:20:42:032 2019-09-01 15:20:52:033
对系统的影响	OSPF邻居状态变化顺序从低到高为：Down->Init->2-Way->ExStart->Exchange->Loading->Full。如果邻居状态由较低状态变为较高状态，则属于正常运行信息，无需关注。如果邻居状态由较高状态变为较低状态，则可能导致业务中断
日志产生原因	• OSPF 邻接状态由 Attempt 等状态变为 1-way 或 Down，或者由 Down 等状态变为 2-way 或 Full。 • 本端或对端的接口配置参数（如 Hello 定时器、Dead 定时器、接口认证等）不一致。 • 通过执行 **reset ospf process**命令重启OSPF协议。 • NBMA 网络或者广播网络上的接口邻接状态由 Full 变为其他状态，或者由其他状态变为 Full。
处理建议	**1.** 请执行 **display ospf peer**命令查看“State”字段，该字段的取值为邻居状态。如果邻居状态为Full，则属于正常运行信息，无需处理。否则，请执行步骤 2。 **2.** 请执行 **display interface** *interface-type interface-number*命令查看连接邻居的接口的状态。 o 如果物理接口状态为 Up，请执行步骤 3。 o 如果物理接口状态为Down，请检查该接口下是否配置了 **shutdown**命令。如果配置了 **shutdown**命令，请执行 **undo shutdown**命令，然后执行步骤 3。如果没有配置 **shutdown**命令，请执行步骤 3。 **3.** 检查能否 ping 通对端接口 IP 地址。 o 如果 ping 不通，请执行步骤 6。 o 如果可以 ping 通，请执行步骤 4。 **4.** 请执行 **display ospf interface**命令查看“State”字段，该字段的取值为OSPF接口的状态。 o 如果与对端建立邻居关系的接口处于 Down 状态，请执行步骤 6。 o 如果与对端建立邻居关系的接口处于非 Down 状态，请执行步骤 5。 **5.** 请执行 **display ospf interface verbose**命令检查本端设备与对端设备配置的参数是否一致。 o 如果不一致，请修改为一致。 o 如果一致，请执行步骤 6。 **6.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

113.7 OSPF_RTRID_CHG

日志内容	OSPF [UINT32] New router ID elected, please restart OSPF if you want to make the new Router ID take effect.
日志含义	OSPF进程选出了新的Router ID，重启进程后新的Router ID生效
参数解释	$1：OSPF进程ID
日志等级	5 (Notification)
举例	OSPF/5/OSPF_RTRID_CHG: OSPF 1 New router ID elected, please restart OSPF if you want to make the new Router ID take effect.
对系统的影响	对系统无影响
日志产生原因	用户更改了Router ID或者是使用的接口IP发生变化而改变了OSPF路由器ID。需要手动重启OSPF使新的路由器ID生效
处理建议	如果希望新的Router ID生效，请保证重启进程不会影响当前业务的前提下，使用**reset ospf process**命令使新的路由器ID生效

113.8 OSPF_RTRID_CONFLICT_INTER

日志内容	OSPF [UINT16] Received newer self-originated ase-LSAs. Possible conflict of router ID [STRING].
日志含义	可能是Router ID冲突导致OSPF进程收到更新的自己生成的AS External LSA
参数解释	$1：OSPF进程ID $2：路由器ID
日志等级	6 (Informational)
举例	OSPF/6/OSPF_RTRID_CONFLICT_INTER: OSPF 1 Received newer self-originated ase-LSAs. Possible conflict of router ID 11.11.11.11.
对系统的影响	AS External LSA不断刷新，ASBR引入的外部路由不断震荡
日志产生原因	同一OSPF域内非直连的两台设备可能配置了相同的路由器ID，其中一台设备为ASBR
处理建议	1. 请根据 OSPF 进程获取 Router ID 方式的不同，选择不同的处理步骤： ○ 如果OSPF进程使用的是全局Router ID，请使用 **router id**命令修改Router ID。 ○ 如果OSPF进程使用的是手工指定的Router ID，请使用 **ospf router-id**命令修改Router ID。 ○ 如果OSPF进程使用的是自动获取的Router ID，请使用 **ip address**命令修改Router ID对应的接口的IP地址。 2. 请使用 **reset ospf process**命令使新的路由器ID生效

113.9 OSPF_RTRID_CONFLICT_INTRA

日志内容	OSPF [UINT16] Received newer self-originated router-LSAs. Possible conflict of router ID [STRING] in area [STRING].
日志含义	可能是Router ID冲突导致OSPF进程收到更新的自己生成的Router LSA
参数解释	$1：OSPF进程ID $2：路由器ID $3：OSPF区域ID
日志等级	6 (Informational)
举例	OSPF/6/OSPF_RTRID_CONFLICT_INTRA: OSPF 1 Received newer self-originated router-LSAs. Possible conflict of router ID 11.11.11.11 in area 0.0.0.1.
对系统的影响	Router LSA不断刷新，路由震荡
日志产生原因	同一OSPF区域内非直连的两台设备可能配置了相同的路由器ID
处理建议	1. 请根据 OSPF 进程获取 Router ID 方式的不同，选择不同的处理步骤： ○ 如果OSPF进程使用的是全局Router ID，请使用 **router id**命令修改Router ID。 ○ 如果OSPF进程使用的是手工指定的Router ID，请使用 **ospf router-id**命令修改Router ID。 ○ 如果OSPF进程使用的是自动获取的Router ID，请使用 **ip address**命令修改Router ID对应的接口的IP地址。 2. 请使用 **reset ospf process**命令使新的路由器ID生效。

113.10 OSPF_VLINKID_CHG

日志内容	OSPF [UINT32] Router ID changed, reconfigure Vlink on peer
日志含义	本端OSPF进程的Router ID发生变化，需要修改对端设备的虚连接配置
参数解释	$1：OSPF进程ID
日志等级	5 (Notification)
举例	OSPF/5/OSPF_VLINKID_CHG:OSPF 1 Router ID changed, reconfigure Vlink on peer
对系统的影响	需要修改对端设备的虚连接配置
日志产生原因	本端OSPF进程新的Router ID生效
处理建议	1. 请使用 **display ospf** *process-id*命令查看OSPF进程的Router ID，*process-id*为本日志中的OSPF进程ID。 2. 请在对端设备上通过 **undo vlink-peer**命令删除原有的虚连接配置。然后，通过 **vlink-peer**命令重新配置虚连接，并指定步骤 1 中的Router ID作为虚连接邻居的Router ID。

114 OSPFV3

本节介绍 OSPFv3 模块输出的日志信息。

114.1 OSPFV3_DUP_RTRID_NBR

日志内容	OSPFv3 [UINT32] Interface [STRING] and neighbor [IPADDR] have the same router ID [STRING].
日志含义	OSPFv3检测到直连邻居配置了相同的Router ID
参数解释	$1：OSPFv3进程ID $2：接口名称 $3：邻居地址 $4：路由器ID
日志等级	6 (Informational)
举例	OSPFV3/6/OSPFV3_DUP_RTRID_NBR: OSPFv3 1 Interface GigabitEthernet0/0/3 and neighbor FE80::1 have the same router ID 1.1.1.1.
对系统的影响	Router LSA不断刷新，产生路由震荡
日志产生原因	两台直连设备配置了相同的路由器ID
处理建议	1. 请检查日志信息中的 OSPFv3 进程号，并进入该进程视图下。 2. 请执行 **undo router-id**命令删除原有的Router ID配置。 3. 请执行 **router-id**命令配置新的Router ID，并确保新的Router ID不会与日志信息中的Router ID相同。

114.2 OSPFV3_IF_NETWORKTYPE_MISMATCH

日志内容	OSPFv3 [UINT16] Network type is inconsistent. Local interface: [STRING], neighbor address: [IPV6ADDR].
日志含义	本端OSPF接口和邻居OSPF接口的网络类型不一致
参数解释	$1：OSPFv3进程ID $2：接口名称 $3：邻居IPv6地址
日志等级	6 (Informational)
举例	OSPFV3/6/OSPFV3_IF_NETWORKTYPE_MISMATCH: OSPFv3 1 Network type is inconsistent. Local interface: GigabitEthernet0/0/1, neighbor address: FE80::4A21:D0FF:0102:0304.
对系统的影响	OSPFv3邻居关系建立失败。需要说明的是，如果双方一端为PTP，另一端为Broadcast，那么邻居关系可以达到Full状态，但无法计算出路由信息。
日志产生原因	两端OSPFv3接口的网络类型不一致
处理建议	1. 请进入日志信息中Local interface指示的接口视图下，然后执行 **ospfv3 network-type**命令修改接口的网络类型，确保两端OSPFv3 接口的网络类型一致。 2. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

114.3 OSPFV3_LAST_NBR_DOWN

日志内容	OSPFv3 [UINT32] Last neighbor down event: Router ID: [STRING] Local interface ID: [UINT32] Remote interface ID: [UINT32] Reason: [STRING].
日志含义	OSPFv3邻居状态变为Down
参数解释	$1：OSPFv3进程ID $2：路由器ID $3：本地接口ID $4：对端接口ID $5：OSPFv3邻居状态变为Down的原因包括： • 1-Way：收到 1-Way 事件 • SeqMsmatch：收到 SeqNumberMismatch 事件 • BadLsreq：收到 BadLSReq 事件 • Ospfv3 Interface Parameters Changed：接口配置变化 • Reset ospfv3 command was performed：执行了 **reset ospfv3 process**命令 • Undo ospfv3 command was performed：执行了 **undo ospfv3**命令 • Undo area command was performed：执行了 **undo area**命令 • Undo ospfv3 interface：接口上关闭 OSPFv3 功能 • Ospfv3 iflchange：接口逻辑属性变化 • Ospfv3 ifachange：接口物理属性变化 • DeadInterval timer expired：Dead 定时器超时 • BFD session down：BFD 会话 down • Silent Interface：执行了 **silent interface**命令 • Configuring stub area：stub 区域配置变化 • Vlink down：虚连接接口 down • Configuring nssa area：NSSA 区域配置变化 • Shamlink down：伪连接接口 down
日志等级	6 (Informational)
举例	OSPFV3/6/OSPFV3_LAST_NBR_DOWN: OSPFv3 1 Last neighbor down event: Router ID: 2.2.2.2 Local interface ID: 1111 Remote interface ID: 2222 Reason: Dead Interval timer expired.
对系统的影响	可能导致业务中断
日志产生原因	• 邻接定时器超时 • 物理接口变化 • OSPFv3 联动的 BFD 会话 Down • OSPFv3 配置发生变化 • 邻居设备原因
处理建议	OSPFv3邻居down的原因为邻接定时器超时，处理建议如下： 1. 请执行 **ping**命令，检查设备链路是否故障（包括传输设备故障）。 ○ 如果 ping 不通，请检查传输设备、链路情况、接口情况，通过调整硬件设备恢复业务。

- 如果能 ping 通，则请执行步骤 2。

2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

OSPFv3邻居down的原因为物理接口变化，处理建议如下：

3. 请执行 **display ipv6 interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令检查建立OSPFv3 邻居关系的物理接口状态是否良好。

- 如果接口的物理状态为 DOWN，请检查传输设备是否正常，通过恢复物理接口状态来消除故障。
- 如果接口的物理状态为“Administratively DOWN”，说明该接口被人为执行 **shutdown**命令关闭，请在接口下执行 **undo shutdown**命令打开接口。
- 如果接口的物理状态为“UP”，则请执行步骤 2。

4. 请执行 **display ospfv3 interface**命令查看接口在OSPFv3 协议下状态是否为正常状态。

- 如果与对端建立邻居关系的接口处于 Down 状态，则请执行步骤 4。
- 如果 OSPFv3 接口状态为 P-2-P、DR、BDR 或 DROther，请执行步骤 3。

5. 请执行 **display ospfv3 interface verbose**命令检查本端设备与对端设备配置的参数是否一致。

- 如果一致，则请执行步骤 4。
- 如果不一致，请修改为一致。

6. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

OSPFv3邻居down的原因为BFD会话down，处理建议如下：

7. 请执行 **ping**命令，检查设备链路是否故障（包括传输设备故障）。

- 如果 ping 不通，请检查传输设备、链路情况、接口情况，通过调整硬件设备恢复业务。
- 如果能 ping 通，则请执行步骤 2。

8. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

OSPFv3邻居down的原因为配置变化，处理建议如下：

9. 请使用 **display ospfv3 interface**命令检查两端OSPFv3 Area ID配置是否一致。

- 如果一致，请执行步骤 2。
- 如果不一致，请修改为一致。

10. 请在使用 **display ospfv3 interface**命令检查本端和对端接口的网络类型是否一致。

- 如果不一致，请修改为一致。
- 如果一致，则请执行步骤 3。

11. 请每隔 10 秒钟使用 **display ospfv3 statistics error**命令检查一次OSPFv3 的错误统计信息，并持续 5 分钟。

- 如果 Authentication failure 字段对应的计数值一直增长，表示建立邻居的两台设备配置的 OSPFv3 认证类型不一致，需要在两端设备上配置相同类型的认证。
- 如果 Hello-time mismatch 字段对应的计数值一直在增长，表示接口上的 Hello 定时器的值不一致，需要将两端接口的 Hello 定时器的值设置为一致。
- 如果 Dead-time mismatch 字段对应的计数值一直在增长，表示接口上的 Dead 定时器的值不一致，需要将两端接口的 Dead 定时器的值设置为一致。
- 如果 Ebit option mismatch 字段对应的计数值一直在增长，表示区域类型配置不一致（一端配置为普通区域，另一端配置为 Stub 或 NSSA 区域），需要将两端的区域类型设置为一致。

	12. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

114.4 OSPFV3_NBR_CHG

日志内容	OSPFv3 [UINT32] Neighbor [STRING] ([STRING]) received [STRING] and its state from [STRING] to [STRING].
日志含义	OSPFv3邻居状态发生变化
参数解释	$1：OSPFv3进程ID $2：邻居路由器ID $3：接口名称 $4：邻居事件 $5：旧邻接状态 $6：新邻接状态
日志等级	5 (Notification)
举例	OSPFV3/5/OSPFV3_NBR_CHG: OSPFv3 1 Neighbor 2.2.2.2 (Vlan100) received 1-Way and its state from Full to Init.
对系统的影响	OSPFv3邻居状态变化顺序从低到高为：Down->Init->2-Way->ExStart->Exchange->Loading->Full。如果邻居状态由较低状态变为较高状态，则属于正常运行信息，无需关注。如果邻居状态由较高状态变为较低状态，则可能导致业务中断
日志产生原因	以下原因可能会导致OSPF邻居状态从2-way或Full状态变为其他状态： • 链路故障，OSPF 报文被丢弃 • 接口的 DR 优先级配置不合理 • 两端配置的 OSPF MTU 值不同 • 邻接定时器超时 • OSPF 联动的 BFD 会话状态变为 Down
处理建议	13. 请执行 **display ospfv3 peer**命令查看“State”字段，该字段的取值为邻居状态。如果邻居状态为Full，则属于正常运行信息，无需处理。否则，请执行步骤 2。 14. 请执行 **display interface** *interface-type interface-number*命令查看连接邻居的接口的状态。 o 如果物理接口状态为 Up，请执行步骤 3。 o 如果物理接口状态为Down，请检查该接口下是否配置了 **shutdown**命令。如果配置了 **shutdown**命令，请执行 **undo shutdown**命令，然后执行步骤 3。如果没有配置 **shutdown**命令，请执行步骤 3。 15. 检查能否 ping 通对端接口 IP 地址。 o 如果 ping 不通，请执行步骤 6。 o 如果可以 ping 通，请执行步骤 4。 16. 请执行 **display ospfv3 interface**命令查看“State”字段，该字段的取值为 OSPFv3 接口的状态。 o 如果与对端建立邻居关系的接口处于 Down 状态，请执行步骤 6。 o 如果与对端建立邻居关系的接口处于非 Down 状态，请执行步骤 5。 17. 请执行 **display ospfv3 interface verbose**命令检查本端设备与对端设备配置的参数是否一致，包括：Hello定时器、Dead定时器、Poll定时器、OSPFv3 网络类型、认证。如果两端配置的参数一致，请执行步骤 6。如果两端配置的参数不一致，请通过如下命令修改配置，保证两端参数一致。 o **ospfv3 timer hello**

	○ **ospfv3 timer dead** ○ **ospfv3 timer poll** ○ **ospfv3 network-type** ○ **ospfv3 authentication-mode** **18.** 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

114.5 OSPFV3_RTRID_CONFLICT_INTER

日志内容	OSPFv3 [UINT16] Received newer self-originated ase-LSAs. Possible conflict of router ID [STRING].
日志含义	可能是Router ID冲突导致OSPFv3进程收到更新的自己生成的AS External LSA
参数解释	$1：OSPFv3进程ID $2：本进程的路由器ID
日志等级	6 (Informational)
举例	OSPFV3/6/OSPFV3_RTRID_CONFLICT_INTER: OSPFv3 1 Received newer self-originated ase-LSAs. Possible conflict of router ID 1.2.3.5.
对系统的影响	AS External LSA不断刷新，ASBR引入的外部路由不断震荡
日志产生原因	同一OSPFv3区域内非直连的两台设备可能配置了相同的路由器ID，且其中一台设备为ASBR，导致OSPFv3进程收到更新的自己生成的AS External LSA
处理建议	**1.** 请检查日志信息中的OSPFv3 进程号，然后进入该OSPFv3 进程视图，使用 **undo router-id**命令删除Router ID。再使用 **router-id**命令重新配置该进程的Router ID。 **2.** 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

114.6 OSPFV3_RTRID_CONFLICT_INTRA

日志内容	OSPFv3 [UINT16] Received newer self-originated router-LSAs. Possible conflict of router ID [STRING] in area [STRING].
日志含义	可能是Router ID冲突导致OSPFv3进程收到更新的自己生成的Router LSA
参数解释	$1：OSPFv3进程ID $2：本进程的路由器ID $3：区域ID
日志等级	6 (Informational)
举例	OSPFV3/6/OSPFV3_RTRID_CONFLICT_INTRA: OSPFv3 1 Received newer self-originated router-LSAs. Possible conflict of router ID 1.1.1.1 in area 0.0.0.0.
对系统的影响	Router LSA不断刷新，路由震荡
日志产生原因	同一OSPFv3区域内非直连的两台设备可能配置了相同的路由器ID，导致OSPFv3进程收到更新的自己生成的Router LSA
处理建议	1. 请检查日志信息中的OSPFv3 进程号，然后进入该OSPFv3 进程视图，使用 **undo router-id**命令删除Router ID。再使用 **router-id**命令重新配置该进程的Router ID。 2. 执行以上操作后，若问题仍未解决，则请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

115 PBB

本节介绍 PBB 模块输出的日志信息。

115.1 PBB_JOINAGG_WARNING

日志内容	Because the aggregate interface [STRING] has been configured with PBB, assigning the interface [STRING] that does not support PBB to the aggregation group will cause incorrect processing.
日志含义	无法将不支持PBB的接口加入配置了PBB的二层聚合接口
参数解释	$1：聚合组名称 $2：接口名称
日志等级	4 (Warning)
举例	PBB/4/PBB_JOINAGG_WARNING: Because the aggregate interface Bridge-Aggregation1 has been configured with PBB, assigning the interface Ten-GigabitEthernet9/0/30 that does not support PBB to the aggregation group will cause incorrect processing.
对系统的影响	引发系统处理错误，PBB功能无法正常运行
日志产生原因	将不支持PBB的接口加入已经配置了PBB的二层聚合接口
处理建议	由于配置为PBB实例上行口的二层聚合接口要求其所有成员端口都支持PBB，请将不支持PBB的成员端口从该二层聚合组中删除

116 PBR

本节介绍 PBR 模块输出的日志信息。

116.1 PBR_HARDWARE_ERROR

日志内容	Failed to update policy [STRING] because of [STRING].
日志含义	策略路由配置更新失败
参数解释	$1：策略名 $2：硬件处理失败的原因，包括以下三种类型： • insufficient hardware resources：硬件资源不足 • unsupported operations：系统不支持该操作 • insufficient hardware resources and unsupported operations：硬件资源不足且系统不支持该操作
日志等级	4 (Warning)
举例	PBR/4/PBR_HARDWARE_ERROR: Failed to update policy aaa because of insufficient hardware resources and not supported operations.
对系统的影响	无法使用最新的策略路由配置指导报文转发
日志产生原因	更新单播策略路由配置失败
处理建议	根据失败原因修改策略中的配置： • 如果提示硬件资源不足，则检查设备上的策略路由配置，并删除不必要的配置。 • 如果提示系统不支持该操作，则检查策略路由配置中是否存在设备不支持的 **if-match**或 **apply**子句。 • 如果提示硬件资源不足且系统不支持该操作，则同时检查设备上是否存在不必要的策略路由配置，和策略路由中是否存在不支持的子句

117 PCE

本节介绍 PCE 模块输出的日志信息。

117.1 PCE_PCEP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
日志含义	PECP会话状态发生变化
参数解释	$1：会话对端IP地址 $2：会话所在VPN实例名称，如果无法获取则显示为unknown $3：会话的状态变更，up或者down，如果状态变更为down，则一并显示会话down的原因
日志等级	3 (Error)
举例	PCE/3/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is up. PCE/3/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is down (dead timer expired).
对系统的影响	可能会导致基于PCEP会话建立的LSP状态发生变化，影响业务流量转发
日志产生原因	显示会话的状态变化以及会话down的原因，包括： • TCP connection down：TCP 连接断开 • received a close message：收到关闭消息 • reception of a malformed PCEP message：收到非法消息 • internal error：内部错误 • memory in critical state：内存不足 • dead timer expired：会话超时 • process deactivated：PCE 进程去激活 • remote peer unavailable/untriggered：对等体失效 • reception of an unacceptable number of unrecognized PCEP messages：收到超过限制的未知消息 • reception of an unacceptable number of unknown requests/replies：收到超过限制的未知计算请求/计算应答 • PCE address changed：PCE 地址变化 • initialization failed：初始化失败
处理建议	• 如果会话的状态变更为 up，不需要进行其它操作 • 如果会话的状态变更为 down，请根据提示原因检查网络环境或者配置

118 PEX（IRF3.1）

本节介绍 IRF3.1 PEX（Port Extender）模块输出的日志信息。

118.1 PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER

日志内容	[STRING] was assigned to [STRING].
日志含义	系统自动将连接PEX的物理接口添加到作为级联接口的聚合组中
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER: GigabitEthernet 1/2/0/1 was assigned to Bridge-Aggregation10.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，自动将连接PEX的物理接口添加到作为级联接口的聚合组中
处理建议	无需处理

118.2 PEX_AUTOCONFIG_BAGG_CREATE

日志内容	[STRING] was created by the PEX auto-config feature.
日志含义	IRF3.1系统自动配置功能自动创建聚合接口用来作级联接口
参数解释	$1：聚合接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_BAGG_CREATE: Bridge-Aggregation10 was created by the PEX auto-config feature.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，自动创建聚合接口用来作级联接口
处理建议	无需处理

118.3 PEX_AUTOCONFIG_BAGG_NORESOURCE

日志内容	Not enough resources to create a Layer 2 aggregate interface.
日志含义	IRF3.1系统自动配置功能没有空闲资源创建二层聚合接口
参数解释	无
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_BAGG_NORESOURCE: Not enough resources to create a Layer 2 aggregate interface.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，没有空闲资源创建二层聚合接口
处理建议	执行**display interface brief**命令查看设备上当前存在的聚合接口，可删除无需使用的聚合接口，释放资源

118.4 PEX_AUTOCONFIG_BAGG_REMOVEMEMBER

日志内容	[STRING] was removed from [STRING].
日志含义	IRF3.1系统自动配置功能将连接PEX的物理接口从其他级联接口的聚合组中删除
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_BAGG_REMOVEMEMBER: GigabitEthernet 1/2/0/1 was removed from Bridge-Aggregation10.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，会自动将连接PEX的物理接口添加到作为级联接口的聚合组中。添加端口时，如果检查到该物理接口已经被添加到其他级联接口的聚合组中，则先将该物理接口从其他级联接口的聚合组中删除
处理建议	无需处理

118.5 PEX_AUTOCONFIG_CAPABILITY_ENABLE

日志内容	PEX connection capability was enabled on [STRING] and the interface was assigned to PEX group [UINT32].
日志含义	IRF3.1系统自动配置功能自动开启连接PEX的聚合接口的PEX连接能力，并将该接口加入PEX组中
参数解释	$1：聚合接口名称 $2：PEX组编号
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_CAPABILITY_ENABLE: PEX connection capability was enabled on Bridge-Aggregation 10 and the interface was assigned to PEX group 1.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，自动开启连接PEX的聚合接口的PEX连接能力，并将该接口加入PEX组中
处理建议	无需处理

118.6 PEX_AUTOCONFIG_CASCADELIMIT

日志内容	Failed to assign cascade port [STRING] to PEX group [UINT32]. Reason: Maximum number of cascade ports already reached in the PEX group.
日志含义	IRF3.1系统自动配置功能无法将聚合接口加入PEX组中
参数解释	$1：聚合接口名称 $2：PEX组编号
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_CASCADELIMIT: Failed to assign cascade port Bridge-Aggregation10 to PEX group1. Reason: Maximum number of cascade ports already reached in the PEX group.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，检测到PEX组中级联接口的数目已达到上限，无法再将聚合接口加入该PEX组中
处理建议	执行**display pex interface brief**命令显示PEX级联接口列表，再在聚合接口视图下执行**undo pex-capability enable**命令将空闲的级联接口从PEX组中删除，释放资源

118.7 PEX_AUTOCONFIG_CONNECTION_ERROR

日志内容	A PEX connected to more than one upper-tier PEXs.
日志含义	IRF3.1系统自动配置功能检测到PEX和两台或两台以上上级PEX之间存在物理连接
参数解释	无
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_CONNECTION_ERROR: A PEX connected to more than one upper-tier PEXs.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，检测到PEX和两台或两台以上上级PEX之间存在物理连接
处理建议	PEX上行链路只能连接到同一台上级PEX，否则可能导致PEX无法上线或上线后功能运行异常。请检查并修改组网连接

118.8 PEX_AUTOCONFIG_DIFFGROUPNUMBER

日志内容	[STRING] failed to join in PEX group [UINT32]. Reason: Its upper-tier PEX was in PEX group [UINT32]. Please make sure they are in the same PEX group.
日志含义	PEX和它的上级PEX属于不同的PEX组
参数解释	$1：聚合接口名称 $2：PEX组编号 $3：PEX组编号
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_DIFFGROUPNUMBER: Bridge-Aggregation10 failed to join in PEX group 1. Reason: Its upper-tier PEX was in PEX group 2. Please make sure they are in the same PEX group.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能，开启PEX二层聚合接口或PEX三层聚合接口连接PEX的能力并将接口加入PEX组时，所指定的PEX组编号与上级PEX所在PEX组编号不同
处理建议	下级PEX只能与上级PEX加入同一PEX组，请在聚合接口视图下执行**pex-capability enable**命令修改接口加入的PEX组

118.9 PEX_AUTOCONFIG_DYNAMICBAGG_STP

日志内容	[STRING] was automatically set to dynamic aggregation mode and configured as an STP edge port.
日志含义	IRF3.1系统自动配置功能将级联接口自动配置为动态聚合模式并且配置为STP边缘端口
参数解释	$1：二层聚合接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_DYNAMICBAGG_STP: Bridge-Aggregation10 was automatically set to dynamic aggregation mode and configured as an STP edge port.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，将级联接口自动配置为动态聚合模式并且配置为STP边缘端口
处理建议	无需处理

118.10 PEX_AUTOCONFIG_GROUP_CREATE

日志内容	PEX group [UINT32] was created.
日志含义	IRF3.1系统自动配置功能自动创建PEX组
参数解释	$1：PEX组编号
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_GROUP_CREATE: PEX group 1 was created.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，自动创建PEX组
处理建议	无需处理

118.11 PEX_AUTOCONFIG_NONUMBERRESOURCE

日志内容	形式一： No virtual slot numbers are available. 形式二： No virtual chassis numbers are available.
日志含义	没有虚拟槽位号/虚拟框号资源用来分配
参数解释	无
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_NONUMBERRESOURCE: No virtual slot numbers are available.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，没有虚拟槽位号/虚拟框号资源用来分配
处理建议	执行**undo interface**命令删除空闲级联接口或在空闲级联接口视图下执行**undo pex associate**命令取消分配虚拟槽位号/虚拟框号的配置，释放资源

118.12 PEX_AUTOCONFIG_NOT_CASCADEPORT

日志内容	[STRING] was already assigned to [STRING], which is an aggregate interface not enabled with PEX connection capability. Please remove [STRING] from [STRING] or use another physical interface to connect the PEX.
日志含义	IRF3.1系统自动配置功能检测到连接PEX的物理接口已经加入到聚合组中，但对应聚合接口没有开启连接PEX的能力
参数解释	$1：物理接口名称 $2：聚合接口名称 $3：物理接口名称 $4：聚合接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_NOT_CASCADEPORT: GigabitEthernet 1/2/0/1 was already assigned to Bridge-Aggregation10, which is an aggregate interface not enabled with PEX connection capability. Please remove GigabitEthernet 1/2/0/1 from Bridge-Aggregation10 or use another physical interface to connect the PEX.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，检测到连接PEX的物理接口已经加入到聚合组中，但对应聚合接口没有开启连接PEX的能力
处理建议	在物理接口视图下执行**undo port link-aggregation group**命令将物理接口从聚合组中退出，或使用其他物理接口作为级联接口

118.13 PEX_AUTOCONFIG_NUMBER_ASSIGN

日志内容	形式一： Virtual slot number [UINT32] was assigned on [STRING]. 形式二： Virtual chassis number [UINT32] was assigned on [STRING].
日志含义	IRF3.1系统自动配置功能自动为PEX分配虚拟槽位号/虚拟框号
参数解释	形式一： $1：虚拟槽位号 $2：聚合接口名称 形式二： $1：虚拟框号 $2：聚合接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_AUTOCONFIG_NUMBER_ASSIGN: Virtual slot number 100 was assigned on Bridge-Aggregation 10.
对系统的影响	对系统无影响
日志产生原因	父设备运行IRF3.1系统自动配置功能时，在连接PEX的聚合接口上，自动为PEX分配虚拟槽位号/虚拟框号
处理建议	无需处理

118.14 PEX_LLDP_DISCOVER

日志内容	Discover peer device on interface [STRING]: MAC=[STRING], priority=[UINT32].
日志含义	父设备或PEX设备通过LLDP协议发现对端
参数解释	$1：接口名称 $2：对端MAC地址 $3：PEX设备上行口的优先级
日志等级	5 (Notification)
举例	PEX/5/PEX_LLDP_DISCOVER: Discover peer device on interface Ten-GigabitEthernet1/0/1: MAC=20f4-9cb6-0100, priority=0.
对系统的影响	对系统无影响
日志产生原因	父设备或PEX设备通过LLDP协议发现对端
处理建议	无需处理

118.15 PEX_MEMBERID_EXCEED

日志内容	To use the IRF fabric connected to interface [STRING] as a PEX, the IRF member ID must be in the range of 1 to 4.
日志含义	PEX为一个IRF系统，有设备的成员编号超出了1～4的范围
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	PEX/4/PEX_MEMBERID_EXCEED: To use the IRF fabric connected to interface Bridge-Aggregation1 as a PEX, the IRF member ID must be in the range of 1 to 4.
对系统的影响	对系统无影响
日志产生原因	设备作为PEX加入IRF3.1系统时，PEX设备的IRF成员编号必须在1～4范围以内
处理建议	登录PEX设备，指定**display irf**命令查看设备的成员编号。对于成员编号不在1～4范围以内的设备，请执行以下处理建议： 1. 使用 **irf member renumber**命令修改设备的成员编号 2. 执行 **reboot**命令重启该设备，使新的成员编号生效 3. 执行 **display irf topology**命令查看到PEX组建的IRF系统拓扑稳定后，再连接PEX和上级设备，让PEX加入IRF3.1 系统

118.16 PEX_PECSP_OPEN_RCVD

日志内容	Received a CSP Open message on interface [STRING].
日志含义	父设备级联口或PEX设备上行口收到PE CSP协议的OPEN报文
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_PECSP_OPEN_RCVD: Received a CSP Open message on interface Bridge-Aggregation1.
对系统的影响	对系统无影响
日志产生原因	父设备级联口或PEX设备上行口收到PE CSP协议的OPEN报文，表示对端请求建立连接。如果双方均能在发送请求后60秒内接收到对端回复的OPEN报文，则父设备和PEX之间的连接建立成功
处理建议	无需处理

118.17 PEX_PECSP_OPEN_SEND

日志内容	Sent a CSP Open message on interface [STRING].
日志含义	父设备级联口或PEX设备上行口发送PE CSP协议的OPEN报文
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	PEX/5/PEX_PECSP_OPEN_SEND: Sent a CSP Open message on interface Bridge-Aggregation1.
对系统的影响	对系统无影响
日志产生原因	父设备级联口或PEX设备上行口发送PE CSP协议的OPEN报文，表示请求与对方建立连接。如果双方均能在发送请求后60秒内接收到对端回复的OPEN报文，则父设备和PEX之间的连接建立成功
处理建议	无需处理

118.18 PEX_PECSP_TIMEOUT

日志内容	PE CSP timed out on interface [STRING].
日志含义	PE CSP协议的OPEN报文超时
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	PEX/4/PEX_PECSP_TIMEOUT: PE CSP timed out on interface Bridge-Aggregation1.
对系统的影响	对系统无影响
日志产生原因	父设备级联口和PEX设备上行口互相发送PE CSP协议的OPEN报文，表示请求与对方建立连接。双方均未能在发送请求后60秒内接收到对端回复的OPEN报文，则认为OPEN报文超时，PEX设备和父设备连接建立失败
处理建议	在父设备上执行**display pex interface**命令查看级联接口的名称以及状态，如果级联接口状态为DOWN，请先定位聚合链路DOWN的问题

119 PEX（IRF3）

本节介绍 PEX（Port Extender）模块输出的日志信息。

119.1 PEX_ASSOCIATEID_MISMATCHING

日志内容	The associated ID of PEX port [UNIT32] is [UNIT32] on the parent fabric, but the PEX connected to the port has obtained ID [UNIT32].
日志含义	用户配置的虚拟槽位号/虚拟框号与实际连接的PEX设备虚拟槽位号/虚拟框号不一致
参数解释	$1：PEX端口编号 $2：父设备侧配置的虚拟槽位号或虚拟框号 $3：实际连接的邻居PEX设备虚拟槽位号或虚拟框号
日志等级	5 (Notification)
举例	PEX/5/PEX_ASSOCIATEID_MISMATCHING: The associated ID of PEX port 1 is 100 on the parent fabric, but the PEX connected to the port has obtained ID 101.
对系统的影响	影响PEX和父设备之间的报文交互
日志产生原因	用户配置的虚拟槽位号/虚拟框号与实际连接的PEX设备虚拟槽位号/虚拟框号不一致
处理建议	• 请执行 **display pex-port**命令，查看PEX端口的信息 • 请检查 PEX 的组网连接，如果是 PEX 连线错误，请将 PEX 从正确的接口接入 • 如果不方便修改PEX连线，可以通过 **associate**命令将分配给PEX的虚拟槽位号/虚拟框号修改到正确的虚拟槽位号/虚拟框号范围

119.2 PEX_CONFIG_ERROR

日志内容	PEX port [UINT32] discarded a REGISTER request received from [STRING] through interface [STRING]. Reason: The PEX was not assigned an ID, or the PEX was assigned an ID equal to or greater than the maximum value ([UINT32]).
日志含义	PEX注册失败
参数解释	$1：PEX端口ID $2：PEX产品型号 $3：PEX物理端口名称 $4：指定PEX类型的设备允许配置的最大虚拟槽位号或虚拟框号
日志等级	4 (Warning)
举例	PEX/4/PEX_CONFIG_ERROR: PEX port 1 discarded a REGISTER request received from PEX-S5120HI-S5500HI through interface Ten-GigabitEthernet10/0/31. Reason: The PEX was not assigned an ID, or the PEX was assigned an ID equal to or greater than the maximum value 130.
对系统的影响	PEX无法加入IRF
日志产生原因	PEX设备启动前必须通过**associate**命令配置虚拟槽位号/虚拟框号 PEX不同型号的产品允许分配的虚拟槽位号/虚拟框号有最大值限制 XX型号的连接到XX端口的PEX没有配置虚拟槽位号/虚拟框号或者配置的虚拟槽位号/虚拟框号超过了产品允许的最大范围
处理建议	通过**associate**命令将分配给PEX的虚拟槽位号/虚拟框号修改到正确的虚拟槽位号/虚拟框号范围内

119.3 PEX_CONNECTION_ERROR

日志内容	PEX port [UINT32] discarded a REGISTER request received from [STRING] through interface [STRING]. Reason: Another PEX has been registered on the PEX port.
日志含义	PEX连接错误导致PEX注册失败
参数解释	$1：PEX端口ID $2：PEX产品型号 $3：PEX物理端口名称
日志等级	4 (Warning)
举例	PEX/4/PEX_CONNECTION_ERROR: PEX port 1 discarded a REGISTER request received from PEX-S5120HI-S5500HI through interface Ten-GigabitEthernet10/0/31. Reason: Another PEX has been registered on the PEX port.
对系统的影响	PEX无法加入IRF
日志产生原因	每个PEX端口只允许加入一个PEX设备，如果有一个PEX已经启动，其他的PEX连接到该端口上属于配置错误，丢弃请求
处理建议	检查连线是否错误，请确认同一个PEX端口下只连接了一个PEX设备

119.4 PEX_FORBID_STACK

日志内容	Can't connect PEXs [UNIT32] and [UNIT32]: The PEX ports to which the PEXs belong are in different PEX port groups.
日志含义	属于不同PEX端口组的PEX设备连接在一起
参数解释	$1：PEX设备的虚拟槽位号或虚拟框号 $2：PEX设备的虚拟槽位号或虚拟框号
日志等级	5 (Notification)
举例	PEX/5/PEX_FORBID_STACK: Can't connect PEXs 100 and 102: The PEX ports to which the PEXs belong are in different PEX port groups.
对系统的影响	PEX无法加入IRF
日志产生原因	属于不同PEX端口组的PEX设备连接在一起
处理建议	请检查组网连接，不同EX端口组的PEX设备不能连接在一起

119.5 PEX_LINK_BLOCK

日志内容	Status of [STRING] changed from [STRING] to blocked.
日志含义	PEX端口状态变成了blocked
参数解释	$1：端口名称 $2：端口的链路状态
日志等级	4 (Warning)
举例	PEX/4/PEX_LINK_BLOCK: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to blocked.
对系统的影响	PEX端口无法转发数据报文
日志产生原因	处于blocked状态的链路可以转发协议包，但是不能转发数据包。Blocked是一种介于down与forwarding之间的过渡状态 下面的事件可以触发PEX链路状态进入blocked状态： • 物理连接错误，即同一 PEX 设备上的 PEX 物理接口连接到了父设备上不同 PEX 端口下绑定的 PEX 物理接口或者父设备上同一 PEX 端口下绑定的 PEX 物理接口连接到了不同的 PEX 设备 • 被设备强制限制成 Blocked 状态。在 PEX 设备启动阶段，PEX 设备会将未被用于加载启动软件包的、物理状态为 UP 的 PEX 物理端口状态设置为 Blocked • 接口的物理状态为 UP，但是父设备和 PEX 设备的 PEX 连接中断
处理建议	• 从 down 到 blocked，说明接口 up 了，属于正常状态。但是如果长期停在 blocked 状态，请确认连线是否正确或者线路是否正常 • 从 forwarding 到 blocked，并且长期停在 blocked，请检查是否存在 IRF 分裂，导致 PEX 存在两个 IRF 组中

119.6 PEX_LINK_DOWN

日志内容	Status of [STRING] changed from [STRING] to down.
日志含义	PEX端口状态变成了down
参数解释	$1：端口名称 $2：端口的链路状态
日志等级	4 (Warning)
举例	PEX/4/PEX_LINK_DOWN: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to down.
对系统的影响	PEX端口无法转发报文
日志产生原因	处于down状态的链路无法转发任何报文 许多事件，例如：物理链路故障、管理员执行**shutdown**命令、系统重启等等，都可以使链路进入down状态
处理建议	请确认是否有管理员输入**shutdown**命令或者系统重启操作导致，如果是以上操作导致，则属于正常状态。如果不是，请检查物理接口的连线是否进行过插拔操作或松动

119.7 PEX_LINK_FORWARD

日志内容	Status of [STRING] changed from [STRING] to forwarding.
日志含义	PEX端口状态变成了正常转发状态
参数解释	$1：端口名称 $2：端口的链路状态
日志等级	5 (Notification)
举例	PEX/5/PEX_LINK_FORWARD: Status of Ten-GigabitEthernet2/0/1 changed from blocked to forwarding.
对系统的影响	对系统无影响

日志产生原因	• 链路进入 forwarding 状态，可以开始转发数据报文
	• 下面的事件可以触发 PEX 链路进入 forwarding 状态：
	  ○ 链路进入 blocked 状态后，重新检测成功
	  ○ PEX 完成软件加载，使 PEX 端口状态变成 forwarding

处理建议	无需处理

119.8 PEX_REG_JOININ

日志内容	PEX ([STRING]) registered successfully on PEX port [UINT32].
日志含义	PEX注册成功
参数解释	$1：虚拟槽位号或虚拟框号 $2：PEX端口ID
日志等级	5 (Notification)
举例	PEX/5/PEX_REG_JOININ: PEX (slot 101) registered successfully on PEX port 1.
对系统的影响	对系统无影响
日志产生原因	PEX端口完成注册，可以开始管理及配置PEX设备。在父设备上可以将PEX设备视为一块接口板进行操作
处理建议	无需处理

119.9 PEX_REG_LEAVE

日志内容	PEX ([STRING]) unregistered on PEX port [UINT32].
日志含义	PEX注销
参数解释	$1：虚拟槽位号或虚拟框号 $2：PEX端口ID
日志等级	4 (Warning)
举例	PEX/4/PEX_REG_LEAVE: PEX (slot 101) unregistered on PEX port 1.
对系统的影响	PEX不属于IRF，不能为IRF转发报文
日志产生原因	PEX端口取消注册，此后从父设备上无法操作PEX设备 下面的事件可以导致PEX端口取消注册： • PEX 设备在 30 分钟内启动失败 • PEX 端口内的所有物理接口 down。例如将所有和父设备连接的接口都 shutdown 或者将物理连接全部断开 • PEX 端口内的所有物理端口的链路检测均失败 • PEX 设备重启
处理建议	1. 如果是 PEX 设备重启或者用户将 PEX 和父设备之间的相连的所有端口都手工关闭了导致 PEX 设备取消注册，属于正常事件，无需任何处理 2. 否则，请使用命令行 **display device**查看PEX的设备的虚拟槽位号/虚拟框号是否存在，State是否正常，如果没有显示PEX设备的虚拟槽位号/虚拟框号或PEX设备的State不是Normal，请前往步骤 3 3. 使用命令行 **display pex-port**检查PEX端口是否存在虚拟槽位号/虚拟框号配置，如果不存在请重新配置；如果存在请检查PEX物理端口状态是否全部为down或者全部blocked，如果PEX物理端口状态全部为down或者全部blocked请前往步骤 4 4. 使用命令行 **display interface**检查PEX端口内的所有物理接口对应的Current state字段是否为down。如果Current state字段显示为 down，请检查接口连接线缆是否被拔出或故障

119.10 PEX_REG_REQUEST

日志内容	Received a REGISTER request on PEX port [UINT32] from PEX ([STRING]).
日志含义	父设备收到PEX的注册请求
参数解释	$1：PEX端口ID $2：虚拟槽位号或虚拟框号
日志等级	5 (Notification)
举例	PEX/5/PEX_REG_REQUEST: Received a REGISTER request on PEX port 1 from PEX (slot 101).
对系统的影响	对系统无影响
日志产生原因	PEX相关配置已经成功，PEX设备和父设备连线正确，PEX设备启动时候，PEX端口收到注册请求后准备启动加载版本
处理建议	无需处理

119.11 PEX_STACKCONNECTION_ERROR

日志内容	A device was connected to a PEX that already had two neighboring devices.
日志含义	PEX堆叠连线错误
参数解释	无
日志等级	5 (Notification)
举例	PEX/5/PEX_STACKCONNECTION_ERROR: A device was connected to a PEX that already had two neighboring devices.
对系统的影响	对系统无影响
日志产生原因	系统中存在PEX接口连线错误，某个PEX同时连接了两个CB设备
处理建议	请执行**display pex-port topology**命令用来查看PEX的拓扑信息，并按照组网规划图检查并纠正组网连线。一个PEX只能连接一个CB设备，不能同时连接两个CB设备

120 PFILTER

本节介绍报文过滤模块输出的日志信息。

120.1 PFILTER_GLB_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction globally. [STRING] ACL [UINT] has already been applied globally.
日志含义	全局应用报文过滤时调用的ACL类型冲突
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：ACL类型 $5：ACL编号
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction globally. IPv6 ACL 3000 has already been applied globally.
对系统的影响	全局应用报文过滤时，调用的ACL规则无法正常匹配报文
日志产生原因	如果在某方向上全局应用报文过滤时，调用了IPv4或IPv6或MAC类型的ACL规则，再次在同一方向上应用全局报文过滤或修改全局报文过滤时，调用相同类型的ACL规则
处理建议	请删除全局报文过滤调用的相同类型的ACL

120.2 PFILTER_GLB_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally. The resources are insufficient.
日志含义	因资源不足对于IPv4报文的全局报文过滤的缺省动作不生效
参数解释	$1：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction globally. The resources are insufficient.
对系统的影响	全局应用报文过滤调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在某个方向全局应用报文过滤并调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.3 PFILTER_GLB_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally.
日志含义	因异常故障对于IPv4报文的全局报文过滤的缺省动作不生效
参数解释	$1：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction globally.
对系统的影响	全局应用报文过滤调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在某个方向全局应用报文过滤并调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.4 PFILTER_GLB_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally. The resources are insufficient.
日志含义	因资源不足对于IPv6报文的全局报文过滤的缺省动作不生效
参数解释	$1：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction globally. The resources are insufficient.
对系统的影响	全局应用报文过滤调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在某个方向全局应用报文过滤并调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.5 PFILTER_GLB_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally.
日志含义	因异常故障对于IPv6报文的全局报文过滤的缺省动作不生效
参数解释	$1：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction globally.
对系统的影响	全局应用报文过滤调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在某个方向全局应用报文过滤并调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.6 PFILTER_GLB_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally. The resources are insufficient.
日志含义	因资源不足对于二层报文的全局报文过滤的缺省动作不生效
参数解释	$1：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction globally. The resources are insufficient.
对系统的影响	全局应用报文过滤调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在某个方向全局应用报文过滤并调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.7 PFILTER_GLB_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally.
日志含义	因异常故障对于二层报文的全局报文过滤的缺省动作不生效
参数解释	$1：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction globally.
对系统的影响	全局应用报文过滤调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在某个方向全局应用报文过滤并调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.8 PFILTER_GLB_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The resources are insufficient.
日志含义	因资源不足全局应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：规则的ID及内容 $4：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The resources are insufficient.
对系统的影响	全局应用的报文过滤不生效
日志产生原因	因硬件资源不足，系统无法在某个方向上全局应用报文过滤并调用ACL规则
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.9 PFILTER_GLB_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The ACL is not supported.
日志含义	因系统不支持ACL规则中参数，全局应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：规则的ID及内容 $4：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The ACL is not supported.
对系统的影响	全局应用的报文过滤不生效
日志产生原因	因系统不支持ACL规则中的参数，导致无法在某个方向上全局应用报文过滤并调用ACL规则
处理建议	检检查报文过滤调用的ACL规则并删除该ACL规则中不支持的参数，具体不支持的参数与设备型号有关，请以设备实际情况为准

120.10 PFILTER_GLB_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally.
日志含义	因系统故障全局应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_GLB_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally.
对系统的影响	全局应用的报文过滤不生效
日志产生原因	因系统故障，无法在某个方向上全局应用报文过滤并调用ACL
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.11 PFILTER_IF_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
日志含义	因资源不足，对于IPv4报文接口下报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
对系统的影响	接口下应用报文过滤调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在接口某个方向应用报文过滤并调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.12 PFILTER_IF_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING].
日志含义	因异常故障，对于IPv4报文接口下报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2.
对系统的影响	接口下应用报文过滤调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在接口某个方向应用报文过滤并调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.13 PFILTER_IF_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
日志含义	因资源不足，对于IPv6报文接口下报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
对系统的影响	接口下应用报文过滤调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在接口某个方向应用报文过滤并调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.14 PFILTER_IF_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING].
日志含义	因异常故障，对于IPv6报文接口下报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2.
对系统的影响	接口下应用报文过滤调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在接口某个方向应用报文过滤并调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.15 PFILTER_IF_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
日志含义	因资源不足，对于二层报文接口下报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
对系统的影响	接口下应用报文过滤调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在接口下某个方向应用报文过滤并调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.16 PFILTER_IF_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING].
日志含义	因异常故障，对于二层报文接口下报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2.
对系统的影响	接口下应用报文过滤调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在接口下某个方向应用报文过滤并调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.17 PFILTER_IF_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The resources are insufficient.
日志含义	因资源不足接口下应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
对系统的影响	接口下应用的报文过滤不生效
日志产生原因	因硬件资源不足，系统无法在接口的某个方向上应用报文过滤并调用ACL规则
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.18 PFILTER_IF_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The ACL is not supported.
日志含义	因系统不支持ACL规则中参数，接口下应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The ACL is not supported.
对系统的影响	接口下应用的报文过滤不生效
日志产生原因	因系统不支持ACL规则中的参数，导致无法在接口某个方向上应用报文过滤并调用ACL规则
处理建议	检查报文过滤调用的ACL规则并删除该ACL规则中不支持的参数，具体不支持的参数与设备型号有关，请以设备实际情况为准

120.19 PFILTER_IF_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of interface [STRING]. [STRING] ACL [UINT] has already been applied to the interface.
日志含义	接口下应用报文过滤时调用的ACL类型冲突
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：接口名称 $5：ACL类型 $6：ACL编号
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of interface Ethernet 3/1/2. IPv6 ACL 3000 has already been applied to the interface.
对系统的影响	接口下应用报文过滤时，调用的ACL规则无法正常匹配报文
日志产生原因	如果在接口某个方向上应用报文过滤时，调用了IPv4或IPv6或MAC类型的ACL规则，再次在同接口的同一方向上应用报文过滤或修改全局报文过滤时，调用相同类型的ACL规则
处理建议	请删除报文过滤调用的相同类型的ACL

120.20 PFILTER_IF_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING].
日志含义	因系统故障接口下应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_IF_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2.
对系统的影响	接口下应用报文过滤不生效
日志产生原因	因系统故障，无法在接口某个方向上应用报文过滤并调用ACL
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.21 PFILTER_IPV4_FLOW_INFO

日志内容	ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
日志含义	报文过滤引用的IPv4高级ACL规则首次匹配到报文
参数解释	$1：ACL编号或名称 $2：流量方向 $3：ACL应用的位置 $4：ACL规则的编号及动作 $5：ACL规则匹配的首个报文的信息
日志等级	6 (Informational)
举例	PFILTER/6/PFILTER_IPV4_FLOW_INFO: ACL 3000 inbound Ethernet 3/1/2 rule 0 permit tcp 192.168.1.1(1024) -> 192.168.5.1(1024).
对系统的影响	对系统无影响
日志产生原因	报文过滤引用的IPv4高级ACL规则首次匹配到的报文信息
处理建议	系统正常运行时产生的信息，无需处理

120.22 PFILTER_IPV4_FLOW_STATIS

日志内容	ACL [STRING] [STRING] rule [STRING] [STRING], [UINT64] packets.
日志含义	报文过滤引用的IPv4高级ACL规则匹配到的报文及其统计信息
参数解释	$1：ACL编号或名称 $2：流量方向 $3：ACL规则的编号及动作 $4：ACL规则匹配的报文的信息 $5：匹配的报文个数
日志等级	6 (Informational)
举例	PFILTER/6/PFILTER_IPV4_FLOWLOG_STATIS: ACL 3000 inbound rule 0 permit icmp 192.168.1.1(1024) -> 192.168.5.1(1024), 1000 packets.
对系统的影响	对系统无影响
日志产生原因	报文过滤引用的IPv4高级ACL规则匹配到的报文及其统计信息
处理建议	系统正常运行时产生的信息，无需处理

120.23 PFILTER_IPV6_FLOW_INFO

日志内容	IPv6 ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
日志含义	报文过滤引用的IPv6高级ACL规则首次匹配到报文
参数解释	$1：ACL编号或名称 $2：流量方向 $3：ACL应用的位置 $4：ACL规则的编号及动作 $5：ACL规则匹配的首个报文的信息
日志等级	6 (Informational)
举例	PFILTER/6/PFILTER_IPV6_FLOW_INFO: IPv6 ACL 3000 inbound Ethernet 3/1/2 rule 0 permit tcp 0:1020::200:0(0)->0:720::200:0(0).
对系统的影响	对系统无影响
日志产生原因	报文过滤引用的IPv6高级ACL规则首次匹配到的报文信息
处理建议	系统正常运行时产生的信息，无需处理

120.24 PFILTER_IPV6_FLOW_STATIS

日志内容	IPv6 ACL [STRING] [STRING] rule [STRING] [STRING], [UINT64] packets.
日志含义	报文过滤引用的IPv6高级ACL规则匹配到的报文及其统计信息
参数解释	$1：ACL编号或名称 $2：流量方向 $3：ACL规则的编号及动作 $4：ACL规则匹配的报文的信息 $5：匹配的报文个数
日志等级	6 (Informational)
举例	PFILTER/6/PFILTER_IPV6_FLOWLOG_STATIS: IPv6 ACL 3000 rule 0 permit icmpv6 0:1020::200:0(0)->0:720::200:0(0), 1000 packets.
对系统的影响	对系统无影响
日志产生原因	报文过滤引用的IPv6高级ACL规则匹配到的报文及其统计信息
处理建议	系统正常运行时产生的信息，无需处理

120.25 PFILTER_IPV6_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter IPv6 [UINT32] [STRING] [STRING] [UINT64] packet(s).
日志含义	报文过滤调用IPv6 ACL规则命中的报文统计信息
参数解释	$1：ACL应用目的地 $2：流量方向 $3：ACL编号 $4：ACL规则的ID及内容 $5：匹配上规则的报文个数
日志等级	6 (Informational)
举例	ACL/6/PFILTER_IPV6_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter IPv6 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
对系统的影响	对系统无影响
日志产生原因	匹配上报文过滤中的IPv6 ACL规则的报文数量发生变化
处理建议	系统正常运行时产生的信息，无需处理

120.26 PFILTER_MAC_FLOW_INFO

日志内容	MAC ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
日志含义	报文过滤引用的二层ACL规则首次匹配到报文
参数解释	$1：ACL编号或名称 $2：流量方向 $3：ACL应用的位置 $4：ACL规则的编号及动作 $5：ACL规则匹配的首个报文的信息
日志等级	6 (Informational)
举例	PFILTER/6/PFILTER_MAC_FLOW_INFO: MAC ACL 4000 inbound Ethernet 3/1/2 rule 0 permit 0800-2700-9000 -> 0CDA-411D-0676.
对系统的影响	对系统无影响
日志产生原因	报文过滤引用二层ACL规则首次匹配到的报文信息
处理建议	系统正常运行时产生的信息，无需处理

120.27 PFILTER_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter [UINT32] [STRING] [UINT64] packet(s).
日志含义	报文过滤调用IPv4 ACL规则命中的报文统计信息
参数解释	$1：ACL应用目的地 $2：流量方向 $3：ACL编号 $4：ACL规则的ID及内容 $5：匹配上规则的报文个数
日志等级	6 (Informational)
举例	ACL/6/PFILTER_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
对系统的影响	对系统无影响
日志产生原因	匹配上报文过滤中的IPv4 ACL规则的报文数量发生变化
处理建议	系统正常运行时产生的信息，无需处理

120.28 PFILTER_VLAN_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
日志含义	因资源不足，对于IPv4报文VLAN中应用报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1. The resources are insufficient.
对系统的影响	VLAN中应用报文过滤调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在VLAN某个方向应用报文过滤并调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.29 PFILTER_VLAN_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16].
日志含义	因异常故障，对于IPv4报文VLAN中应用报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1.
对系统的影响	VLAN中应用报文过滤调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在VLAN某个方向应用报文过滤并调用IPv4 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.30 PFILTER_VLAN_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
日志含义	因资源不足，对于IPv6报文VLAN中应用报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1. The resources are insufficient.
对系统的影响	VLAN中应用报文过滤调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在VLAN某个方向应用报文过滤并调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.31 PFILTER_VLAN_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16].
日志含义	因异常故障，对于IPv6报文VLAN中应用报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1.
对系统的影响	VLAN中应用报文过滤调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在VLAN某个方向应用报文过滤并调用IPv6 ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.32 PFILTER_VLAN_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
日志含义	因资源不足，对于二层报文VLAN中应用报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1. The resources are insufficient.
对系统的影响	VLAN中应用报文过滤调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因硬件资源不足，在VLAN某个方向应用报文过滤并调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.33 PFILTER_VLAN_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16].
日志含义	因异常故障，对于二层报文VLAN中应用报文过滤的缺省动作不生效
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1.
对系统的影响	VLAN中应用报文过滤调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
日志产生原因	因异常故障，在VLAN某个方向应用报文过滤并调用二层ACL规则时，应用或修改报文过滤的缺省动作不生效
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.34 PFILTER_VLAN_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
日志含义	因资源不足VLAN中应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of VLAN 1. The resources are insufficient.
对系统的影响	VLAN中应用的报文过滤不生效
日志产生原因	因硬件资源不足，系统无法在VLAN的某个方向上应用报文过滤并调用ACL规则
处理建议	请使用**display qos-acl resource**命令检查硬件资源使用情况，收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

120.35 PFILTER_VLAN_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The ACL is not supported.
日志含义	因系统不支持ACL规则中参数，VLAN中应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_NOT_SUPPORT: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1. The ACL is not supported.
对系统的影响	VLAN中应用的报文过滤不生效
日志产生原因	因系统不支持ACL规则中的参数，导致无法在VLAN中某个方向上应用报文过滤并调用ACL规则
处理建议	检查报文过滤调用的ACL规则并删除该ACL规则中不支持的参数，具体不支持的参数与设备型号有关，请以设备实际情况为准

120.36 PFILTER_VLAN_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of VLAN [UINT16]. [STRING] ACL [UINT] has already been applied to the VLAN.
日志含义	VLAN中应用报文过滤时调用的ACL类型冲突
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：VLAN ID $5：ACL类型 $6：ACL编号
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of VLAN 1. IPv6 ACL 3000 has already been applied to the VLAN.
对系统的影响	VLAN中应用报文过滤时，调用的ACL规则无法正常匹配报文
日志产生原因	如果在VLAN某个方向上应用报文过滤时，调用了IPv4或IPv6或MAC类型的ACL规则，再次在同VLAN的同一方向上应用报文过滤或修改全局报文过滤时，调用相同类型的ACL规则
处理建议	请删除报文过滤调用的相同类型的ACL

120.37 PFILTER_VLAN_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16].
日志含义	因系统故障VLAN中应用报文过滤失败
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3 (Error)
举例	PFILTER/3/PFILTER_VLAN_UNK_ERR: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1.
对系统的影响	VLAN中应用报文过滤不生效
日志产生原因	因系统故障，无法在VLAN中某个方向上应用报文过滤并调用ACL
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

121 PIM

本节介绍 PIM 模块输出的日志信息。

121.1 PIM_CBSR_TO_EBSR

日志内容	PIM C-BSR wins BSR Election. (C-BSRAddr=[STRING], VPNName=[STRING])
日志含义	CBSR选举为BSR
参数解释	$1：C-BSR地址 $2：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6 (Notification)
举例	PIM/6/PIM_CBSR_TO_EBSR: PIM C-BSR wins BSR Election. (C-BSRAddr=192.168.40.2, VPNName=vpn-test)
对系统的影响	系统相关表项的BSR更新为最新BSR地址
日志产生原因	C-BSR赢得BSR选举
处理建议	1. 请确认当前 BSR 变化是否为管理员所期望。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 2。 2. 请确认旧的 E-BSR 地址所在设备是否存在故障，或者存在当前设备和旧的 E-BSR 之间的链路恢复，或者删除 BSR 配置，或者修改 BSR 配置。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 3。 3. 请在旧的当选BSR的设备上，执行 **display pim interface**命令查看当前是否有对应生效的PIM接口。 o 如果没有，请配置正确的对应 PIM 接口。 o 如果有，则请执行步骤 4。 4. 请用 **display memory**命令查看当前设备是否内存不足。 o 如果内存不足，请先解决内存问题。 o 如果内存充足，则请执行步骤 5。 5. 请在当前设备上执行 **ping**命令，检查和旧的当选BSR的设备之间的链路是否连通。 o 如果连通，则请执行步骤 6。 o 如果不连通，则请先解决链路连通问题。 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

121.2 PIM_DR_ELECTION

日志内容	The interface is elected as a DR. (IfIndex:[UINT32], IfName:[STRING], IfAddr:[STRING], VPNName:[STRING])
日志含义	接口所在的设备被选举为DR
参数解释	$1：接口索引 $2：接口名称 $3：接口地址 $4：VPN实例名称
日志等级	5 (Notification)
举例	PIM/5/PIM_DR_ELECTION: The interface is elected as a DR. (IfIndex:12, IfName:iftest, IfAddr:10.1.1.1, VPNName:vpntest)
对系统的影响	系统相关表项的DR更新为最新DR接口地址
日志产生原因	接口所在的设备被选举为DR
处理建议	确认该设备被选举为DR是否为管理员所期望的： • 如果不是，可通过为该设备的接口配置较低的 DR 优先级或者较小 IP 地址，使得该设备不当选 DR • 如果是，无需处理

121.3 PIM_ERR_INVALID_JP

日志内容	PIM receives an Invalid Join/Prune message. (GroupMappingOrigin=[STRING], GroupMappingAddrType=[STRING], GrpAddr=[STRING], GrpPfxLen=[UINT32], GroupMappingRPAddrType=[STRING], RPAddr=[STRING], GroupMappingPimMode=[STRING], InvJPAddrType=[STRING], InvJPOriginAddr=[STRING], InvJPGrpAddr=[STRING], InvJPRpAddr=[STRING], NbrIfIndex=[UINT32], NbrAddrType=[STRING], NbrAddr=[NbrAddr], NbrUpTime=[STRING], VPNName=[STRING], RecvIfName=[STRING])
日志含义	PIM收到无效的加入/剪枝报文
参数解释	$1：RP映射组类型 $2：组地址类型 $3：JP报文中的组地址 $4：组掩码长度 $5：RP地址的类型 $6：RP地址 $7：当前运行的PIM模式 $8：无效的JP报文的地址类型 $9：无效的JP报文中的源地址 $10：无效的JP报文的组地址 $11：无效的JP报文中的RP地址 $12：邻居接口索引 $13：邻居地址的类型 $14：邻居的地址 $15：邻居存活的时间 $16：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称 $17：接收该报文的接口名
日志等级	4(Notification)
举例	PIM/4/PIM_ERR_INVALID_JP: PIM receives an Invalid Join/Prune message. (GroupMappingOrigin=bsr-rp, GroupMappingAddrType=IPv4, GrpAddr=231.1.1.1, GrpPfxLen=32, GroupMappingRPAddrType=IPv4, RPAddr=192.168.56.3, GroupMappingPimMode=PIM-SM, InvJPAddrType=IPv4, InvJPOriginAddr=192.168.56.12, InvJPGrpAddr=231.1.1.1, InvJPRpAddr=192.168.56.12, NbrIfIndex=258, NbrAddrType=IPv4, NbrAddr=192.168.56.3, NbrUpTime=18:12:15, VPNName= vpn-test, RecvIfName=GigabitEthernet2/0/1)
对系统的影响	对系统无影响
日志产生原因	PIM收到无效的加入/剪枝报文。
处理建议	检查本路由器和J/P报文发送端路由器，二者SSM范围是否相同： • 如果 SSM 范围相同，则请修改 J/P 报文发送端路由器和本路由器对于该组的 RP 配置，使得二者一致 • 如果SSM范围不同，则请执行 **ssm-policy**命令配置相同的SSM范围

121.4 PIM_ERR_INVALID_REG

日志内容	PIM receives an Invalid register message. (GroupMappingOrigin=[STRING], GroupMappingAddrType=[STRING], GrpAddr=[STRING], GrpPfxLen=[UINT32], GroupMappingRPAddrType=[STRING], RPAddr=[STRING], GroupMappingPimMode=[STRING], InvRegAddrType=[STRING], InvRegOriginAddr=[STRING], InvRegGrpAddr=[STRING], InvRegRpAddr=[STRING], VPNName=[STRING])
日志含义	PIM收到无效的注册报文
参数解释	$1：RP映射组类型 $2：组地址类型 $3：JP报文中的组地址 $4：组掩码长度 $5：RP地址的类型 $6：RP地址 $7：当前运行的PIM模式 $8：无效的JP报文的地址类型 $9：无效的JP报文中的源地址 $10：无效的JP报文的组地址 $11：无效的JP报文中的RP地址 $12：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称。
日志等级	4 (Notification)
举例	PIM/4/PIM_ERR_INVALID_REG: PIM receives an Invalid register message. (GroupMappingOrigin=bsr-rp, GroupMappingAddrType=IPv4, GrpAddr=225.0.0.1, GrpPfxLen=32, GroupMappingRPAddrType=IPv4, RPAddr=91.91.91.91, GroupMappingPimMode=PIM-SM, InvRegAddrType=IPv4, InvRegOriginAddr=192.168.40.1, InvRegGrpAddr=225.0.0.1, InvRegRpAddr=192.168.40.2, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	PIM收到无效的注册报文。
处理建议	检查本路由器和J/P报文发送端路由器，二者SSM范围是否相同： • 如果 SSM 范围相同，则请修改 J/P 报文发送端路由器和本路由器对于该组的 RP 配置，使得二者一致 • 如果 SSM 范围不同，则请执行 ssm-policy 命令配置相同的 SSM 范围

121.5 PIM_EBSR_TO_CBSR

日志内容	PIM E-BSR lost BSR Election. (C-BSRAddr=[STRING], Priority=[UINT32], VPNName=[STRING])
日志含义	已当选BSR的当前设备BSR选举失败
参数解释	$1：C-BSR地址 $2：BSR优先级 $3：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6 (Notification)
举例	PIM/6/CBSR_TO_EBSR: PIM C-BSR wins BSR Election. (C-BSRAddr=192.168.40.2, Priority=10, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	已当选BSR的当前设备BSR选举失败
处理建议	1. 请确认当前 BSR 变化是否为管理员所期望。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 2。 2. 请确认新的 BSR 地址所在设备是否存在故障恢复，或者存在当前设备和新的 E-BSR 之间的链路恢复，或者新增 BSR 配置，或者修改 BSR 配置。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 3。 3. 请在 PIM 视图下执行 display this 命令查看当前设备是否配置正确的 BSR 地址。 o 如果未配置，则请配置对应的 BSR 地址。 o 如果已配置，则请执行步骤 4。 4. 请执行 **display pim bsr-info**命令查看当前设备是否为C-BSR。 o 如果不是，则请执行步骤 4。 o 如果是，则请执行步骤 6。 5. 请执行 **display pim interface**命令查看当前C-BSR地址是否有对应生效的PIM 接口。 o 如果没有，请配置正确的对应 PIM 接口。 o 如果有，则请执行步骤 6。 6. 请执行 **display memory**命令查看当前设备是否内存不足。 o 如果内存不足，请先解决内存问题。 o 如果内存充足，则请执行步骤 7。 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

121.6 PIM_NBR_DOWN

日志内容	[STRING]: Neighbor [STRING] ([STRING]) is down.
日志含义	接口PIM邻居Down
参数解释	$1：公网侧PIM邻居down时，该参数为空；私网侧PIM邻居down时，该参数为VPN实例的名称 $2：PIM邻居的IP地址 $3：接口名称
日志等级	5 (Notification)
举例	PIM/5/PIM_NBR_DOWN: Neighbor 10.1.1.1(Vlan-interface10) is down.
对系统的影响	PIM邻居连接中断或建立连接失败，路由不可达，数据转发业务中断
日志产生原因	• PIM 邻居的 HoldTime 定时器超时 • PIM 邻居所在接口 Down • PIM 邻居被删除 • 设备收到 HoldTime 为零的邻居消息 • 邻居的 BFD 会话 down
处理建议	1. 请在本设备对应的接口视图下执行 **display this**命令查看接口是否配置了 **pim neighbor-policy**或 **ipv6 pim neighbor-policy**： o 如果已配置，则请执行步骤 2 o 如果未配置，则请执行步骤 3 2. 请在本设备执行 **display acl**或 **display acl ipv6**命令查看ACL规则，该邻居是否在ACL规则允许的范围内： o 如果在范围内，则请执行步骤 3 o 如果不在范围内，则重新配置 ACL 规则，使得该邻居在 ACL 规则允许的范围内 3. 请在本设备和邻居设备上检查接口物理状态，用 **display interface**命令查看对应的接口状态是否是UP状态： o 如果接口物理状态是Administratively DOWN，可执行 **undo shutdown**命令 o 如果接口物理状态是 Down，请查看物理链接是否正常（包括网线、光模块等硬件是否松动或脱落），重新正确连接物理线路 o 如果接口物理状态是 Up，则请执行步骤 4 4. 请在本设备和邻居设备上检查接口协议状态，用 **display ip interface**或 **display ipv6 interface**命令查看对应的接口状态是否是UP状态。该接口是否配有IP地址： o 如果协议层状态是 Up，则请执行步骤 5 o 如果协议层状态是Down，可执行 **ip address**或 **ipv6 address**命令为接口配置IP地址 5. 请在本设备和邻居设备上对应的接口视图下用 **display this** 命令查看接口是否使能 **pim sm**或 **ipv6 pim sm**： o 如果已使能，则请执行步骤 6 o 如果没有使能，则请在接口上配置 **pim sm**或 **ipv6 pim sm** 6. 请在本设备和邻居设备的任意视图下执行命令 **display current-configuration**，查看对应VPN实例是否使能了 **multicast routing**或者 **ipv6 multicast routing**：

	○ 如果已使能，则请执行步骤 7 ○ 如果未使能，可在系统视图下执行 **multicast routing**或者 **ipv6 multicast routing**命令使能三层组播功能 **7.** 请在本设备和邻居设备上执行 **display memory**命令查看系统内存占用率： ○ 如果内存不足，请先解决内存问题 ○ 如果内存充足，则请执行步骤 8 **8.** 请在本设备执行 **ping**或 **ping ipv6**命令检查和邻居之间的链路是否连通： ○ 如果连通，则请执行步骤 10 ○ 如果不连通，则请执行步骤 9 **9.** 请在本设备和邻居设备上执行 **display ip routing-table**或 **display ipv6 routing-table**命令检查到对方的单播路由是否正常： ○ 如果路由正常，则请执行步骤 10 ○ 如果路由不正常，则排除单播路由故障来解决告警问题 **10.** 请收集配置文件、日志信息和告警信息，并联系技术支持

121.7 PIM_NBR_UP

日志内容	[STRING]: Neighbor [STRING] ([STRING]) is up.
日志含义	接口PIM邻居UP
参数解释	$1：公网侧PIM邻居up时，该参数为空；私网侧PIM邻居up时，该参数为VPN实例的名称 $2：PIM邻居的IP地址 $3：接口名称
日志等级	5 (Notification)
举例	PIM/5/PIM_NBR_UP: Neighbor 10.1.1.1(Vlan-interface10) is up.
对系统的影响	对系统无影响
日志产生原因	PIM接口收到Hello报文，添加了新的PIM邻居
处理建议	无需处理

121.8 PIM_NBR_LOSS

日志内容	STRING] Neighbor [STRING] ([STRING]) is loss, and the router has no other neighbors on the same interface with the same IP version and a lower IP address than itself.(UpTime=[STRING], NeighborDownReason=[STRING])
日志含义	接口PIM邻居关系丢失
参数解释	$1：公网侧PIM邻居down时，该参数为空；私网侧PIM邻居down时，该参数为VPN实例的名称 $2：PIM邻居的IP地址 $3：接口名称 $4：接口UP时长 $5：PIM邻居down的原因： • Neighbor timer expired.：邻居的 HoldTime 定时器超时 • Neighbor is deleted.：邻居删除 • Receive hello cancel message.：收到 HoldTime 为零的邻居消息 • BFD session is down.：邻居的 BFD 会话 down
日志等级	6 (Notification)
举例	PIM/6/PIM_NBR_LOSS: Neighbor 10.1.1.1(Vlan-interface10) is loss, and the router has no other neighbors on the same interface with the same IP version and a lower IP address than itself.(UpTime=00:01:20, NeighborDownReason=Interface is down.)
对系统的影响	PIM邻居关系丢失或建立连接失败，路由不可达，数据转发业务中断
日志产生原因	PIM邻居的状态变为down，且同一接口上没有其他IP版本相同且IP地址较小的PIM邻居
处理建议	检查PIM配置是否错误以及检查网络是否发生故障

121.9 PIM_RP_CHANGED

日志内容	The RP changes. (RPType:[STRING], GrpAddr:[STRING], GrpPfxLen:[UINT32], RPAddr:[STRING], PimMode:[STRING], Priority:[UINT32], VPNName:[STRING])
日志含义	RP发生改变
参数解释	$1：RP的类型： • static-rp：静态 RP • auto-rp：自动 RP • bsr-rp：BSR RP • embedded：嵌入式 RP 2：组播组地址 3：组播组地址掩码长度 4：当选的RP地址 5：当前运行的PIM模式： • PIM-SM：PIM-SM 模式 • Bidir-PIM：双向 PIM 模式 6：RP的优先级 7：VPN实例名称
日志等级	5 (Notification)
举例	PIM/5/PIM_RP_CHANGED: The RP changes. (RPType:static-rp, GrpAddr:224.0.0.0, GrpPfxLen:4, RPAddr:10.1.1.1, PimMode:PIM-SM, Priority:64, VPNName:vpntest)
对系统的影响	系统相关表项的RP更新为最新RP接口地址
日志产生原因	RP发生改变
处理建议	确认RP变化是否为管理员所期望的： • 如果不是，则可以将本设备配置为静态 RP，或者提高 RP 的优先级，使得本设备重新被选举为 RP • 如果是，在无需处理

121.10 PIM_SELECTUPSTREAM_FAIL

日志内容	[STRING]: During multicast load balancing based on bandwidth usage, the system failed to select an upstream interface for the ([STRING], [STRING]) entry due to insufficient available bandwidth for multicast streams on all links.
日志含义	等价链路组播流量可使用带宽不足，（S，G）表项选择上游接口失败
参数解释	$1：公网侧，该参数为空；私网侧，该参数为VPN实例的名称 $2：组播源地址 $3：组播组地址
日志等级	5 (Notification)
举例	PIM/5/SELECTUPSTREAM_FAIL: During multicast load balancing based on bandwidth usage, the system failed to select an upstream interface for the (1.2.3.4, 225.0.0.1) entry due to insufficient available bandwidth for multicast streams on all links.
对系统的影响	（S，G）表项选择上游接口失败，组播流量转发异常
日志产生原因	组播流量负载分担为**flow-ucmp**方式时，所有等价链路组播流量可使用带宽不足
处理建议	请重新调整网络中组播流量带宽规划

122 PIM6

本节介绍 IPv6 PIM 模块输出的日志信息。

122.1 PIM_CBSR_TO_EBSR

日志内容	PIM C-BSR wins BSR Election. (C-BSRAddr=[STRING], VPNName=[STRING])
日志含义	CBSR选举为BSR
参数解释	$1：C-BSR地址 $2：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6 (Notification)
举例	PIM6/6/PIM_CBSR_TO_EBSR: PIM C-BSR wins BSR Election. (C-BSRAddr=100::1, VPNName=vpn-test)
对系统的影响	系统相关表项的BSR更新为最新BSR地址
日志产生原因	C-BSR赢得BSR选举
处理建议	1. 请确认当前 BSR 变化是否为管理员所期望。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 2。 2. 请确认旧的 E-BSR 地址所在设备是否存在故障，或者存在当前设备和旧的 E-BSR 之间的链路恢复，或者删除 BSR 配置，或者修改 BSR 配置。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 3。 3. 请在旧的当选BSR的设备上，执行 **display ipv6 pim interface**命令查看当前是否有对应生效的PIM接口。 o 如果没有，请配置正确的对应 PIM 接口。 o 如果有，则请执行步骤 4。 4. 请用 **display memory**命令查看当前设备是否内存不足。 o 如果内存不足，请先解决内存问题。 o 如果内存充足，则请执行步骤 5。 5. 请在当前设备上执行 **ping**命令，检查和旧的当选BSR的设备之间的链路是否连通。 o 如果连通，则请执行步骤 6。 o 如果不连通，则请先解决链路连通问题。 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

122.2 PIM_DR_ELECTION

日志内容	The interface is elected as a DR. (IfIndex:[UINT32], IfName:[STRING], IfAddr:[STRING], VPNName:[STRING])
日志含义	接口所在的设备被选举为DR
参数解释	$1：接口索引 $2：接口名称 $3：接口地址 $4：VPN实例名称
日志等级	5 (Notification)
举例	PIM6/5/PIM_DR_ELECTION: The interface is elected as a DR. (IfIndex:12, IfName:iftest, IfAddr:100::2, VPNName:vpntest)
对系统的影响	系统相关表项的DR更新为最新DR接口地址
日志产生原因	接口所在的设备被选举为DR
处理建议	确认该设备被选举为DR是否为管理员所期望的： • 如果不是，可通过为该设备的接口配置较低的 DR 优先级或者较小 IP 地址，使得该设备不当选 DR • 如果是，无需处理

122.3 PIM_ERR_INVALID_JP

日志内容	PIM receives an Invalid Join/Prune message. (GroupMappingOrigin=[STRING], GroupMappingAddrType=[STRING], GrpAddr=[STRING], GrpPfxLen=[UINT32], GroupMappingRPAddrType=[STRING], RPAddr=[STRING], GroupMappingPimMode=[STRING], InvJPAddrType=[STRING], InvJPOriginAddr=[STRING], InvJPGrpAddr=[STRING], InvJPRpAddr=[STRING], NbrIfIndex=[UINT32], NbrAddrType=[STRING], NbrAddr=[NbrAddr], NbrUpTime=[STRING], VPNName=[STRING], RecvIfName=[STRING])
日志含义	PIM收到无效的加入/剪枝报文
参数解释	$1：RP映射组类型 $2：组地址类型 $3：JP报文中的组地址 $4：组掩码长度 $5：RP地址的类型 $6：RP地址 $7：当前运行的PIM模式 $8：无效的JP报文的地址类型 $9：无效的JP报文中的源地址 $10：无效的JP报文的组地址 $11：无效的JP报文中的RP地址 $12：邻居接口索引 $13：邻居地址的类型 $14：邻居的地址 $15：邻居存活的时间 $16：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称 $17：接收该报文的接口名
日志等级	4(Notification)
举例	PIM6/4/PIM_ERR_INVALID_JP: PIM receives an Invalid Join/Prune message. (GroupMappingOrigin=bsr-rp, GroupMappingAddrType=IPv6, GrpAddr=fe33::1, GrpPfxLen=64, GroupMappingRPAddrType=IPv6, RPAddr=100::2, GroupMappingPimMode=PIM-SM, InvJPAddrType=IPv6 ,InvJPOriginAddr=100::12, InvJPGrpAddr= fe33::1, InvJPRpAddr=100::22, NbrIfIndex=258, NbrAddrType=IPv6, NbrAddr=100::2, NbrUpTime=18:12:15, VPNName= vpn-test, RecvIfName=GigabitEthernet2/0/1)
对系统的影响	对系统无影响
日志产生原因	PIM收到无效的加入/剪枝报文。
处理建议	检查本路由器和J/P报文发送端路由器，二者SSM范围是否相同： • 如果 SSM 范围相同，则请修改 J/P 报文发送端路由器和本路由器对于该组的 RP 配置，使得二者一致 • 如果SSM范围不同，则请执行 **ssm-policy**命令配置相同的SSM范围

122.4 PIM_ERR_INVALID_REG

日志内容	PIM receives an Invalid register message. (GroupMappingOrigin=[STRING], GroupMappingAddrType=[STRING], GrpAddr=[STRING], GrpPfxLen=[UINT32], GroupMappingRPAddrType=[STRING], RPAddr=[STRING], GroupMappingPimMode=[STRING], InvRegAddrType=[STRING], InvRegOriginAddr=[STRING], InvRegGrpAddr=[STRING], InvRegRpAddr=[STRING], VPNName=[STRING])
日志含义	PIM收到无效的注册报文
参数解释	$1：RP映射组类型 $2：组地址类型 $3：JP报文中的组地址 $4：组掩码长度 $5：RP地址的类型 $6：RP地址 $7：当前运行的PIM模式 $8：无效的JP报文的地址类型 $9：无效的JP报文中的源地址 $10：无效的JP报文的组地址 $11：无效的JP报文中的RP地址 $12：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称。
日志等级	4 (Notification)
举例	PIM6/4/PIM_ERR_INVALID_REG: PIM receives an Invalid register message. (GroupMappingOrigin=bsr-rp, GroupMappingAddrType=IPv4, GrpAddr= fe31::1, GrpPfxLen=64, GroupMappingRPAddrType=IPv6, RPAddr=100::1, GroupMappingPimMode=PIM-SM, InvRegAddrType=IPv4, InvRegOriginAddr=200::1, InvRegGrpAddr=fe31::1, InvRegRpAddr=200::1, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	PIM收到无效的注册报文。
处理建议	检查本路由器和J/P报文发送端路由器，二者SSM范围是否相同： • 如果 SSM 范围相同，则请修改 J/P 报文发送端路由器和本路由器对于该组的 RP 配置，使得二者一致 • 如果 SSM 范围不同，则请执行 ssm-policy 命令配置相同的 SSM 范围

122.5 PIM_EBSR_TO_CBSR

日志内容	PIM E-BSR lost BSR Election. (C-BSRAddr=[STRING], Priority=[UINT32], VPNName=[STRING])
日志含义	已当选BSR的当前设备BSR选举失败
参数解释	$1：C-BSR地址 $2：BSR优先级 $3：公网时，该参数为"_public_"；私网时，该参数为VPN实例的名称
日志等级	6 (Notification)
举例	PIM6/6/CBSR_TO_EBSR: PIM C-BSR wins BSR Election. (C-BSRAddr=100::3, Priority=10, VPNName=vpn-test)
对系统的影响	对系统无影响
日志产生原因	已当选BSR的当前设备BSR选举失败
处理建议	1. 请确认当前 BSR 变化是否为管理员所期望。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 2。 2. 请确认新的 BSR 地址所在设备是否存在故障恢复，或者存在当前设备和新的 E-BSR 之间的链路恢复，或者新增 BSR 配置，或者修改 BSR 配置。 o 如果是，则属于正常运行信息，无需处理。 o 如果不是，则请执行步骤 3。 3. 请在 PIM 视图下执行 display this 命令查看当前设备是否配置正确的 BSR 地址。 o 如果未配置，则请配置对应的 BSR 地址。 o 如果已配置，则请执行步骤 4。 4. 请执行 **display ipv6 pim bsr-info**命令查看当前设备是否为C-BSR。 o 如果不是，则请执行步骤 4。 o 如果是，则请执行步骤 6。 5. 请执行 **display ipv6 pim interface**命令查看当前C-BSR地址是否有对应生效的PIM接口。 o 如果没有，请配置正确的对应 PIM 接口。 o 如果有，则请执行步骤 6。 6. 请执行 **display memory**命令查看当前设备是否内存不足。 o 如果内存不足，请先解决内存问题。 o 如果内存充足，则请执行步骤 7。 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

122.6 PIM_NBR_LOSS

日志内容	STRING] Neighbor [STRING] ([STRING]) is loss, and the router has no other neighbors on the same interface with the same IP version and a lower IP address than itself.(UpTime=[STRING], NeighborDownReason=[STRING])
日志含义	接口PIM邻居关系丢失
参数解释	$1：公网侧PIM邻居down时，该参数为空；私网侧PIM邻居down时，该参数为VPN实例的名称 $2：PIM邻居的IP地址 $3：接口名称 $4：接口UP时长 $5：PIM邻居down的原因： • Neighbor timer expired.：邻居的 HoldTime 定时器超时 • Neighbor is deleted.：邻居删除 • Receive hello cancel message.：收到 HoldTime 为零的邻居消息 • BFD session is down.：邻居的 BFD 会话 down
日志等级	6 (Notification)
举例	PIM6/6/PIM_NBR_LOSS: Neighbor 100::1(Vlan-interface10) is loss, and the router has no other neighbors on the same interface with the same IP version and a lower IP address than itself.(UpTime=00:01:20, NeighborDownReason=Interface is down.)
对系统的影响	PIM邻居关系丢失或建立连接失败，路由不可达，数据转发业务中断
日志产生原因	PIM邻居的状态变为down，且同一接口上没有其他IP版本相同且IP地址较小的PIM邻居
处理建议	检查PIM配置是否错误以及检查网络是否发生故障

122.7 PIM_RP_CHANGED

日志内容	The RP changes. (RPType:[STRING], GrpAddr:[STRING], GrpPfxLen:[UINT32], RPAddr:[STRING], PimMode:[STRING], Priority:[UINT32], VPNName:[STRING])
日志含义	RP发生改变
参数解释	$1：RP的类型： • static-rp：静态 RP • auto-rp：自动 RP • bsr-rp：BSR RP • embedded：嵌入式 RP 2：组播组地址 3：组播组地址掩码长度 4：当选的RP地址 5：当前运行的PIM模式： • PIM-SM：PIM-SM 模式 • Bidir-PIM：双向 PIM 模式 6：RP的优先级 7：VPN实例名称
日志等级	5 (Notification)
举例	PIM6/5/PIM_RP_CHANGED: The RP changes. (RPType:static-rp, GrpAddr:fe45::1, GrpPfxLen:8, RPAddr:100::2, PimMode:PIM-SM, Priority:64, VPNName:vpntest)
对系统的影响	系统相关表项的RP更新为最新RP接口地址
日志产生原因	RP发生改变
处理建议	确认RP变化是否为管理员所期望的： • 如果不是，则可以将本设备配置为静态 RP，或者提高 RP 的优先级，使得本设备重新被选举为 RP • 如果是，在无需处理

123 PING

本节介绍 ping 模块输出的日志信息。

123.1 PING_STATISTICS

日志内容	[STRING] statistics for [STRING]: [UINT32] packet(s) transmitted, [UINT32] packet(s) received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
日志含义	公网Ping的统计信息
参数解释	$1：Ping或Ping6 $2：目的IP地址，IPv6地址，或主机名 $3：发送的回显请求数量 $4：接收的回显应答数量 $5：没有回复的报文占总请求报文比 $6：最小往返时间 $7：平均往返时间 $8：最大往返时间 $9：往返时间标准差
日志等级	6 (Informational)
举例	PING/6/PING_STATISTICS: Ping statistics for 192.168.0.115: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
对系统的影响	对系统无影响
日志产生原因	用户执行**ping**命令查看公网中对端是否可达

处理建议	• 如果统计结果中丢包率为 0，则说明通信正常，无需处理
	• 如果统计结果中丢包率大于 0，小于 100%，则说明有丢包，丢包原因可能为链路不稳定或者有突发流量挤占带宽导致丢包。您可以进行以下处理：
	  ◦ 请使用 **display interface**命令查看接口状态，如果接口状态频繁的在up和down之间切换，可能为网线故障或者接口元器件故障，请进一步定位并解决
	  ◦ 执行 **display counter**命令显示最近一个统计周期内处于up状态的接口的报文速率统计信息，如果接口流量有明显增长，则说明可能存在突发流量，需要对流量进行抓包或者镜像分析，可设置ACL规则对非法流量进行过滤
	• 如果统计结果中丢包率为 100%，您可以进行以下处理：
	  ◦ 请执行 **display interface**命令检查接口是否down，如果接口状态为down，请根据显示信息中的提示进一步解决接口故障问题
	  ◦ 请执行 **display routing-table**或**display ipv6 routing-table**命令查看公网路由表中是否有去往目的端的路由，如果无路由，请手工添加路由或者通过动态协议引入路由

123.2 PING_VPN_STATISTICS

日志内容	[STRING] statistics for [STRING] in VPN instance [STRING]: [UINT32] packet(s) transmitted, [UINT32] packet(s) received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
日志含义	私网Ping的统计信息
参数解释	$1：Ping或Ping6 $2：目的IP地址，IPv6地址，或主机名 $3：VPN实例名 $3：发送的回显请求数量 $4：接收的回显应答数量 $5：没有回复的报文占总请求报文比 $6：最小往返时间 $7：平均往返时间 $8：最大往返时间 $9：往返时间标准差
日志等级	6 (Informational)
举例	PING/6/PING_VPN_STATISTICS: Ping statistics for 192.168.0.115 in VPN instance vpn1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
对系统的影响	对系统无影响
日志产生原因	用户执行**ping**命令查看VPN中的对端是否可达

处理建议	• 如果统计结果中丢包率为 0，则说明通信正常，无需处理
	• 如果统计结果中丢包率大于 0，小于 100%，则说明有丢包，丢包原因可能为链路不稳定或者有突发流量挤占带宽导致丢包。您可以进行以下处理：
	  ○ 请使用 **display interface**命令查看接口状态，如果接口状态频繁的在up和down之间切换，可能为网线故障或者接口元器件故障，请进一步定位并解决
	  ○ 执行 **display counter**命令显示最近一个统计周期内处于up状态的接口的报文速率统计信息，如果接口流量有明显增长，则说明可能存在突发流量，需要对流量进行抓包或者镜像分析，可设置ACL规则对非法流量进行过滤
	• 如果统计结果中丢包率为 100%，您可以进行以下处理：
	  ○ 请执行 **display interface**命令检查接口是否down，如果接口状态为down，请根据显示信息中的提示进一步解决接口故障问题
	  ○ 请执行带 **vpn**参数的 **display routing-table**或**display ipv6 routing-table**命令查看VPN的路由表中是否有去往目的端的路由，如果无路由，请手工添加路由或者通过动态协议引入路由

124 PKG

本节介绍包管理模块输出的日志信息。

124.1 PKG_ACTIVE_NEED_RESTART

日志内容	The installation of patch [STRING] on [STRING] requires a restart.
日志含义	补丁包安装需要重启
参数解释	$1：补丁包名称 $2：需要重启的设备或单板
日志等级	5
举例	PKG/5/PKG_ACTIVE_NEED_RESTART: The installation of patch system-patch1.bin on CPU 0 of slot 5 requires a restart.
对系统的影响	*对系统无影响*
日志产生原因	安装完需要重启才能生效的补丁包后，打印此日志信息，提示用户重启
处理建议	1. 检查补丁包是否为需要重启才能生效的补丁包 2. 检查补丁包是否安装成功 3. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

124.2 PKG_BOOTLOADER_FILE_FAILED

日志内容	Failed to execute the boot-loader file command.
日志含义	用户执行**boot-loader file**命令配置设备下次启动时使用的软件包失败
参数解释	无
日志等级	5 (Notification)
举例	PKG/5/PKG_BOOTLOADER_FILE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the boot-loader file command.
对系统的影响	对系统无影响
日志产生原因	用户执行**boot-loader file**命令配置设备下次启动时使用的软件包失败，需根据提示信息分析原因
处理建议	请根据提示信息采取相应措施

124.3 PKG_BOOTLOADER_FILE_SUCCESS

日志内容	Executed the boot-loader file command successfully.
日志含义	用户执行**boot-loader file**命令配置设备下次启动时使用的软件包成功
参数解释	无
日志等级	5 (Notification)
举例	PKG/5/PKG_BOOTLOADER_FILE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the boot-loader file command successfully.
对系统的影响	对系统无影响
日志产生原因	用户执行**boot-loader file**命令配置设备下次启动时使用的软件包成功
处理建议	无需处理

124.4 PKG_INACTIVE_NEED_RESTART

日志内容	The uninstallation of patch [STRING] on [STRING] requires a restart.
日志含义	补丁包卸载需要重启
参数解释	$1：补丁包名称 $2：需要重启的设备或单板
日志等级	5
举例	PKG/5/ PKG_INACTIVE_NEED_RESTART: The uninstallation of patch system-patch1.bin on CPU 0 of slot 5 requires a restart.
对系统的影响	*对系统无影响*
日志产生原因	卸载完需要重启才能生效的补丁包后，打印此日志信息，提示用户重启
处理建议	**1.** 检查补丁包是否为需要重启才能生效的补丁包 **2.** 检查补丁包是否卸载成功 **3.** 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

124.5 PKG_INSTALL_ACTIVATE_FAILED

日志内容	Failed to execute the install activate command.
日志含义	用户执行**install activate**命令用来激活或查看软件包，操作失败
参数解释	无
日志等级	5 (Notification)
举例	PKG/5/PKG_INSTALL_ACTIVATE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the install activate command.
对系统的影响	对系统无影响
日志产生原因	用户执行**install activate**命令用来激活或查看软件包失败，需根据提示信息分析原因
处理建议	请根据提示信息采取相应措施

124.6 PKG_INSTALL_ACTIVATE_SUCCESS

日志内容	Executed the install activate command successfully.
日志含义	用户执行**install activate**命令用来激活或查看软件包成功
参数解释	无
日志等级	5 (Notification)
举例	PKG/5/PKG_INSTALL_ACTIVATE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the install activate command successfully.
对系统的影响	对系统无影响
日志产生原因	用户执行**install activate**命令用来激活或查看软件包，操作成功
处理建议	无需处理

124.7 PKG_UPGRADE_INFO

日志内容	The [STRING] device upgraded the software version from [STRING] to software [STRING].
日志含义	升级成功显示升级前后的版本信息
参数解释	$1：设备名 $2：升级前的版本号 $3：升级后的版本
日志等级	5 (Notification)
举例	PKG/5/PKG_UPGRADE_INFO: The S6850-56HF device upgraded the software version from software version 1-patch version 1 to software version 2-patch version 2.
对系统的影响	对系统无影响
日志产生原因	执行**install**、**issu**或**boot-loade**r命令成功，新版本生效
处理建议	无需处理

125 PKI

本节包含 PKI 日志消息。

125.1 GET_CERT_FROM_CA_SERVER_FAIL

日志内容	Failed to get the CA or RA certificate from the CA server. Reason: [STRING].
日志含义	从CA服务器获取CA/RA证书失败
参数解释	$1：获取CA/RA证书失败原因： • 获取 PKI 的源 IP 地址失败，显示为：failed to get the source IP address of PKI protocol packets. • 获取证书链失败，显示为：failed to get the certificate chain. • 证书链没有根 CA，显示为：root CA not found in the certificate chain. • 验证 CA/RA 证书链失败，显示为：failed to verify the CA/RA certificate chain (%s).
日志等级	5 (Notification)
举例	PKI/5/GET_CERT_FROM_CA_SERVER_FAIL: Failed to get the CA or RA certificate from the CA server. Reason: root CA not found in the certificate chain.
对系统的影响	证书相关业务功能不可用
日志产生原因	从CA服务器获取CA/RA证书失败，具体原因见【参数解释】
处理建议	根据日志中具体提示的失败原因，进行相应处理

125.2 IMPORT_CERT_FAIL

日志内容	Failed to import the certificate. Reason: [STRING].
日志含义	导入证书失败
参数解释	$1：失败原因： • 获取颁发者证书失败，显示为：unable to get issuer certificate. • 无法获取证书的 CRL，显示为：unable to get certificate CRL. • 无法解密 CRL 的签名，显示为：unable to decrypt CRL's signature. • 无法解析颁发者的公钥，显示为：unable to decode issuer public key. • 证书签名错误，显示为：certificate signature failure. • CRL 签名失败，显示为：CRL signature failure. • 解密证书签名失败，显示为：unable to decrypt certificate's signature. • 证书尚未生效，显示为：certificate is not yet valid. • 证书已失效，显示为：certificate has expired. • CRL 尚未生效，显示为：CRL is not yet valid. • CRL 已经失效，显示为：CRL has expired. • 证书的起始时间格式错误，显示为：format error in certificate's notBefore field. • 证书的结束时间格式错误，显示为：format error in certificate's notAfter field. • CRL 的上次更新时间格式错误，显示为：format error in CRL's lastUpdate field. • CRL 的下次更新时间格式错误，显示为：format error in CRL's nextUpdate field. • 内存不足，显示为：out of memory. • 自签名证书，显示为：self signed certificate. • 证书链中存在自签名证书，显示为：self signed certificate in certificate chain. • 获取本地颁发者证书失败，显示为：unable to get local issuer certificate. • 验证首个证书失败，显示为：unable to verify the first certificate. • 证书链过长，显示为：certificate chain too long. • 证书被撤回，显示为：certificate revoked. • 无效的 CA 证书，显示为：invalid CA certificate. • 无效的非 CA 证书，显示为：invalid non-CA certificate (has CA markings). • 超过路径深度约束，显示为：path length constraint exceeded. • 超过代理路径深度约束，显示为：proxy path length constraint exceeded. • 代理证书不通过，请设置合适的标记，显示为：proxy certificates not allowed, please set the appropriate flag. • 不支持的证书用途，显示为：unsupported certificate purpose. • 证书不被信任，显示为：certificate not trusted. • 证书被拒绝，显示为：certificate rejected. • 证书应用验证失败，显示为：application verification failure. • 证书主题颁发者不匹配，显示为：subject issuer mismatch. • 授权和主题密钥认证人不匹配，显示为：authority and subject key identifier mismatch. • 授权和颁发者序列号不匹配，显示为：authority and issuer serial number

	mismatch. • 密钥用途不包括证书签名，显示为：key usage does not include certificate signing. • 获取 CRL 颁发者证书失败，显示为：unable to get CRL issuer certificate. • 不受控的决定性的扩展，显示为：unhandled critical extension. • 密钥用途不包括 CRL 签名，显示为：key usage does not include CRL signing. • 密钥用途不包括数字签名，显示为：key usage does not include digital signature. • 不受控的决定性的 CRL 扩展，显示为：unhandled critical CRL extension. • 无效或不一致的证书扩展，显示为：invalid or inconsistent certificate extension. • 无效或不一致的证书策略扩展，显示为：invalid or inconsistent certificate policy extension. • 不存在明确的策略，显示为：no explicit policy. • CRL 范围不同，显示为：Different CRL scope. • 不支持的扩展特性，显示为：Unsupported extension feature. • RFC 3779 资源不是父资源的子集，显示为：RFC 3779 resource not subset of parent's resources. • 被允许的子树违规，显示为：permitted subtree violation. • 被排除的子树违规，显示为：excluded subtree violation. • 名字约束的最小和最大范围不支持，显示为：name constraints minimum and maximum not supported. • 不支持的名字约束类型，显示为：unsupported name constraint type. • CRL 路径检验失败，显示为：CRL path validation error. • 不支持的或无效的名字语法，显示为：unsupported or invalid name syntax. • 不支持的或无效的名字约束语法，显示为：unsupported or invalid name constraint syntax. • Suite B：证书版本号无效，显示为：Suite B: certificate version invalid. • Suite B：无效的公钥算法，显示为：Suite B: invalid public key algorithm. • Suite B：无效的 ECC 曲线，显示为：Suite B: invalid ECC curve. • Suite B：无效的签名算法，显示为：Suite B: invalid signature algorithm. • Suite B：曲线不被本 LOS 准许，显示为：Suite B: curve not allowed for this LOS. • Suite B：不能使用 P-256 给 P-384 签名，显示为：Suite B: cannot sign P-384 with P-256. • 主机名不匹配，显示为：Hostname mismatch. • 邮件地址簿匹配，显示为：Email address mismatch. • IP 地址不匹配，显示为：IP address mismatch. • 无效的证书认证上下文，显示为：Invalid certificate verification context. • 颁发者证书检查失败，显示为：Issuer certificate lookup error. • 代理主题名称不规范，显示为：proxy subject name violation.

日志等级	5 (Notification)
举例	PKI/5/IMPORT_CERT_FAIL: Failed to import the certificate. Reason: invalid CA certificate.
对系统的影响	证书相关业务功能不可用
日志产生原因	证书导入失败，具体原因见【参数解释】
处理建议	根据日志中具体提示的失败原因，进行相应处理

125.3 REQUEST_CERT_FAIL

日志内容	Failed to request certificate of domain [STRING].
日志含义	获取本地证书失败
参数解释	$1：PKI域名
日志等级	5 (Notification)
举例	PKI/5/REQUEST_CERT_FAIL: Failed to request certificate of domain abc.
对系统的影响	• 系统没有证书，证书相关业务功能不可用 • 证书到期后，证书相关业务功能不可用
日志产生原因	为PKI域申请证书失败
处理建议	1. 执行 **display clock**命令检查设备时间是否正确： o 如果不正确，在用户视图下执行 **clock datetime**命令修改设备时间 o 如果正确，请执行步骤 2 2. 通过 Ping 方式检查设备与 CA 服务器之间的路由是否可达： o 如果不可达，请排查路由和物理链路，使得两者之间路由可达 o 如果可达，请执行步骤 3 3. 检查 CA 服务器的服务是否正常： o 如果不正常，请确保 CA 服务器的服务正常 o 如果正常，请执行步骤 4 4. 请收集配置文件、日志信息和告警信息，并联系技术支持

125.4 REQUEST_CERT_SUCCESS

日志内容	Request certificate of domain [STRING] successfully.
日志含义	获取本地证书成功
参数解释	$1：PKI域名
日志等级	5 (Notification)
举例	PKI/5/REQUEST_CERT_SUCCESS: Request certificate of domain abc successfully.
对系统的影响	对系统无影响
日志产生原因	为PKI域申请证书成功
处理建议	无需处理

125.5 RETRIEVE_CRL_FAIL

日志内容	Failed to retrieve the CRL. Reason: [STRING].
日志含义	获取CRL失败
参数解释	$1：失败原因： • 证书请求 URL 未配置，显示为：certificate request URL is not configured. • 本地证书不存在，显示为：no local certificate. • 从 RA 服务器获取 CRL 时，RA 证书不存在，显示为：no RA certificate. • 证书申请的注册受理机构未配置，显示为：type of certificate request reception authority is not configured. • 获取 PKI 的源 IP 地址失败，显示为：failed to get the source IP address of PKI protocol packets. • 本地证书和密钥不匹配，显示为：local certificate and key mismatch. • 获取加密证书失败，显示为：failed to get the encryption certificate. • 从 CA 获取证书签发者失败，显示为：failed to get issuer name from CA certificate. • 从 CA 证书获取 CA 证书的序列号失败，显示为：failed to get serial number from CA certificate. • 解析 URL 失败，显示为：failed to parse the URL. • 从回应消息中获取 CRL 失败，显示为：failed to get CRLs from reply. • 从回应消息中获取 CRL 数据失败，显示为：failed to get CRL data from the reply. • 获取本地颁发者 CA 失败，显示为：unable to get local issuer certificate. • CRL 签名失败，显示为：CRL signature failure. • 解码颁发者公钥失败，显示为：unable to decode issuer public key. • CRL 的上次更新时间格式错误，显示为：Format error in CRL's lastUpdate field. • CRL 尚未生效，显示为：CRL is not yet valid. • CRL 的下次更新时间格式错误，显示为：Format error in CRL's nextUpdate field. • CRL 已经失效，显示为：CRL has expired. • 获取颁发者证书失败，显示为：unable to get issuer certificate. • 保存 CRL 到设备失败，显示为：Failed to save the CRL to the device. • 无法获取证书的 CRL，显示为：unable to get certificate CRL. • 无法解密 CRL 的签名，显示为：unable to decrypt CRL's signature
日志等级	5 (Notification)
举例	PKI/5/RETRIEVE_CRL_FAIL: Failed to retrieve the CRL. Reason: CRL has expired.
对系统的影响	• 系统没有 CRL，证书相关业务功能不可用 • CRL 到期后，证书相关业务功能不可用
日志产生原因	获取CRL失败，具体原因见【参数解释】
处理建议	根据日志中具体提示的失败原因，进行相应处理

125.6 VALIDATE_CERT_FAIL

日志内容	Failed to validate the certificate. Reason: [STRING].
日志含义	证书验证失败
参数解释	$1：失败原因： • 获取颁发者证书失败，显示为：unable to get issuer certificate. • 无法获取证书的 CRL，显示为：unable to get certificate CRL. • 无法解密 CRL 的签名，显示为：unable to decrypt CRL's signature. • 无法解析颁发者的公钥，显示为：unable to decode issuer public key. • 证书签名错误，显示为：certificate signature failure. • CRL 签名失败，显示为：CRL signature failure. • 解密证书签名失败，显示为：unable to decrypt certificate's signature. • 证书尚未生效，显示为：certificate is not yet valid. • 证书已失效，显示为：certificate has expired. • CRL 尚未生效，显示为：CRL is not yet valid. • CRL 已经失效，显示为：CRL has expired. • 证书的起始时间格式错误，显示为：format error in certificate's notBefore field. • 证书的结束时间格式错误，显示为：format error in certificate's notAfter field. • CRL 的上次更新时间格式错误，显示为：format error in CRL's lastUpdate field. • CRL 的下次更新时间格式错误，显示为：format error in CRL's nextUpdate field. • 内存不足，显示为：out of memory. • 自签名证书，显示为：self signed certificate. • 证书链中存在自签名证书，显示为：self signed certificate in certificate chain. • 获取本地颁发者证书失败，显示为：unable to get local issuer certificate. • 验证首个证书失败，显示为：unable to verify the first certificate. • 证书链过长，显示为：certificate chain too long. • 证书被撤回，显示为：certificate revoked. • 无效的 CA 证书，显示为：invalid CA certificate. • 无效的非 CA 证书，显示为：invalid non-CA certificate (has CA markings). • 超过路径深度约束，显示为：path length constraint exceeded. • 超过代理路径深度约束，显示为：proxy path length constraint exceeded. • 代理证书不通过，请设置合适的标记，显示为：proxy certificates not allowed, please set the appropriate flag. • 不支持的证书用途，显示为：unsupported certificate purpose. • 证书不被信任，显示为：certificate not trusted. • 证书被拒绝，显示为：certificate rejected. • 证书应用验证失败，显示为：application verification failure. • 证书主题颁发者不匹配，显示为：subject issuer mismatch. • 授权和主题密钥认证人不匹配，显示为：authority and subject key identifier mismatch. • 授权和颁发者序列号不匹配，显示为：authority and issuer serial number

	mismatch. • 密钥用途不包括证书签名，显示为：key usage does not include certificate signing. • 获取 CRL 颁发者证书失败，显示为：unable to get CRL issuer certificate. • 不受控的决定性的扩展，显示为：unhandled critical extension. • 密钥用途不包括 CRL 签名，显示为：key usage does not include CRL signing. • 密钥用途不包括数字签名，显示为：key usage does not include digital signature. • 不受控的决定性的 CRL 扩展，显示为：unhandled critical CRL extension. • 无效或不一致的证书扩展，显示为：invalid or inconsistent certificate extension. • 无效或不一致的证书策略扩展，显示为：invalid or inconsistent certificate policy extension. • 不存在明确的策略，显示为：no explicit policy. • CRL 范围不同，显示为：Different CRL scope. • 不支持的扩展特性，显示为：Unsupported extension feature. • RFC 3779 资源不是父资源的子集，显示为：RFC 3779 resource not subset of parent's resources. • 被允许的子树违规，显示为：permitted subtree violation. • 被排除的子树违规，显示为：excluded subtree violation. • 名字约束的最小和最大范围不支持，显示为：name constraints minimum and maximum not supported. • 不支持的名字约束类型，显示为：unsupported name constraint type. • CRL 路径检验失败，显示为：CRL path validation error. • 不支持的或无效的名字语法，显示为：unsupported or invalid name syntax. • 不支持的或无效的名字约束语法，显示为：unsupported or invalid name constraint syntax. • Suite B：证书版本号无效，显示为：Suite B: certificate version invalid. • Suite B：无效的公钥算法，显示为：Suite B: invalid public key algorithm. • Suite B：无效的 ECC 曲线，显示为：Suite B: invalid ECC curve. • Suite B：无效的签名算法，显示为：Suite B: invalid signature algorithm. • Suite B：曲线不被本 LOS 准许，显示为：Suite B: curve not allowed for this LOS. • Suite B：不能使用 P-256 给 P-384 签名，显示为：Suite B: cannot sign P-384 with P-256. • 主机名不匹配，显示为：Hostname mismatch. • 邮件地址簿匹配，显示为：Email address mismatch. • IP 地址不匹配，显示为：IP address mismatch. • 无效的证书认证上下文，显示为：Invalid certificate verification context. • 颁发者证书检查失败，显示为：Issuer certificate lookup error. • 代理主题名称不规范，显示为：proxy subject name violation.

日志等级	5 (Notification)
举例	PKI/5/VALIDATE_CERT_FAIL: Failed to validate the certificate. Reason: Invalid CA certificate.
对系统的影响	证书相关业务功能不可用
日志产生原因	证书验证失败，具体原因见【参数解释】
处理建议	根据日志中具体提示的失败原因，进行相应处理

126 PKT2CPU

本节包含 PKT2CPU 日志消息。

126.1 PKT2CPU_NO_RESOURCE

日志内容	-Interface=[STRING]-ProtocolType=[UINT32]-MacAddr=[STRING]; The resources are insufficient. -Interface=[STRING]-ProtocolType=[UINT32]-SrcPort=[UINT32]-DstPort=[UINT32]; The resources are insufficient.
日志含义	硬件资源不足
参数解释	$1：接口名 $2：协议类型 $3：MAC地址或源端口 $4：目的端口
日志等级	4 (Warning)
举例	PKT2CPU/4/PKT2CPU_NO_RESOURCE: -Interface=Ethernet0/0/2-ProtocolType=21-MacAddr=0180-c200-0014; The resources are insufficient.
对系统的影响	设备硬件资源紧张，影响业务处理能力
日志产生原因	当设备硬件资源不足时，打印该日志
处理建议	1. 根据实际情况，取消不必要的配置 2. 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

127 PKTCPT

本节介绍 PKTCPT（Packet Capture）模块输出的日志信息。

127.1 PKTCPT_AP_OFFLINE

日志内容	Failed to start packet capture. Reason: AP was offline.
日志含义	开启AP的报文捕获功能失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_AP_OFFLINE: Failed to start packet capture. Reason: AP was offline.
对系统的影响	对系统无影响
日志产生原因	开启AP的报文捕获功能失败，因为AP未上线
处理建议	执行**display wlan ap all**命令查看AP的状态，如果State字段取值为R、R/M或者R/B，则说明AP已上线且稳定运行，可以开启报文捕获功能

127.2 PKTCPT_AREADY_EXIT

日志内容	Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
日志含义	AC/FIT AP组网，在AC上开启AP的报文捕获功能失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_AREADY_EXIT: Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
对系统的影响	对系统无影响
日志产生原因	AC/FIT AP组网，当AC上的报文捕获功能先停止时，AP还在上传捕获的报文。此时用户再次开启报文捕获功能，报文捕获功能会启动失败
处理建议	请稍后重新开启报文捕获功能

127.3 PKTCPT_CONN_FAIL

日志内容	Failed to start packet capture. Reason: Failed to connect to the FTP server.
日志含义	开启报文捕获功能失败，因为连接FTP服务器失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_CONN_FAIL: Failed to start packet capture. Reason: Failed to connect to the FTP server.
对系统的影响	对系统无影响
日志产生原因	配置报文捕获功能时，指定将捕获的报文保存到FTP服务器。因为无法连接到与FTP服务器，导致报文捕获功能启动失败
处理建议	• 对 FTP 服务器地址执行 Ping 操作。如果 Ping 失败，请先解决 Ping 不通问题 • 重新开启报文捕获功能，如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

127.4 PKTCPT_INVALID_FILTER

日志内容	Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
日志含义	捕获过滤规则非法，启动报文捕获功能失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_INVALD_FILTER: Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
对系统的影响	对系统无影响
日志产生原因	捕获过滤规则非法，启动报文捕获功能失败
处理建议	修改捕获过滤规则

127.5 PKTCPT_LOGIN_DENIED

日志内容	Packet capture aborted. Reason: FTP server login failure.
日志含义	登录FTP服务器失败，报文捕获退出
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_LOGIN_DENIED: Packet capture aborted. Reason: FTP server login failure.
对系统的影响	对系统无影响
日志产生原因	登录FTP服务器失败，报文捕获退出
处理建议	登录FTP服务器使用的用户名密码必须和FTP服务器上配置的用户名、密码一致，否则，无法登录FTP服务器。在设备上执行**ftp**命令，输入用户名和密码，尝试给FTP服务器上传一个文件。如果测试失败，请定位并解决FTP上传失败问题

127.6 PKTCPT_MEMORY_ALERT

日志内容	Packet capture aborted. Reason: Memory threshold reached.
日志含义	设备达到内存门限时，报文捕获功能退出
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_MEMORY_ALERT: Packet capture aborted. Reason: Memory threshold reached.
对系统的影响	对系统无影响
日志产生原因	设备达到内存门限时，报文捕获功能退出

处理建议	• 释放内存资源。例如，执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源
	• 执行 **display memory**命令查看内存使用情况：
	  ○ 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，可以开启或者关闭进程对应的软件功能，来释放内存
	  ○ 如果内存占用率恢复到告警阈值以下，内存告警解除，Tcl 监控策略会继续生效，无需额外处理
	• 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员工程师

127.7 PKTCPT_OPEN_FAIL

日志内容	Failed to start packet capture. Reason: File for storing captured frames not opened.
日志含义	因为文件无法打开，开启报文捕获功能失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_OPEN_FAIL: Failed to start packet capture. Reason: File for storing captured frames not opened.
对系统的影响	对系统无影响
日志产生原因	将报文文件保存到FLASH时，文件路径无法打开，报文捕获功能启动失败
处理建议	• 若当前登录用户不具有写文件权限，请管理员通过 RBAC 功能为用户配置写文件权限。或者切换具有写文件权限的用户重新登录设备，再开启报文捕获功能 • 您指定的文件可能正在被别的进程访问，请使用其它文件名重新尝试

127.8 PKTCPT_OPERATION_TIMEOUT

日志内容	Failed to start or continue packet capture. Reason: Operation timed out.
日志含义	操作超时导致报文捕获失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_OPERATION_TIMEOUT: Failed to start or continue packet capture. Reason: Operation timed out.
对系统的影响	对系统无影响
日志产生原因	由于指定的与设备在不同网段的FTP服务器不可达，连接超时导致报文捕获启动失败；由于指定的与设备在不同网段的FTP服务器不在线，上传捕获的报文超时，导致报文捕获退出
处理建议	• 对 FTP 服务器执行 Ping 操作，检查 FTP 服务器是否可达。如果 Ping 失败，请先解决 FTP 服务器 Ping 不通的问题 • 检查FTP服务器能否正常提供个服务。在设备上执行 **ftp**命令，输入用户名和密码，尝试给FTP服务器上传一个文件。如果测试失败，请定位并解决FTP上传失败问题

127.9 PKTCPT_SERVICE_FAIL

日志内容	Failed to start packet capture. Reason: TCP or UDP port binding faults.
日志含义	由于TCP或者UDP端口绑定冲突等原因导致报文捕获功能启动失败
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_SERVICE_FAIL: Failed to start packet capture. Reason: TCP or UDP port binding faults.
对系统的影响	对系统无影响
日志产生原因	由于TCP或者UDP端口绑定冲突等原因导致报文捕获功能启动失败
处理建议	请使用新的端口号重新进行报文捕获： 1. 在设备上执行 **display tcp**和 **display udp**命令查看设备当前正在使用的TCP端口号和UDP端口号 2. 重新执行 **packet-capture remote**命令，端口号使用当前未被使用的TCP端口号或UDP端口号作为RPCAP服务侦听端口号 3. 请将客户端连接到设备，并在客户端上指定服务器端的IP地址为设备的IP地址以及服务器端的侦听的端口号为 **packet-capture remote**命令配置的 *port*值。客户端会使用该地址和端口号，和设备建立RPCAP连接 4. 设备通过 RPCAP 连接将捕获的报文发送给客户端 5. 客户端收到设备发送的报文后，对报文进行解析和展示

127.10 PKTCPT_UNKNOWN_ERROR

日志内容	Failed to start or continue packet capture. Reason: Unknown error.
日志含义	其它未知原因导致服务启动失败或者退出
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_UNKNOWN_ERROR: Failed to start or continue packet capture. Reason: Unknown error.
对系统的影响	对系统无影响
日志产生原因	其它未知原因导致服务启动失败或者退出
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

127.11 PKTCPT_UPLOAD_ERROR

日志内容	Packet capture aborted. Reason: Failed to upload captured frames.
日志含义	由于上传捕获的数据报文失败，导致报文捕获退出
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_UPLOAD_ERROR: Packet capture aborted. Reason: Failed to upload captured frames.
对系统的影响	对系统无影响
日志产生原因	指定文件目录不存在或者文件目录无写权限导致上传捕获的数据报文失败，导致报文捕获退出
处理建议	1. 确认 **packet-capture**命令中指定的目录在FTP服务器是否存在。如果不存在，请先在FTP服务器上创建目录，再在设备上执行报文捕获操作 2. 确认对 **packet-capture**命令中指定的目录是否具有写权限。在设备上执行 **ftp**命令，输入用户名和密码，尝试给 **packet-capture**命令中指定的目录上传一个文件： o 如果上传成功，则说明具有写权限 o 如果上传失败，则说明可能无写权限。请换一个 FTP 服务器工作路径下的目录再次尝试

127.12 PKTCPT_WRITE_FAIL

日志内容	Packet capture aborted. Reason: Not enough space to store captured frames.
日志含义	无存储空间导致报文捕获功能退出
参数解释	无
日志等级	6 (Informational)
举例	PKTCPT/6/PKTCPT_WRITE_FAIL: Packet capture aborted. Reason: Not enough space to store captured frames.
对系统的影响	对系统无影响
日志产生原因	报文文件保存到FLASH时，FLASH已满，报文捕获功能退出
处理建议	在用户视图执行**dir**命令，查看设备存储介质中的文件信息，可执行**delete /unreserved**命令删除无用文档来释放存储空间

128 PoE

本节介绍 PoE 模块输出的日志信息。

128.1 POE_AI_CLEAR

日志内容	Clearing all preceding AI configurations on PoE port [STRING]. Reason: The port still cannot supply power to the PD after forced power supply has been enabled on the port.
日志含义	AI PoE清除所有AI PoE配置，因为开启PoE接口的强制供电功能后，接口仍不能给PD供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_CLEAR: Recover the ai PoE configration on the PoE port GigabitEthernet1/0/1. Reason: The port still cannot supply power to the PD after forced power supply has been enabled on the port.
对系统的影响	对系统无影响
日志产生原因	AI PoE清除所有AI PoE配置，因为开启PoE接口的强制供电功能后，接口仍不能给PD供电
处理建议	1. 确认是否因为 PD 故障导致无法 PoE 供电。为 PD 切换电源，查看 PD 能否正常工作，如果 PD 不能正常工作，请先解决 PD 故障 2. 确认是否因为 PoE 接口故障导致无法 PoE 供电。更换 PoE 接口。将当前 PoE 接口的配置拷贝到其它 PoE 接口下，并将 PD 连接到新的 PoE 接口上，执行查看是否能够正常给 PD 供电。如果能正常供电，则说明原 PoE 接口可能存在故障，请定位 PoE 接口的问题 3. 确认是否因为 PoE 线缆故障导致无法 PoE 供电。更换 PoE 线缆查看是否能够正常给 PD 供电。如果能正常供电，则说明 PoE 线缆存在故障 4. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

128.2 POE_AI_DETECTIONMODE_NONE

日志内容	Changing the PD detection mode for PoE port [STRING] to none. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to simple.
日志含义	AI PoE修改对PD支持标准的检测方式为**none**来尝试恢复PoE供电，因为使用**simple**检测方式仍无法恢复PoE供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_DETECTIONMODE_NONE: Changing the PD detection mode for PoE port GigabitEthernet1/0/1 to **none**. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to **simple**.
对系统的影响	对系统无影响
日志产生原因	AI PoE修改对PD支持标准的检测方式为**none**来尝试恢复PoE供电，因为使用**simple**检测方式仍无法恢复PoE供电
处理建议	无需处理

128.3 POE_AI_DETECTIONMODE_SIMPLE

日志内容	Changing the PD detection mode for PoE port [STRING] to simple. Reason: The port still cannot supply power to the PD after non-standard PD detection is enabled.
日志含义	AI PoE修改对PD支持标准的检测方式为**simple**来尝试恢复PoE供电，因为开启接口的非标准PD检测功能仍无法恢复PoE供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_DETECTIONMODE_SIMPLE:Changing the PD detection mode for PoE port GigabitEthernet1/0/1 to **simple**. Reason: The port still cannot supply power to the PD after non-standard PD detection is enabled.
对系统的影响	对系统无影响
日志产生原因	AI PoE修改对PD支持标准的检测方式为**simple**来尝试恢复PoE供电，因为开启接口的非标准PD检测功能仍无法恢复PoE供电
处理建议	无需处理

128.4 POE_AI_DISCONNECT_AC

日志内容	Changing from MPS detection to AC detection on PoE port [STRING]. Reason: The port still cannot supply power to the PD after MPS detection is delayed.
日志含义	AI PoE切换MPS电流检测为AC检测来尝试恢复PoE供电，因为延迟启动MPS电流检测时间仍无法恢复PoE接口供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_DISCONNET_AC: Changing from MPS detection to AC detection on PoE port GigabitEthernet1/0/1. Reason: The port still cannot supply power to the PD after MPS detection is delayed.
对系统的影响	对系统无影响
日志产生原因	AI PoE切换MPS电流检测为AC检测来尝试恢复PoE供电，因为延迟启动MPS电流检测时间仍无法恢复PoE接口供电
处理建议	无需处理

128.5 POE_AI_DISCONNECT_DELAY

日志内容	Delaying the MPS detection on PoE port [STRING]. Reason: The port has stopped power supply because of MPS current insufficiency.
日志含义	AI PoE延迟启动MPS电流检测来尝试恢复PoE供电，因为MPS电流过小导致PoE接口停止对外供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_DISCONNET_DELAY:Delaying the MPS detection on PoE port GigabitEthernet1/0/1. Reason: The port has stopped power supply because of MPS current insufficiency.
对系统的影响	对系统无影响
日志产生原因	AI PoE延迟启动MPS电流检测来尝试恢复PoE供电，因为MPS电流过小导致PoE接口停止对外供电
处理建议	无需处理

128.6 POE_AI_FORCE_PoE

日志内容	Enabling forced power supply on PoE port [STRING]. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to **none**.
日志含义	AI PoE开启PoE接口强制供电功能来尝试恢复PoE供电，因为修改对PD支持标准的检测方式为**none**仍无法恢复PoE供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_FORCE_PoE: Enabling forced power supply on PoE port GigabitEthernet1/0/1. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to **none**.
对系统的影响	对系统无影响
日志产生原因	AI PoE开启PoE接口强制供电功能来尝试恢复PoE供电，因为修改对PD支持标准的检测方式为**none**仍无法恢复PoE供电
处理建议	无需处理

128.7 POE_AI_HIGH_INRUSH

日志内容	Increasing the inrush current threshold for PoE port [STRING]. Reason: The port has stopped power supply because of a high inrush current.
日志含义	AI PoE自动提高Inrush冲击电流阈值允许高冲击电流通过来尝试恢复PoE供电，因为Inrush冲击电流过大导致PoE接口停止对外供电
参数解释	无
日志等级	6 (Informational)
举例	POE/6/POE_AI_HIGH_INRUSH:Increasing the inrush current threshold for PoE port GigabitEthernet1/0/1. Reason: The port has stopped power supply because of a high inrush current.
对系统的影响	对系统无影响
日志产生原因	AI PoE自动提高Inrush冲击电流阈值允许高冲击电流通过来尝试恢复PoE供电，因为Inrush冲击电流过大导致PoE接口停止对外供电
处理建议	无需处理

128.8 POE_AI_LEGACY

日志内容	Enabling non-standard PD detection on PoE port [STRING]. Reason: The port cannot supply power to the PD.
日志含义	AI PoE自动开启接口的非标准PD检测功能来尝试恢复PoE供电，因为PoE接口不能给PD供电
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_LEGACY:Enabling non-standard PD detection on PoE port GigabitEthernet1/0/1. Reason: The port cannot supply power to the PD.
对系统的影响	对系统无影响
日志产生原因	AI PoE自动开启接口的非标准PD检测功能来尝试恢复PoE供电，因为PoE接口不能给PD供电
处理建议	无需处理

128.9 POE_AI_MAXPOWER

日志内容	Increasing the maximum power of PoE port [STRING] to [UINT32]. Reason: An instant power surge has caused overload self-protection of the port
日志含义	AI PoE自动提高PoE接口的最大供电功率来尝试恢复PoE供电，因为瞬间功率过大导致过载保护，PoE接口无法对外供电
参数解释	$1：PoE接口名称 $2：最大输出功率值
日志等级	6 (Informational)
举例	POE/6/POE_AI_MAXPOWER:Increasing the maximum power of PoE port GigabitEthernet1/0/1 to 2000. Reason: An instant power surge has caused overload self-protection of the port.
对系统的影响	对系统无影响
日志产生原因	AI PoE自动提高PoE接口的最大供电功率来尝试恢复PoE供电，因为瞬间功率过大导致过载保护，PoE接口无法对外供电
处理建议	无需处理

128.10 POE_AI_RESTART

日志内容	Re-enabling PoE on port [STRING]. Reason: The power consumption of the port is 0.
日志含义	AI PoE自动复位接口的PoE供电功能，因为PoE接口处于供电状态，但功率消耗为0
参数解释	$1：PoE接口名称
日志等级	6 (Informational)
举例	POE/6/POE_AI_RESTART:Re-enabling PoE on port GigabitEthernet1/0/1. Reason: The power consumption of the port is 0.
对系统的影响	对系统无影响
日志产生原因	AI PoE自动复位接口的PoE供电功能，因为PoE接口处于供电状态，但功率消耗为0
处理建议	无需处理

128.11 POE_TRACK_POWEROFF

日志内容	Shut off power to PoE port [STRING]. Reason: The associated track entry detects that the PD is unreachable.
日志含义	停止对PoE接口供电，因为关联的Track项检测到PD不可达
参数解释	$1：PoE接口名称
日志等级	5 (Notification)
举例	POE/5/POE_TRACK_POWEROFF: Shut off power to PoE port GigabitEthernet 1/0/1. Reason: The associated track entry detects that the PD is unreachable.
对系统的影响	对系统无影响
日志产生原因	关联的Track项检测到PD不可达
处理建议	**1.** 检查设备与 PD 之间的链路是否通畅 **2.** 检查 PD 是否运行正常 **3.** 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

128.12 POE_TRACK_UNREACHABLE

日志内容	The associated track entry detects that the PD connected to port [STRING] is unreachable.
日志含义	PoE接口关联的Track项检测到PD不可达
参数解释	$1：PoE接口名称
日志等级	5 (Notification)
举例	POE/5/POE_TRACK_UNREACHABLE: The associated track entry detects that the PD connected to port GigabitEthernet 1/0/1 is unreachable.
对系统的影响	对系统无影响
日志产生原因	PoE接口关联的Track项检测到PD不可达
处理建议	**1.** 检查设备与 PD 之间的链路是否通畅 **2.** 检查 PD 是否运行正常 **3.** 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

128.13 PSE_PORT_ON_OFF_CHANGE

日志内容	Trap <pethPsePortOnOffNotification>: PSE [UINT32], IfIndex [UINT32], Detection Status [INTEGER] [STRING]
日志含义	PoE接口的供电状态发生了改变
参数解释	$1：PSE的编号 $2：PoE接口的索引 $3：PoE接口的供电状态码 $4：PoE接口的供电状态，取值包括： • disabled：对应供电状态码 1，表示 PoE 接口的供电功能处于关闭状态 • searching：对应供电状态码 2，表示 PoE 接口正在查找 PD • deliveringPower：对应供电状态码 3，表示 PoE 接口正在供电 • fault：对应供电状态码 4，表示 PoE 接口供电故障，例如 PSE 功率不足，无法给 PD 供电 • test：对应供电状态码 5，表示 PoE 接口正在检测 PD 是否符合供电要求 • otherFault：对应供电状态码 6，表示 PoE 接口其它供电故障，例如 PD 存在过载、短路等情况，导致 PoE 无法供电
日志等级	1 (Alert)
举例	PoE/1/PSE_PORT_ON_OFF_CHANGE: Trap <pethPsePortOnOffNotification>: PSE 1, IfIndex 25, Detection Status 3(deliveringPower)
对系统的影响	对系统无影响
日志产生原因	当设备检测到PoE接口的供电状态发生改变时，系统生成该日志

处理建议	• 当PoE接口的供电状态为disabled，请根据需要在PoE接口视图下执行 **poe enable** 命令开启PoE接口的远程供电功能
	• 当 PoE 接口的供电状态为 searching、deliveringPower 和 test 时，无需处理
	• 当 PoE 接口的供电状态为 fault 和 otherFault 时，可参照以下步骤进行处理：
	  ○ 检查设备与 PD 之间的链路是否通畅
	  ○ 检查 PD 是否运行正常
	  ○ 执行 **display poe interface**，如果Remaining字段的取值小于“GardBand+PD额定功率”，请增加PSE
	• 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

129 PORTAL

本节介绍 PORTAL 模块输出的日志信息。

129.1 PORTAL_RULE_FAILED

日志内容	Failed to assign a portal rule. Reason=[STRING].
日志含义	Portal过滤规则下发失败
参数解释	$1：Portal过滤规则下发失败的原因
日志等级	4 (Warning)
举例	PORTAL/4/PORTAL_RULE_FAILED: Failed to assign a portal rule. Reason=Not enough resources.
对系统的影响	无法对用户报文进行正确控制
日志产生原因	Portal过滤规则下发失败，具体原因详见表129-1
处理建议	请根据过滤规则下发失败的原因选择相应的处理方式，详见表129-1

表129-1 规则下发失败原因列表

规则下发失败原因	说明	处理建议
Portal failed to assign a rule to the driver.	规则下发驱动失败	请收集配置文件、日志信息和告警信息，并联系技术支持
Input parameters in the rule are incorrect.	下发驱动的规则的参数有问题	请收集配置文件、日志信息和告警信息，并联系技术支持
The rule already exists.	驱动已经存在该条规则	请收集配置文件、日志信息和告警信息，并联系技术支持
The driver doesn't support rule assignment.	驱动不支持	请确认产品是否支持。如果支持，请收集配置文件、日志信息和告警信息，并联系技术支持
Not enough resources.	驱动资源不足	使用**display qos-acl resource**命令检查硬件资源使用情况 释放一部分硬件资源

130 PORTSEC

本节介绍端口安全模块输出的日志信息。

130.1 PORTSEC_ACL_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; ACL authorization failed because[STRING].
日志含义	下发ACL失败及其原因
参数解释	$1：接口名 $2：MAC地址 $3：下发ACL失败的原因，包括如下取值： o the specified ACL didn't exist.：下发的 ACL 不存在 o this type of ACL is not supported.：不支持此 ACL 类型 o hardware resources were insufficient.：硬件资源不足 o the specified ACL conflicted with other ACLs applied to the interface.：下发的 ACL 与接口上应用的其他 ACL 冲突 o the specified ACL didn't contain any rules.：下发的 ACL 中未包含规则 o unknown error.：未知原因
日志等级	4 (Warning)
举例	PORTSEC/4/PORTSEC_ACL_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; ACL authorization failed because the specified ACL didn't exist.
对系统的影响	无法通过ACL对上线用户访问网络资源实施过滤与控制操作
日志产生原因	参见本日志打印的失败原因
处理建议	1. 请根据打印的失败原因确保 ACL 相关配置正确，如确保设备支持该 ACL、ACL 已创建且配置了相关规则等 2. 如果因当前设备上业务繁忙导致硬件资源不足，则请用户等待一段时间或关闭部分非必要业务后重新进行认证授权 3. 如果问题仍无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

130.2 PORTSEC_CAR_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign CAR attributes to driver.
日志含义	下发CAR到驱动失败
参数解释	$1：接口名 $2：MAC地址
日志等级	5 (Notification)
举例	PORTSEC/5/PORTSEC_CAR_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign CAR attributes to driver.
对系统的影响	无法利用该CAR对数据流进行限速
日志产生原因	• 设备不支持 CAR 特性 • 硬件资源不足
处理建议	**1.** 请确认设备是否支持 CAR 特性。如果不支持，则请下发其它设备支持的授权属性；如果支持，则请执行步骤 2 **2.** 如果因当前设备上业务繁忙导致硬件资源不足，则请用户等待一段时间或关闭部分非必要业务后重新进行认证授权 **3.** 如果问题仍无法解决，则请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

130.3 PORTSEC_CREATEAC_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to create AC. Reason: [STRING].
日志含义	创建AC失败及其原因
参数解释	$1：接口名 $2：MAC地址 $3：创建AC失败的原因： ○ hardware resources were insufficient：硬件资源不足 ○ unknown error：未知原因
日志等级	3 (Error)
举例	PORTSEC/3/PORTSEC_CREATEAC_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to create AC. Reason: hardware resources were insufficient.
对系统的影响	用户无法访问该VSI内的资源
日志产生原因	• VSI 不存在 • 硬件资源不足导致 AC 创建失败
处理建议	1. 使用 **display l2vpn vsi**命令查询设备上是否已创建相应的VSI。如果不存在，请通过 **vsi**命令创建对应的VSI；如果存在，则请执行步骤 2 2. 如果因当前设备上业务繁忙导致硬件资源不足，则请用户等待一段时间或关闭部分非必要业务后重新进行认证授权，设备将自动创建 AC 与授权 VSI 关联 3. 如果问题仍未解决，则请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

130.4 PORTSEC_LEARNED_MACADDR

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; A new MAC address was learned.
日志含义	端口学习到新的安全MAC地址
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID
日志等级	6 (Informational)
举例	PORTSEC/6/PORTSEC_LEARNED_MACADDR:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444; A new MAC address was learned.
对系统的影响	对系统无影响
日志产生原因	端口上线了新用户
处理建议	无需处理

130.5 PORTSEC_NTK_NOT_EFFECTIVE

日志内容	The NeedToKnow feature is configured but is not effective on interface [STRING].
日志含义	NeedToKnow模式在接口上不生效，因为该接口不支持NeedToKnow模式
参数解释	$1：接口名
日志等级	3 (Error)
举例	PORTSEC/3/PORTSEC_NTK_NOT_EFFECTIVE: The NeedToKnow feature is configured but is not effective on interface Ethernet3/1/2.
对系统的影响	Need To Know功能不生效
日志产生原因	NeedToKnow模式在接口上不生效，因为该接口不支持NeedToKnow模式
处理建议	选择在接口上配置其它端口安全特性或关闭接口的端口安全特性配置其它安全功能

130.6 PORTSEC_PORTMODE_NOT_EFFECTIVE

日志内容	The port security mode is configured but is not effective on interface [STRING].
日志含义	端口安全模式在接口上不生效，因为该接口不支持这种端口安全模式
参数解释	$1：接口名
日志等级	3 (Error)
举例	PORTSEC/3/PORTSEC_PORTMODE_NOT_EFFECTIVE: The port security mode is configured but is not effective on interface Ethernet3/1/2.
对系统的影响	端口安全功能不生效
日志产生原因	在不支持端口安全模式的接口上配置了端口安全模式
处理建议	关闭接口的端口安全特性或切换成接口支持的端口安全模式

130.7 PORTSEC_PROFILE_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign a user profile to driver.
日志含义	下发User Profile到驱动失败
参数解释	$1：接口名 $2：MAC地址
日志等级	4 (Warning)
举例	PORTSEC/4/PORTSEC_PROFILE_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign a user profile to driver.
对系统的影响	无法通过User Profile对上线用户访问网络资源实施过滤与控制操作
日志产生原因	下发User Profile失败的常见原因包括： • 下发的 User Profile 不存在 • 设备不支持 User Profile • 硬件资源不足 • 未配置相应的 User Profile 策略
处理建议	1. 请确保 User Profile 相关配置正确，如确保设备支持 User Profile、User Profile 已创建且配置了相关策略等 2. 如果因当前设备上业务繁忙导致硬件资源不足，则请用户等待一段时间或关闭部分非必要业务后重新进行认证授权 3. 如果问题仍无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

130.8 PORTSEC_URL_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; URL authorization failed because [STRING].
日志含义	授权URL失败
参数解释	$1：接口名 $2：MAC地址 $3：下发URL失败的原因 ○ this operation was not supported：不支持授权 URL ○ hardware resources were insufficient：硬件资源不足 ○ parameters were invalid：参数错误 ○ an unknown error existed：其它错误
日志等级	4 (Warning)
举例	PORTSEC/4/PORTSEC_URL_FAILURE:-IfName=GigabitEthernet1/0/1-MACAddr=0010-8400-22b9; URL authorization failed because hardware resources were insufficient.
对系统的影响	用户无法重定向到该URL指定的页面
日志产生原因	参见本日志打印的失败原因
处理建议	**1.** 请确认设备是否支持重定向 URL 特性。如果不支持，则请下发其它设备支持的授权属性；如果支持，则请执行步骤 2 **2.** 请确认服务器和设备上 URL 相关参数配置正确。 **3.** 如果因当前设备上业务繁忙导致硬件资源不足，则请用户等待一段时间或关闭部分非必要业务后重新进行认证授权 **4.** 如果问题仍无法解决，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

130.9 PORTSEC_VIOLATION

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-IfStatus=[STRING]; Intrusion protection was triggered.
日志含义	入侵检测功能被触发
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：接口状态
日志等级	5 (Notification)
举例	PORTSEC/5/PORTSEC_VIOLATION:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-IfStatus=Up; Intrusion protection was triggered.
对系统的影响	当入侵检测日志输出过多时，系统有可能正在被非法报文攻击
日志产生原因	配置入侵检测功能后，端口收到非法报文（源MAC地址未被端口学习到的报文或未通过认证的报文）时，系统输出此日志
处理建议	1. 请确认 802.1X、MAC 地址认证以及安全 MAC 地址配置正确 2. 请在任意视图下分别执行 **display port-security**、**display port-security access-user**命令，查看当前端口在线用户数 是否达到配置的允许学习的最大安全MAC地址数 ： o 如果当前端口下在线用户数或学习的安全 MAC 地址数已达到最大值且最大值过小，则请重新调整在线用户数以及允许学习的安全 MAC 地址数的最大值 o 如果当前在线用户数以及安全 MAC 地址数未达到最大值且入侵检测告警偶发，则无需处理 3. 当入侵检测日志过多时，系统可能受到入侵攻击，请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

130.10 PORTSEC_VLANMACLIMIT

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; Maximum number of MAC addresses already reached in the VLAN.
日志含义	VLAN内同时接入的MAC地址数量已达到上限
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID
日志等级	5 (Notification)
举例	PORTSEC/5/PORTSEC_VLANMACLIMIT:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444; Maximum number of MAC addresses already reached in the VLAN.
对系统的影响	新MAC地址用户无法接入
日志产生原因	当VLAN内同时接入的MAC地址数量达到上限时，系统生成此日志
处理建议	1. 请在任意视图下分别执行 **display port-security**、**display port-security access-user**命令，查看当前端口在线用户数 是否达到允许学习的最大安全MAC地址数： o 如果当前端口下在线用户数已达到最大值且最大值过小，则请重新在接口视图下执行 **port-security max-mac-count**命令调整该VLAN内允许学习的安全MAC地址数的最大值 o 如果当前在线用户数以及安全 MAC 地址数未达到最大值，则请执行步骤 3 2. 当同一个接口不断生成本日志时，端口可能受到大量未知源报文攻击，则请执行步骤 3 3. 请收集告警信息、日志信息和配置信息，并联系技术支持工程师进行处理

131 PPP

本节介绍 PPP 模块输出的日志信息。

131.1 IPPOOL_ADDRESS_EXHAUSTED

日志内容	The address pool [STRING] was exhausted.
日志含义	PPP地址池中地址已耗尽
参数解释	$1：地址池名称
日志等级	5 (Notification)
举例	PPP/5/IPPOOL_ADDRESS_EXHAUSTED: The address pool aaa was exhausted.
对系统的影响	无法再通过该地址池为新上线用户分配地址
日志产生原因	当地址池里最后一个地址分配出去时，打印本信息
处理建议	向地址池里添加新地址

131.2 PPP_USER_LOGOFF

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User logged off.
日志含义	用户正常下线
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层Vlan $5：内层Vlan $6：MAC地址 $7：下线原因，取值请参见表131-1
日志等级	6 (Informational)
举例	PPP/6/PPP_USER_LOGOFF: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVlan=1000-InVlan=4000-MACAddr=0230-0103-5601-Reason=Use request; User logged off.
对系统的影响	无
日志产生原因	用户下线原因请见表131-1
处理建议	无需处理

表131-1 主要下线原因列表

下线原因	说明
User request	用户主动要求终止连接
Lost carrier	协议保活报文丢失。 一般指BAS下一级网络设备（含该设备）到用户设备间的故障。
Lost service	业务服务器（例如：L2TP）主动发起终止用户业务服务的报文
BAS error	由于BAS内部软件处理异常造成的用户掉线
BAS reboot	BAS异常重启前发送断线信息，以进行非管理性的重启
Admin reset	由于管理的需要，暂时中断用户的链接
BAS request	其它未规定的掉线原因
Session timeout	用户上线时间达到了规定值或者用户的流量达到了规定值
Server command	AAA服务器强制下线
Idle timeout	用户在规定时间内的流量没有达到设定值
Account update fail	计费更新失败
Port error	BAS主动检测到用户接入端口的错误
Admin reboot	在重启BAS前，发送断线信息

131.3 PPP_USER_LOGON_FAILED

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User got online failed.
日志含义	用户上线失败
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层Vlan $5：内层Vlan $6：MAC地址 $7：上线失败原因，取值请参见表131-2
日志等级	5 (Notification)
举例	PPP/5/PPP_USER_LOGON_FAILED: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVlan=1000-InVlan=4000-MACAddr=0230-0103-5601-Reason=Authentication failed; User got online failed.
对系统的影响	用户上线失败
日志产生原因	用户上线失败原因请见表131-2
处理建议	• 检查用户名和密码是否正确 • 检查认证和计费服务器是否工作正常 • 检查设备上地址池是否配置正确

表131-2 主要上线失败原因列表

上线失败原因	说明
Authentication failed	认证失败
Authorization failed	授权失败
Assign IP failed	分配IP失败
Accounting failed	计费失败

131.4 PPP_USER_LOGON_SUCCESS

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]; User got online successfully.
日志含义	用户上线成功
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层Vlan $5：内层Vlan $6：MAC地址
日志等级	6 (Informational)
举例	PPP/6/PPP_USER_LOGON_SUCCESS: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVlan=1000-InVlan=4000-MACAddr=0230-0103-5601; User got online successfully.
对系统的影响	无
日志产生原因	用户上线成功
处理建议	无需处理

132 PTP

本节介绍 PTP 模块输出的日志信息。

132.1 PTP_MASTER_CLOCK_CHANGE

日志内容	PTP master clock property changed. (OldMasterClockId=[STRING], CurrentMasterClockId=[STRING], NewSourceIfIndex=[UINT16], OldSourcePortNum=[UINT16], CurrentSourcePortNum=[UINT16], OldSourcePortName=[STRING], CurrentSourcePortName=[STRING])
日志含义	时钟源发生切换
参数解释	$1：原来主时钟ID $2：当前主时钟ID $3：新的时钟源索引 $4：曾为本设备提供时钟源的接口编号 $5：当前为本设备提供时钟源的接口编号 $6：曾为本设备提供时钟源的接口名称 $7：当前为本设备提供时钟源的接口名称
日志等级	4 (Warning)
举例	PTP/4/PTP_MASTER_CLOCK_CHANGE: PTP master clock property changed. (OldMasterClockId=000FE2-FFFE-FF0000, CurrentMasterClockId=000FE2-FFFE-FF0001, NewSourceIfIndex=3, OldSourcePortNum=2, CurrentSourcePortNum=1, OldSourcePortName=GigabitEthernet1/0/2, CurrentSourcePortName=GigabitEthernet1/0/1)
对系统的影响	对系统无影响
日志产生原因	主时钟源属性发生改变，原因包括： • PTP 域内的时钟设备属性发生变化，导致出现了优先级更高的时钟源或获取时钟源的路径发生了改变 • 接入了优先级更高的时钟源 • 接收时钟源信号的 PTP 接口所在链路故障或者 PTP 接口 DOWN
处理建议	正常运行信息，无需处理 也可以继续定位原PTP接口是否故障导致时钟源切换。执行**display ptp interface**命令查看是否存在PTP接口处于Disabled状态。若存在接口处于Disabled状态，则表示PTP接口故障，请先处理接口故障

132.2 PTP_MEAN_PATH_DELAY_ABNORMAL

日志内容	In PTP instance [UINT16], PTP mean path delay is abnormal. (Delay-mechanism=[UINT64], MeanPathDelay=[UINT64] ns, MeanPathDelayThreshold=[UINT64] ns)
日志含义	PTP接口与对端PTP接口之间的平均路径延时超过平均路径延时的域值
参数解释	$1：PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准） $2：设备的延时测量机制，取值为： o **e2e**：表示请求应答机制。 o **p2p**：表示端延时机制 $3：平均路径延时，单位为ns $4：平均路径延时的域值，单位为ns
日志等级	5 (Notification)
举例	PTP/5/PTP_MEAN_PATH_DELAY_ABNORMAL: In PTP instance 1, PTP mean path delay is abnormal. (Delay-mechanism=e2e, MeanPathDelay=70000 ns, MeanPathDelayThreshold=7000 ns)
对系统的影响	对系统无影响
日志产生原因	PTP接口与对端PTP接口之间的平均路径延时超过平均路径延时的域值时，生成该日志
处理建议	PTP时间同步链路平均路径延时增大，PTP时间同步会正常进行，建议您根据原因进行相应的处理： • 如果因为组网环境变动，导致网络延时增加，请检查网络 • 网络时延未出现波动，请收集告警、日志和配置信息，联系技术支持

132.3 PTP_PKTLOST

日志内容	PTP packets were lost. (PktType=[STRING])
日志含义	PTP协议报文丢失
参数解释	$1：PTP报文类型，取值包括： o Delay_Resp：PTP Delay_Resp 报文 o Announce：PTP Announce 报文 o Sync：PTP Sync 报文 o Pdelay_Resp：PTP Pdelay_Resp 报文
日志等级	4 (Warning)
举例	PTP/4/PTP_PKTLOST: PTP packets were lost. (PktType=Announce)
对系统的影响	偶尔丢包不影响时间同步，如果长时间持续丢包会影响时钟同步
日志产生原因	Slave端口检测Announce、Delay_Resp、Sync报文，超过检测时间没有收到报文，则认为报文丢失
处理建议	在打印该日志的PTP从时钟设备上使用**display ptp statistics**命令查看接收报文统计计数是否增长 • 若增长，则表示链路延时过长导致的超时，无须处理 • 若不增长，则在PTP主时钟设备使用 **display ptp statistics**命令查看发送报文统计计数是否增长 o 若增长，则表示链路故障导致对端超时没收到报文，排除故障恢复链路 o 若不增长，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

132.4 PTP_PKTLOST_RECOVER

日志内容	PTP packets lost were recovered. (PktType=[STRING])
日志含义	PTP协议报文丢失问题恢复
参数解释	$1：PTP报文类型，取值包括： ○ Delay_Resp：PTP Delay_Resp 报文 ○ Announce：PTP Announce 报文 ○ Sync：PTP Sync 报文 ○ Pdelay_Resp：PTP Pdelay_Resp 报文
日志等级	4 (Warning)
举例	PTP/4/PTP_PKTLOST_RECOVER: PTP packets lost were recovered. (PktType =Announce)
对系统的影响	对系统无影响
日志产生原因	从PTP报文丢失告警状态中恢复正常。只有当Slave端口检测Announce、Delay_Resp、Sync报文超时后又重新收到Announce、Delay_Resp报文或者超时时间过长设备自身由从时钟转变为主时钟时，才会打印此日志
处理建议	无需处理

132.5 PTP_PORT_BMCINFO_CHANGE

日志内容	The BMC info for port [UINT16] changed. (PortName=[STRING], PortSourceId=[STRING], PortSourcePortNum=[UINT16], PortSourceStepsRemoved=[UINT16], CurrentMasterClockId=[STRING])
日志含义	PTP端口收到的报文中的BMC信息发生变化
参数解释	$1：PTP接口索引 $2：PTP接口名称 $3：PTP接口接收到的时钟源ID $4：PTP接口接收到的时钟源端口号 $5：PTP接口接收到的时钟源跳数 $6：设备当前主时钟ID
日志等级	5 (Notification)
举例	PTP/5/PTP_PORT_BMCINFO_CHANGE: The BMC info for port 1 changed. (PortName=GigabitEthernet1/0/1, PortSourceId=000FE2-FFFE-FF0001, PortSourcePortNum=1, PortSourceStepsRemoved=5, CurrentMasterClockId=000FE2-FFFE-FF0000)
对系统的影响	可能会导致时钟源变更
日志产生原因	PTP接口收到的时钟源ID、时钟源端口号或时钟源跳数等时钟源信息发生变化
处理建议	无需处理

132.6 PTP_PORT_STATE_CHANGE

日志内容	PTP port state changed. (IfIndex=[UINT16], PortName=[STRING], PortState=[STRING], OldPortState=[STRING])
日志含义	PTP端口状态发生变化
参数解释	$1：PTP接口索引 $2：PTP接口名称 $3：PTP接口当前的状态，取值包括： o Master：接口状态为 Master，对外发布时间信息 o Slave：接口状态为 Slave，跟踪外部时间信息 o Passive：接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息 o Listening：接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息 o Faulty：接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文 o Initializing：接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文 o Premaster：接口状态为 Premaster，Master 状态前的临时状态 o Disable：接口状态为Disabled，接口上PTP 协议未运行，接口不处理协议报文 o Uncalibrated：接口状态为 Uncalibrated，Slave 状态前的临时状态 $4：PTP接口变化前的状态，取值包括： o Master：接口状态为 Master，对外发布时间信息 o Slave：接口状态为 Slave，跟踪外部时间信息 o Passive：接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息 o Listening：接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息 o Faulty：接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文 o Initializing：接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文 o Premaster：接口状态为 Premaster，Master 状态前的临时状态 o Disable：接口状态为Disabled，接口上PTP 协议未运行，接口不处理协议报文 o Uncalibrated：接口状态为 Uncalibrated，Slave 状态前的临时状态
日志等级	5 (Notification)
举例	PTP/5/PTP_PORT_STATE_CHANGE: PTP port state changed. (IfIndex=2, PortName=GigabitEtherne1/0/1, PortState=Slave, OldPortState=Master)
对系统的影响	对系统无影响
日志产生原因	PTP接口状态发生改变，原因包括： • PTP 域内的时钟设备属性发生变化，比如优先级、时钟等级、时钟精度、接口的 NotSlave 属性等 • 接入了优先级更高的时钟源 • PTP 接口所在链路故障或者 PTP 接口 DOWN

处理建议	Faulty和Disable状态需要关注，其它状态为短暂的中间状态，无需处理 • 接口收到的 PdelayResp 报文个数和 PdelayRespFollowUp 报文个数不等，会导致接口处于 Faulty 状态。可采取以下处理措施： a. 请在对端执行 **display ptp statistics**命令，查看Sent packets中PdelayResp和PdelayRespFollowUp字段的取值。如果这两个取值不等，对端PTP功能异常，可在接口视图下关闭后再开启PTP功能尝试恢复 b. 请在本端执行 **display ptp statistics**命令，查看Received packets中PdelayResp和PdelayRespFollowUp字段的取值。如果这两个取值和对端Sent packets中PdelayResp和PdelayRespFollowUp字段的取值不等，请定位网络丢包问题 c. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 • 接口未收到 Announce 报文，会导致接口处于 Disable 状态。可采取以下处理措施： d. 请根据对端 **ptp announce-interval**命令的配置计算指定时间段对端应该发送的Announce报文的个数，并在对端执行 **display ptp statistics**命令且查看Sent packets中Announce字段的取值。如果这两个值不等，请定位对端未发送Announce报文问题 e. 在本端执行 **display ptp statistics**命令且查看Received packets中Announce字段的取值。如果该取值和对端Sent packets中Announce字段的取值不等，请定位Announce报文网络丢包问题 f. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

132.7 PTP_SRC_CHANGE

日志内容	Clock source property changed. (SourceName=[STRING], Priority1=[UCHAR], Priority2=[UCHAR], ClockClass=[UINT16], ClockAccuracy=[UINT16]], ClockSourceType=[STRING])
日志含义	时钟源属性发生改变
参数解释	$1：时钟源，取值包括：（设备支持的时钟源类型与设备型号有关，请以设备实际情况为准） o Local：本地时钟 o Tod0：第一路 ToD 时钟 o Tod1：第二路 ToD 时钟 $2：第一优先级 $3：第二优先级 $4：时钟源的时间等级 $5：时钟源的时间精度 $6：最优时钟的时钟类别，取值包括： o Atomic clock：原子时钟 o GPS：Global Positioning System，全球定位系统 o Handset：手持设备 o Internal oscillator：内部震荡器 o NTP：Network Time Protocol，网络时间协议 o Other：其他 o PTP：Precision Time Protocol，精确时间协议 o Terrestrial radio：陆基无线电 o Unknown：未知
日志等级	5 (Notification)
举例	PTP/5/PTP_SRC_CHANGE: Clock source property changed.(SourceName=LOCAL,Priority1=128,Priority2=128,ClockClass=248,ClockAccuracy=254,ClockSourceType=(Internal oscillator)).
对系统的影响	对系统无影响
日志产生原因	时钟源属性发生改变，原因包括： • 用户通过命令行改变时钟源属性 • 接收到了精度更高的外接时钟源
处理建议	无需处理

132.8 PTP_SRC_SWITCH

日志内容	Clock source switched. (LastClockID=[STRING], CurrentClockID=[STRING])
日志含义	系统时钟源变更
参数解释	$1：原来的时钟源ID $2：当前的时钟源ID
日志等级	4 (Warning)
举例	PTP/4/PTP_SRC_SWITCH: Clock source switched.(LastClockID=4CBD4E-FFFE-C00100,CurrentClockID=AA479F-FFFE-EE0200).
对系统的影响	对系统无影响
日志产生原因	新的更好的时钟源加入PTP域，设备跟踪的时钟源发生切换
处理建议	无需处理

132.9 PTP_SYNC_RESUME

日志内容	In PTP instance [UINT16], PTP time synchronization resumed because the PTP time offset between the instance and the master fell below the threshold or the maximum suppression counts were reached. (TimeOffset=[INT64] ns, TimeOffsetThreshold=[UINT64] ns, SuppressionCounts=[UINT16])
日志含义	PTP实例的当前PTP时间和Master提供的最新PTP时间之间的偏差小于等于设备允许的最大偏差，或者PTP抑制时间同步的次数达到阈值，PTP时间同步抑制解除
参数解释	$1：PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准） $2：当前PTP时间和Master提供的最新PTP时间之间的偏差，单位为ns $3：设备允许的、当前PTP时间和Master提供的最新PTP时间之间的最大偏差，单位为ns $4：PTP连续抑制时间同步的次数
日志等级	4 (Warning)
举例	PTP/4/PTP_SYNC_RESUME: In PTP instance 1, PTP time synchronization resumed because the PTP time offset between the instance and the master fell below the threshold or the maximum suppression counts were reached. (TimeOffset=50 ns, TimeOffsetThreshold=3000 ns, SuppressionCounts=3)
对系统的影响	对系统无影响
日志产生原因	PTP实例的当前PTP时间和Master提供的最新PTP时间之间的偏差小于等于设备允许的最大偏差，或者PTP抑制时间同步的次数达到阈值，PTP时间同步抑制解除
处理建议	无需处理

132.10 PTP_SYNC_SUPPRESS

日志内容	In PTP instance [UINT16], PTP time synchronization was suppressed because the PTP time offset between the instance and the master exceeded the threshold. (TimeOffset=[INT64] ns, TimeOffsetThreshold=[UINT64] ns)
日志含义	PTP实例的当前PTP时间和Master提供的最新PTP时间之间的偏差大于设备允许的最大偏差，设备认为最新的PTP时间信号不可靠，抑制时间同步，即不进行PTP时间同步
参数解释	$1：PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准） $2：当前PTP时间和Master提供的最新PTP时间之间的偏差，单位为ns $3：设备允许的、当前PTP时间和Master提供的最新PTP时间之间的最大偏差，单位为ns
日志等级	4 (Warning)
举例	PTP/4/PTP_SYNC_SUPPRESS: In PTP instance 1, PTP time synchronization was suppressed because the PTP time offset between the instance and the master exceeded the threshold. (TimeOffset=5000 ns, TimeOffsetThreshold=3000 ns)
对系统的影响	可能会影响PTP时间的精度
日志产生原因	PTP实例的当前PTP时间和Master提供的最新PTP时间之间的偏差大于设备允许的最大偏差，设备认为最新的PTP时间信号不可靠，抑制时间同步，即不进行PTP时间同步
处理建议	请收集告警、日志和配置信息，联系技术支持

132.11 PTP_TIME_LOCK

日志内容	Time resumed to locked state.
日志含义	系统时间恢复到锁定状态
参数解释	无
日志等级	3 (Error)
举例	PTP/3/PTP_TIME_LOCK: Time resumed to locked state.
对系统的影响	对系统无影响
日志产生原因	时钟从失锁状态中恢复为正常
处理建议	无需处理

132.12 PTP_TIME_NOT_LOCK

日志内容	Time not in locked state.
日志含义	时钟失锁
参数解释	无
日志等级	3 (Error)
举例	PTP/3/PTP_TIME_NOT_LOCK: Time not in locked state.
对系统的影响	会影响本地时钟的精度
日志产生原因	时钟失锁告警，原因包括： • 当PTP时钟源的时间偏移大于 *unlock-value*时，PTP时间为失锁状态，触发时钟失锁日志 • 子卡逻辑或者时钟扣板硬件故障 • DSP 收到的时间戳不变或者时戳错误
处理建议	1. 执行 **display interfcae**命令检查PTP Slave接口是否链路故障或接口down。若链路故障或接口down，排除故障恢复链路 2. 通过 iNQA 和 iFIT 等功能测量网络时延，确认是否因为网络时延增加，导致时钟源提供的时钟偏差过大。如果是，请先解决网络时延过大问题 3. 执行 **display current-configuration | include "time-unlock"**命令查看PTP时间失锁阈值配置是否合理，如果不合理，可通过 **ptp alarm-threshold time-unlock unlock-value**命令修改

133 PTS

本节介绍 PTS（Platform Trust Services，平台可信服务）模块输出的日志信息。

133.1 PTS_AK_AUTH_FAILED

日志内容	Inconsistent authorization data for attestation key [STRING].
日志含义	AK密钥对应的授权数据不一致
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_AK_AUTH_FAILED: Inconsistent authorization data for attestation key abc.
对系统的影响	对应AK密钥无法使用
日志产生原因	AK密钥对应的授权数据错误
处理建议	配置可信报告使用的AK密钥时使用的授权数据需要和创建该密钥时配置的授权数据一致（相关命令为**key create**）

133.2 PTS_AK_INVALID

日志内容	The attestation key [STRING] is incorrect.
日志含义	AK密钥不正确
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_AK_INVALID: The attestation key abc is incorrect.
对系统的影响	对应AK密钥无法使用
日志产生原因	AK密钥无效
处理建议	重新配置可信报告使用的AK密钥

133.3 PTS_AK_NO_CERT

日志内容	No certificate file found for attestation key [STRING].
日志含义	AK密钥未找到证书
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_AK_NO_CERT: No certificate file found for attestation key abc.
对系统的影响	对应AK密钥无法使用
日志产生原因	AK密钥缺少证书
处理建议	通过管理端为设备的AK密钥签发AK证书

133.4 PTS_AK_NO_EXIST

日志内容	Attestation key [STRING] doesn't exist.
日志含义	指定名称的AK密钥不存在
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_AK_NO_EXIST: Attestation key abc doesn't exist.
对系统的影响	对应AK密钥无法使用
日志产生原因	指定名称的AK密钥不存在
处理建议	配置AK密钥（相关命令为**`key create`**）

133.5 PTS_AK_NO_LOAD

日志内容	The attestation key [STRING] is not loaded.
日志含义	AK密钥未加载
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_AK_NO_LOAD: The attestation key abc is not loaded.
对系统的影响	对应AK密钥无法使用
日志产生原因	AK密钥未加载到安全芯片
处理建议	通过**key load**命令将AK密钥加载到可信计算芯片

133.6 PTS_BTW_PCR_FAILED

日志内容	Hash value computed based on BootWare IML is not consistent with that in PCR ([UINT]).
日志含义	使用BootWare可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同
参数解释	$1：PCR的索引
日志等级	4 (Warning)
举例	PTS/4/PTS_BTW_PCR_FAILED: Hash value computed based on BootWare IML is not consistent with that in PCR(0).
对系统的影响	BootWare程序不可信
日志产生原因	使用BootWare可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.7 PTS_CHECK_RM_VERSION_FAILED

日志内容	Version the RM file [STRING] is not supported.
日志含义	RM文件版本不支持
参数解释	$1：RM文件名称
日志等级	4 (Warning)
举例	PTS/4/PTS_CHECK_RM_VERSION_FAILED: Version the RM file BOOTWARE_BASIC_52B.rm is not supported.
对系统的影响	可信状态变为不可信
日志产生原因	设备不支持当前RM文件版本
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.8 PTS_CREATE_AGED_TIMER_FAILED

日志内容	Failed to create PTS session ageing timer.
日志含义	创建PTS会话老化定时器失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_CREATE_AGED_TIMER_FAILED: Failed to create PTS session ageing timer.
对系统的影响	PTS服务无法正常使用
日志产生原因	创建PTS会话老化定时器失败
处理建议	• 依次执行 **undo pts**和 **pts**命令重启PTS服务 • 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.9 PTS_CREATE_CHECK_TIMER_FAILED

日志内容	Failed to create server check timer.
日志含义	创建Server检查定时器失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_CREATE_CHECK_TIMER_FAILED: Failed to create server check timer.
对系统的影响	PTS服务无法正常使用
日志产生原因	创建Server检查定时器失败
处理建议	• 依次执行 **undo pts**和 **pts**命令重启PTS服务 • 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.10 PTS_CREATE_CONTEXT_FAILED

日志内容	Failed to create TSS context.
日志含义	TSS上下文创建失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_CREATE_CONTEXT_FAILED: Failed to create TSS context.
对系统的影响	可信计算功能无法使用
日志产生原因	TSS（TPM Software Stack，TPM芯片软件栈）上下文初始化失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.11 PTS_CREATE_EPOLL_FAILED

日志内容	Failed to create epoll service.
日志含义	epoll服务创建失败
参数解释	无
日志等级	3 (Error)
举例	PTS/3/PTS_CREATE_EPOLL_FAILED: Failed to create epoll service.
对系统的影响	PTS服务无法正常使用
日志产生原因	PTS模块创建epoll（I/O event notification facility）服务失败
处理建议	1. 依次执行 **undo pts**和 **pts**命令重启PTS服务 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.12 PTS_CREATE_HASH_FAILED

日志内容	Failed to create hash table.
日志含义	HASH表创建失败
参数解释	无
日志等级	3 (Error)
举例	PTS/3/PTS_CREATE_HASH_FAILED: Failed to create hash table.
对系统的影响	PTS服务无法正常使用
日志产生原因	PTS模块创建HASH表失败
处理建议	1. 依次执行 **undo pts**和 **pts**命令重启PTS服务 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.13 PTS_CREATE_SELFVERIFY_COUNTER_FAILED

日志内容	Failed to create selfverify counter.
日志含义	自检计数器创建失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_CREATE_SELFVERIFY_COUNTER_FAILED: Failed to create selfverify counter.
对系统的影响	PTS服务无法正常使用
日志产生原因	可信自检的IML计数器创建失败
处理建议	1. 依次执行 **undo pts**和 **pts**命令重启PTS服务 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.14 PTS_CREATE_SELFVERIFY_TIMER_FAILED

日志内容	Failed to create selfverify timer.
日志含义	自检定时器创建失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_CREATE_SELFVERIFY_TIMER_FAILED: Failed to create selfverify timer.
对系统的影响	PTS定期自检服务无法正常使用
日志产生原因	周期可信自检的定时器创建失败
处理建议	• 可以通过 **integrity selfverify**命令手动执行可信自检 • 可以收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.15 PTS_CREATE_SOCKET_FAILED

日志内容	Failed to create socket service.
日志含义	socket服务创建失败
参数解释	无
日志等级	3 (Error)
举例	PTS/3/PTS_CREATE_SOCKET_FAILED: Failed to create socket service.
对系统的影响	PTS服务无法正常使用
日志产生原因	PTS模块创建socket服务失败
处理建议	1. 依次执行 **undo pts**和 **pts**命令重启PTS服务 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.16 PTS_CREATE_TIMER_FAILED

日志内容	Failed to create timer.
日志含义	定时器创建失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_CREATE_TIMER_FAILED: Failed to create timer.
对系统的影响	PTS服务无法正常使用
日志产生原因	创建定时器失败 当PTS模块的任一定时器创建失败时，都会产生本日志
处理建议	1. 依次执行 **undo pts**和 **pts**命令重启PTS服务 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.17 PTS_FILE_HASH_FAILED

日志内容	Hash value of file [STRING] is not consistent with that in the RM file.
日志含义	目标文件的HASH值与RM文件中该文件的HASH值不一致
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	PTS/4/PTS_FILE_HASH_FAILED: Hash value of file /sbin/ls is not consistent with that in the RM file.
对系统的影响	该文件不可信
日志产生原因	目标文件的HASH值与RM文件中该文件的HASH值不匹配
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.18 PTS_LOAD_KEY_FAILED

日志内容	Failed to load attestation key [STRING].
日志含义	加载AK密钥失败
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_LOAD_KEY_FAILED: Failed to load attestation key abc.
对系统的影响	加载密钥无法正常使用
日志产生原因	向TPM芯片加载AK密钥失败
处理建议	1. 检查指定名称的AK密钥是否存在且处于使能状态（相关显示命令为 **display tcsm key name**） 2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.19 PTS_PARSE_IML_FAILED

日志内容	Failed to parse IML.
日志含义	IML解析失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_PARSE_IML_FAILED: Failed to parse IML.
对系统的影响	PTS服务无法正常使用
日志产生原因	可信度量日志解析失败
处理建议	1. 依次执行 **undo pts**和 **pts**命令重启PTS服务 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.20 PTS_PKG_PCR_FAILED

日志内容	Hash value computed based on Package IML is not consistent with that in PCR ([UINT]).
日志含义	使用软件包IML计算出来的HASH值与PCR中的HASH值不同
参数解释	$1：PCR的索引
日志等级	4 (Warning)
举例	PTS/4/PTS_PKG_PCR_FAILED: Hash value computed based on Package IML is not consistent with that in PCR (12).
对系统的影响	Comware软件包不可信
日志产生原因	使用Comware软件包的可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.21 PTS_READ_PCR_FAILED

日志内容	Failed to read PCR ([UINT]).
日志含义	PCR数据读取失败
参数解释	$1：TPM芯片的PCR索引
日志等级	4 (Warning)
举例	PTS/4/PTS_READ_PCR_FAILED: Failed to read PCR(0).
对系统的影响	PTS服务无法正常使用
日志产生原因	PCR数据读取失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.22 PTS_RM_FILE_FAILED

日志内容	Wrong signature for RM file [STRING].
日志含义	RM文件签名错误
参数解释	$1：RM文件名称
日志等级	4 (Warning)
举例	PTS/4/PTS_RM_FILE_FAILED: Wrong signature for RM file BOOTWARE_BASIC_52B.rm.
对系统的影响	可信计算度量功能无法正常使用
日志产生原因	RM文件签名错误
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.23 PTS_RUNTIME_PCR_FAILED

日志内容	Hash value computed based on runtime IML is not consistent with that in PCR ([UINT]).
日志含义	使用Runtime的IML计算出来的HASH值与PCR中的HASH值不同
参数解释	$1：PCR的索引
日志等级	4 (Warning)
举例	PTS/4/PTS_RUNTIME_PCR_FAILED: Hash value computed based on runtime IML is not consistent with that in PCR (10).
对系统的影响	Comware运行过程中度量的可执行文件不可信
日志产生原因	使用Runtime（运行的软件进程）相关的可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.24 PTS_SELFVERIFY_FAILED

日志内容	Failed to start integrity selfverify. Reason: TPM doesn't exist or isn't enabled.
日志含义	由于TPM芯片不存在或者被禁用，可信自检启动失败
参数解释	$1：AK密钥的名称
日志等级	4 (Warning)
举例	PTS/4/PTS_SELFVERIFY_FAILED: Failed to start integrity selfverify. Reason: TPM doesn't exist or isn't enabled.
对系统的影响	PTS服务无法正常使用
日志产生原因	TPM芯片不存在或者被禁用
处理建议	查看设备的可信计算芯片信息（相关显示命令为**display tcsm trusted-computing-chip**），确保TPM芯片可用

133.25 PTS_SELFVERIFY_START_FAILED

日志内容	Failed to start selfverify.
日志含义	启动可信自检失败
参数解释	无
日志等级	4 (Warning)
举例	PTS/4/PTS_SELFVERIFY_START_FAILED: Failed to start selfverify.
对系统的影响	PTS服务无法正常使用
日志产生原因	启动可信自检失败
处理建议	1. 尝试重新启动可信自检 2. 如果问题仍然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

133.26 PTS_TEMPLATE_HASH_FAILED

日志内容	Calculated template hash value of [STRING] is not consistent with that in IML.
日志含义	目标文件的模板HASH值与IML中的模板HASH值不同
参数解释	$1：可信度量的目标文件名称
日志等级	4 (Warning)
举例	PTS/4/PTS_TEMPLATE_HASH_FAILED: Calculated template hash value of /sbin/ls is not consistent with that in IML.
对系统的影响	目标文件不可信
日志产生原因	根据目标文件的HASH值和日志度量时间等参数计算的模板HASH值与可信度量日志中的模板HASH值不同，此时该可信度量日志内容可能被篡改
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

134 PWDCTL

本节介绍 Password control 模块输出的日志信息。

134.1 PWDCTL_ADD_BLACKLIST

日志内容	User [STRING] from [STRING] was added to the blacklist for failed login attempts.
日志含义	用户尝试登录设备失败，被加入密码控制黑名单
参数解释	$1：用户名 $2：用户IP地址
日志等级	6 (Informational)
举例	PWDCTL/6/PWDCTL_ADD_BLACKLIST: User hhh from 1.1.1.1 was added to the blacklist for failed login attempts.
对系统的影响	用户被加入黑名单但不会被锁定，当输入密码错误达到登录最大尝试次数时，用户账号将被锁定
日志产生原因	• 用户输入密码错误 • 用户接入类型不匹配 • 用户未激活
处理建议	1. 请使用正确的密码登录设备。如果密码正确，用户仍登录失败则请执行步骤 2 2. 请检查设备密码管理及用户服务类型等相关配置正确。如果配置正确，则请执行步骤 3 3. 请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.2 PWDCTL_CHANGE_PASSWORD

日志内容	[STRING] changed the password because [STRING].
日志含义	出于某种原因，用户修改了密码
参数解释	$1：用户名 $2：更改密码原因 o it was the first login of the account：用户首次登录 o the password had expired：密码已经过期 o the password was too short：密码长度过短 o the password was not complex enough：密码复杂度不满足要求 o the password was default password：密码是缺省密码
日志等级	6 (Informational)
举例	PWDCTL/6/PWDCTL_CHANGE_PASSWORD: hhh changed the password because It was the first login of the account.
对系统的影响	对系统无影响
日志产生原因	出现以下任一情况时，用户需要修改密码，成功修改密码后，系统输出此日志信息： • 首次登录修改密码功能处于开启状态时，用户首次登录 • 用户密码的使用时间超过密码老化时间 • 用户密码长度低于系统配置的密码最小长度 • 用户密码不符合密码复杂度检查策略 • 通过 Telnet、SSH、HTTP、HTTPS 方式登录的设备管理类用户，使用缺省密码登录时必须修改密码
处理建议	用户修改密码后，请用户重新登录时使用修改后的新密码登录设备

134.3 PWDCTL_FAILED_COPYFILE

日志内容	Failed to copy the password records to all backup files.
日志含义	设备无法将密码记录拷贝到备用主控板的记录文件
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_FAILED_COPYFILE: Failed to copy the password records to all backup files.
对系统的影响	用户的密码记录备份失败
日志产生原因	设备无法将密码记录拷贝到备用主控板的记录文件
处理建议	请先在用户视图下执行**cd**命令切换到备用主控板工作路径，再执行**dir**命令查看当前备用主控板的剩余存储空间大小： • 若剩余存储空间过小，则请删除非必要文件释放部分空间 • 若剩余存储空间充足，则请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.4 PWDCTL_FAILED_PROCMSG

日志内容	Failed to process request message.
日志含义	LAUTHD进程处理请求消息失败
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_FAILED_PROCMSG: Failed to process request message.
对系统的影响	用户无法登录设备
日志产生原因	内部进程错误
处理建议	请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.5 PWDCTL_FAILED_TO_WRITEPWD

日志内容	Failed to write the password records to file.
日志含义	设备无法将用户密码写入密码记录文件
参数解释	无
日志等级	6 (Informational)
举例	PWDCTL/6/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.
对系统的影响	用户无法登录设备
日志产生原因	系统存储空间不足
处理建议	请在用户视图下执行**dir**命令查看系统当前剩余存储空间大小： • 若剩余存储空间过小，则请删除非必要文件释放部分空间 • 若剩余存储空间充足，则请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.6 PWDCTL_FAILED_TO_OPENFILE

日志内容	Failed to open the password file.
日志含义	创建或打开*.dat文件失败
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_FAILED_TO_OPENFILE: Failed to open the password file.
对系统的影响	密码管理功能不可用
日志产生原因	• 系统存储空间不足 • 系统运行内存不足
处理建议	1. 请在用户视图下执行 **dir**命令查看系统当前剩余存储空间大小，若剩余存储空间过小，请删除非必要文件释放部分空间；若剩余存储空间充足，则执行步骤 2 2. 释放内存资源。例如，执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源 3. 执行 **display memory**命令查看内存使用情况： o 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，且该进程非必要运行，可以开启或者关闭进程对应的软件功能，来释放内存 o 如果内存占用率恢复到告警阈值以下，内存告警解除，密码管理功能会继续生效 4. 如果问题仍未解决，请收集配置文件、日志信息和告警信息，并联系技术支持工程师

134.7 PWDCTL_NOENOUGHSPACE

日志内容	Not enough free space on the storage media where the file is located.
日志含义	*.dat文件所在介质（Flash或CF卡等）存储空间不足
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_NOENOUGHSPACE: Not enough free space on the storage media where the file is located.
对系统的影响	密码管理功能配置失败
日志产生原因	*.dat文件所在介质（Flash或CF卡等）存储空间不足
处理建议	请在用户视图下执行**dir**命令查看系统当前剩余存储空间大小： • 若剩余存储空间过小，则请删除非必要文件释放部分空间 • 若剩余存储空间充足，则请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.8 PWDCTL_NOTFOUNDUSER

日志内容	Can't find the username in the file.
日志含义	在*.dat文件中获取不到用户信息
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_NOTFOUNDUSER: Can't find the username in the file.
对系统的影响	本地用户密码设置失败，该用户无法登录设备
日志产生原因	• LAUTHD 进程异常 • 本地用户设置异常
处理建议	**1.** 请关闭 Password Control 功能后再重新开启 Password Control 功能。若未解决问题，则请执行步骤 2 **2.** 请重新创建一个本地用户，若未解决问题，则请执行步骤 3 **3.** 请收集配置文件、日志信息和告警信息，并联系技术支持工程师

134.9 PWDCTL_NOTIFYWRITEFILE

日志内容	Notification of writing password records to file failed.
日志含义	将用户密码写入密码记录文件的通知下发失败
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_NOTIFYWRITEFILE: Notification of writing password records to file failed.
对系统的影响	用户密码无法写入密码记录文件，用户无法登录设备
日志产生原因	内部进程错误
处理建议	请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.10 PWDCTL_RECFORMATCONV

日志内容	Failed to convert the password record format.
日志含义	用户密码记录格式转换失败
参数解释	无
日志等级	3 (Error)
举例	PWDCTL/3/PWDCTL_RECFORMATCONV: Failed to convert the password record format.
对系统的影响	用户密码记录无法以规定的格式写入文件，用户无法登录设备
日志产生原因	内部进程错误
处理建议	请收集告警信息、日志信息和配置信息，并联系技术支持工程师

134.11 PWDCTL_UPDATETIME

日志内容	Last login time updated after clock update.
日志含义	用户最近登录时间已同步更新
参数解释	无
日志等级	6 (Informational)
举例	PWDCTL/6/PWDCTL_UPDATETIME: Last login time updated after clock update.
对系统的影响	对系统无影响
日志产生原因	用户最近登录时间已同步更新
处理建议	无需处理

135 QOS

本节介绍 QoS 模块输出的日志信息。

135.1 MIRROR_SYNC_CFG_FAIL

日志内容	Failed to restore configuration for monitoring group [UINT32] in [STRING], because [STRING]
日志含义	监控组的配置数据恢复失败
参数解释	$1：监控组编号 $2：槽位号 $3：数据恢复失败的详细原因
日志等级	4 (Warning)
举例	QOS/4/MIRROR_SYNC_CFG_FAIL: Failed to restore configuration for monitoring group 1 in chassis 2 slot 1, because monitoring resources are insufficient.
对系统的影响	监控组中的成员端口不生效
日志产生原因	业务板插入设备后，恢复该业务板监控组配置信息失败，即监控组的成员端口相关配置不存在。失败原因如下： • 监控端口总数超过当前监控组支持的最大数量 • 当前业务板监控资源不足 • 监控组中端口的类型在当前业务板不支持
处理建议	请根据实际需求重新配置监控组的成员端口

135.2 QOS_CAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to the user. Reason: [STRING].
日志含义	基于User Profile或User Group Profile或Session Group Profile的流量监管对上线用户应用失败
参数解释	$1：用户标识信息 $2：CAR应用方向 $3：Profile类型 $4：Profile名称 $5：失败原因 ○ The resources are insufficient.：资源不足 ○ The operation is not supported.：操作不支持
日志等级	4 (Warning)
举例	QOS/4/QOS_CAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet5/1/5; Failed to apply the inbound CAR in user profile a to the user. Reason: The resources are insufficient.
对系统的影响	上线用户绑定的User Profile或User Group Profile或Session Group Profile中配置的流量监管无效
日志产生原因	• 用户上线过程中，下发的 User Profile 或 User Group Profile 或 Session Group Profile 中配置的 CAR 失败 • 用户已经上线，在用户绑定的User Profile或User Group Profile或Session Group Profile中修改或新增 CAR 失败
处理建议	• 请删除该 User Profile 或 User Group Profile 或 Session Group Profile 下的 CAR 配置 • 请执行 **display resource-monitor**命令检查显示字段中bras_car对应的剩余资源是否充足，如果资源不足，则删除部分无用的流量监管配置 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.3 QOS_CBQ_REMOVED

日志内容	CBQ is removed from [STRING].
日志含义	接口上应用的基于类的队列被删除
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	QOS/4/QOS_CBQ_REMOVED: CBQ is removed from GigabitEthernet4/0/1.
对系统的影响	接口上应用的QoS策略中的流行为如果配置了基于类的队列，则该接口上符合QoS策略流分类的报文不遵循流行为中定义的CBQ队列调度
日志产生原因	因接口最大可用带宽或接口速率更改后低于接口上原来配置的CBQ要求的最小保证带宽，系统从接口上删除CBQ
处理建议	请执行**bandwidth**命令重新修改接口最大可用带宽，使接口最大可用带宽满足CBQ中带宽需求，再重新在接口下应用含CBQ流行为的QoS策略

135.4 QOS_GTS_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply GTS in user profile [STRING] to the user. Reason: [STRING].
日志含义	基于User Profile的流量整形应用失败
参数解释	$1：用户标识信息 $2：User profile名称 $3：失败原因
日志等级	4 (Warning)
举例	QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply GTS in user profile a to the user. Reason: The resources are insufficient.
对系统的影响	应用的User Profile中的流量整形不生效
日志产生原因	• 用户上线过程中，下发的 GTS 信息失败 • 用户已经上线，修改 GTS 信息或者新增 GTS 信息失败
处理建议	**1.** 请删除或修改该 User Profile 下的 GTS 配置 **2.** 请执行 **display resource-monitor**命令检查显示字段中queue_shape对应的剩余资源是否充足，如果资源不足，则删除部分无用的流量整形配置 **3.** 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.5 IFA_CONFIG_FAIL

日志内容	Failed to configure [STRING]. [STRING]
日志含义	INT的相关配置失败
参数解释	$1：IFA具体配置，取值为： • the collector：下发 INT 报文的封装参数命令失败 • the device ID：下发 INT 设备的设备 ID 命令失败 • packet dorp：下发开启全局丢弃 INT 报文命令失败 具体失败原因： • Reason：The operation conflicts with some existing configurations：与设备已存在的配置冲突
日志等级	4 (Warning)
举例	QOS/4/IFA_CONFIG_FAIL: -Slot=2; Failed to configure the device ID.Reason：The operation conflicts with some existing configurations.
对系统的影响	INT功能无法正常生效
日志产生原因	设备已存在Telemetry stream、NetStream、Sflow等功能配置，Slot上新下发的INT配置失败
处理建议	• 请删除 Telemetry stream、NetStream 和 Sflow 功能配置，再重新配置 INT 功能 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.6 IFA_REFRESH_FAIL

日志内容	Failed to refresh IFA action [UINT32] on interface [STRING].
日志含义	接口的INT动作下发失败
参数解释	$1：INT动作的编号 $2：接口名称
日志等级	4 (Warning)
举例	QOS/4/IFA_REFRESH_FAIL: Failed to refresh IFA action 1 on interface GigabitEthernet1/0/1.
对系统的影响	
日志产生原因	接口上配置的INT动作错误
处理建议	• 请检查 INT 动作引用的 ACL 的配置是否正确，按要求修改 ACL 规则后，在接口上重新配置 INT 动作 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.7 QOS_LR_APPLYIF_FAIL

日志内容	Failed to apply the rate limit on interface [STRING]. Reason: [STRING]
日志含义	接口上配置流量限速失败
参数解释	$1：接口名称 $2：失败原因 ○ The operation is not supported.：操作不支持 ○ The resources are insufficient.：资源不足
日志等级	4 (Warning)
举例	QOS/4/QOS_LR_APPLYIF_FAIL: Failed to apply the rate limit on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
对系统的影响	接口上配置的流量限速不生效
日志产生原因	业务单板插入时，配置数据恢复过程中： • 系统检测到单板的接口不支持配置限速功能 • 由于硬件资源不足，导致在接口上配置的限速失败
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

135.8 QOS_MPORT_APPLY_FAIL

日志内容	Failed to refresh configuration for interface [STRING] in the monitoring group [UINT32]. [STRING].
日志含义	监控组成员口应用失败
参数解释	$1：接口名称 $2：监控组号 $3：失败原因 ○ Monitoring resources are insufficient.：监控组资源不足. ○ Ports of the specified type cannot be configured as monitoring ports：监控组成员口不支持
日志等级	4 (Warning)
举例	QOS/4/QOS_MPORT_APPLY_FAIL: Failed to refresh configuration for interface M-GigabitEthernet0/0/0 in monitoring group 1. Monitoring resources are insufficient.
对系统的影响	监控组成员不生效
日志产生原因	• 监控组资源不足 • 监控组成员口接口类型不支持
处理建议	• 请在其他业务板卡的接口上监控流量 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.9 QOS_NOT_ENOUGH_BANDWIDTH

日志内容	Policy [STRING] request bandwidth [UINT32](kbps). Only [UINT32](kbps) available on [STRING].
日志含义	带宽不足，基于类的队列应用失败
参数解释	$1：QoS策略名称 $2：CBWFQ需要的带宽 $3：接口可用带宽 $4：接口名称
日志等级	3 (Error)
举例	QOS/3/QOS_NOT_ENOUGH_BANDWIDTH: Policy d request bandwidth 10000(kbps). Only 80(kbps) available on GigabitEthernet4/0/1.
对系统的影响	接口上应用的基于类的队列CBQ不生效
日志产生原因	因CBQ要求的最小保证带宽大于接口最大可用带宽，CBQ配置失败
处理建议	请修改CBQ配置的最小保证带宽，再重新在接口下应用含CBQ流行为的QoS策略，或者执行**bandwidth**命令重新修改接口最大可用带宽，使接口最大可用带宽满足CBQ中带宽需求

135.10 QOS_NOT_ENOUGH_NNIBANDWIDTH

日志内容	形式一： The total UNI bandwidth is greater than the NNI bandwidth. 形式二： The total UNI bandwidth is greater than the NNI bandwidth.The bandwidth of [STRING] is changed. 形式三： The total UNI bandwidth is greater than the NNI bandwidth.[STRING] is created based on [STRING] of the UNI interface.
日志含义	带宽保证组的UNI接口配置的下行带宽之和超出上行带宽阈值
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	形式一： QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. 形式二： QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. The bandwidth of GigabitEthernet4/0/1 is changed. 形式三： QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. Virtual-Access1 is created based on Virtual-Template1 of the UNI interface.
对系统的影响	上行流量可能出现拥塞丢包的情况
日志产生原因	形式一： • 当用户增加上行接口带宽或降低下行接口带宽限速后，下行总带宽仍然大于上行带宽阈值 形式二： • 接口带宽改变导致下行接口总带宽大于上行接口总带宽 形式三： • 新创建的 Virtual-Access 接口导致下行接口总带宽大于上行接口总带宽
处理建议	增加上行带宽阈值或降低UNI接口配置的下行限制带宽

135.11 QOS_POLICY_APPLYCOPP_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
日志含义	控制平面下的QoS策略中的流行为应用失败
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：槽位号 $5：失败原因 ○ The behavior is empty：流行为为空 ○ Only one rate-limiting action is supported in one behavior to be applied to the control plane：一个流行为中仅支持配置一个限速动作
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYCOPP_CBFAIL: Failed to apply classifier-behavior d in policy b to the inbound direction of control plane slot 3. The behavior is empty.
对系统的影响	在控制平面下应用QoS策略，该QoS策略中的某个流行为不生效
日志产生原因	在控制平面的某个方向上新增或修改QoS策略中的某个CB对配置
处理建议	请根据失败原因，修改QoS策略中的流行为的配置

135.12 QOS_POLICY_APPLYCOPP_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
日志含义	控制平面上应用QoS策略失败
参数解释	$1：QoS策略名称 $2：流量方向 $3：槽位号 $4：失败原因 ○ The operation is not supported：不支持的 QoS 策略
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYCOPP_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of control plane slot 3. The operation is not supported.
对系统的影响	控制平面上应用QoS策略不生效
日志产生原因	在控制平面的某个方向上应用或更新QoS策略失败
处理建议	**1.** 请修改该 QoS 策略并重新在控制平面下应用 **2.** 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.13 QOS_POLICY_APPLYGLOBAL_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction globally. [STRING].
日志含义	全局应用的QoS策略中的流行为应用失败
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：失败原因 ○ The behavior is empty：流行为为空
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYGLOBAL_CBFAIL: Failed to apply classifier-behavior a in policy b to the outbound direction globally. The behavior is empty.
对系统的影响	全局应用QoS策略，该QoS策略中的某个流行为不生效
日志产生原因	在全局的某个方向上新增或修改QoS策略中的某个CB对配置
处理建议	**1.** 请修改该 QoS 策略中的 CB 对，并重新在控制平面下应用该 QoS 策略 **2.** 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.14 QOS_POLICY_APPLYGLOBAL_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction globally. [STRING].
日志含义	全局应用的QoS策略失败
参数解释	$1：QoS策略名称 $2：流量方向 $3：失败原因 ○ The operation is not supported.：操作不支持
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYGLOBAL_FAIL: Failed to apply or refresh QoS policy b to the inbound direction globally. The operation is not supported.
对系统的影响	全局应用的QoS策略不生效
日志产生原因	新配置或修改的QoS策略应用到全局某个方向上
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

135.15 QOS_POLICY_APPLYIF_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
日志含义	接口下应用的QoS策略中的流行为应用失败
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：接口名称 $5：失败原因 ○ The behavior is empty.：流行为为空，未配置任何动作 ○ The card where the interface specified in the class-behavior association resides is not in position.：CB 对中配置的接口所在的单板不在位 ○ Only one service class marking action is supported for the same EXP value on the same interface and the service class value can't be modified except that the old value has been deleted.：对于同一个 EXP 值，同一接口上仅支持配置一个重新标记报文的 MPLS TE 隧道转发类值的动作；且仅支持通过删除并重新配置的方式进行修改
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYIF_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of interface Ethernet3/1/2. The behavior is empty.
对系统的影响	接口下应用QoS策略，该QoS策略中的某个流行为不生效
日志产生原因	在接口的某个方向上新增或修改QoS策略中的某个CB对配置
处理建议	**1.** 请根据失败原因，修改 QoS 策略中的 CB 对配置 **2.** 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.16 QOS_POLICY_APPLYIF_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
日志含义	接口下的QoS策略应用失败
参数解释	$1：QoS策略名称 $2：流量方向 $3：接口名称 $4：失败原因 ○ The operation is not supported.：操作不支持
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYIF_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of interface Ethernet3/1/2. The operation is not supported.
对系统的影响	接口下配置的QoS策略不生效
日志产生原因	在接口的某个方向上配置或修改QoS策略
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

135.17 QOS_POLICY_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] QoS policy [STRING] in user profile [STRING] to the user.Reason: [STRING].
日志含义	基于User Profile下的应用的QoS策略失败
参数解释	$1：用户标识信息 $2：QoS策略应用方向 $3：QoS策略名称 $4：User Profile名称 $5：失败原因 ○ The QoS policy is not supported.：User Profile 下不支持该 QoS 策略
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound QoS policy p in user profile a to the user.Reason: The QoS policy is not supported.
对系统的影响	基于User Profile下的应用的QoS策略不生效
日志产生原因	• 用户上线过程中，下发的 User Profile 中配置了 QoS 策略 • 用户已经上线，修改 User Profile 中的 QoS 策略信息或者新增 QoS 策略
处理建议	• 请删除或修改 User Profile 中配置的 QoS 策略 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.18 QOS_POLICY_APPLYVLAN_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
日志含义	基于VLAN应用QoS策略中的流行为应用失败
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：VLAN ID $5：失败原因 ○ The behavior is empty.
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYVLAN_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of VLAN 2. The behavior is empty.
对系统的影响	基于VLAN应用QoS策略，该QoS策略中的某个流行为不生效
日志产生原因	在在VLAN的某个方向上新增或修改QoS策略中的某个CB对配置
处理建议	• 请根据失败原因，修改 QoS 策略中的 CB 对配置 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.19 QOS_POLICY_APPLYVLAN_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
日志含义	基于VLAN的QoS策略应用失败
参数解释	$1：QoS策略名称 $2：流量方向 $3：VLAN ID $4：失败原因 ○ The operation is not supported.：VLAN 下不支持该 QoS 策略
日志等级	4 (Warning)
举例	QOS/4/QOS_POLICY_APPLYVLAN_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of VLAN 2. The operation is not supported.
对系统的影响	基于VLAN应用的QoS策略不生效
日志产生原因	在VLAN的某个方向上新增或修改QoS策略
处理建议	• 请删除或修改 VLAN 的某个方向上应用的 QoS 策略 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.20 QOS_QMPROFILE_APPLYIF_FAIL

日志内容	Failed to apply queue scheduling profile [STRING] on interface [STRING]. Reason: [STRING]
日志含义	接口上应用队列调度策略失败
参数解释	$1：队列调度策略名称 $2：接口名称 $3：失败原因 ○ The operation is not supported.：操作不支持 ○ The resources are insufficient.：资源不足
日志等级	4 (Warning)
举例	QOS/4/QOS_QMPROFILE_APPLYIF_FAIL: Failed to apply queue scheduling profile b on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
对系统的影响	接口上应用的队列调度策略功能不生效
日志产生原因	插入业务单板，配置数据恢复过程中： • 系统检测到该接口不支持应用队列调度策略 • 由于硬件资源不足，导致在接口上应用队列调度策略失败
处理建议	请在接口上删除队列调度策略的配置或者收集配置文件、日志信息和告警信息，并联系技术支持

135.21 QOS_QMPROFILE_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply queue scheduling profile [STRING] in session group profile [STRING] to the user. Reason: [STRING].
日志含义	上线用户授权的Session Group Profile中配置的队列调度策略应用失败
参数解释	$1：用户标识信息 $2：队列调度策略名称 $3：Session Group Profile名称 $4：失败原因 ○ The QMProfile is not supported.：队列调度策略不支持
日志等级	4 (Warning)
举例	QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply queue scheduling profile b in session group profile a to the user. Reason: The QMProfile is not supported.
对系统的影响	上线用户授权的Session Group Profile中配置的队列调度策略不生效
日志产生原因	• 用户上线过程中，下发 Session Group Profile 中配置了队列调度策略 • 用户已经上线，修改或者新增 Session Group Profile 中的队列调度策略配置
处理建议	请在上线用户授权的Session Group Profile中删除队列调度策略

135.22 QOS_QMPROFILE_MODIFYQUEUE_FAIL

日志内容	Failed to configure queue [UINT32] in queue scheduling profile [STRING]. [STRING].
日志含义	队列调度策略中的队列调度方式和参数修改失败
参数解释	$1：队列编号 $2：队列调度策略的名称 $3：失败原因 o The value is out of range.
日志等级	4 (Warning)
举例	QOS/4/QOS_QMPROFILE_MODIFYQUEUE_FAIL: Failed to configure queue 1 in queue scheduling profile myqueue. The value is out of range.
对系统的影响	队列调度策略中的队列调度无法修改，仍按原队列调度方式和参数生效
日志产生原因	在接口下应用队列调度策略之后，再修改队列调度策略中某队列的配置，新配置的参数超出端口能力范围
处理建议	• 请先在接口下删除应用队列调度策略，再修改队列调度策略下的队列参数 • 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.23 QOS_QUEUE_APPLYIF_FAIL

日志内容	Failed to apply queue scheduling on interface [STRING]. Reason: [STRING]
日志含义	接口上应用队列失败
参数解释	$1：接口名称 $2：失败原因 o The operation is not supported.：操作不支持 o The resources are insufficient.：资源不足
日志等级	4 (Warning)
举例	QOS/4/QOS_QUEUE_APPLYIF_FAIL: Failed to apply queue scheduling on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
对系统的影响	接口上应用的队列，例如接口上配置的WFQ、WRR或SP队列等不生效
日志产生原因	插入业务单板，配置数据恢复过程中： • 系统检测到该接口不支持配置队列调度 • 由于硬件资源不足，导致在接口上队列配置失败
处理建议	请在接口上删除队列配置或者收集配置文件、日志信息和告警信息，并联系技术支持

135.24 QOS_UNI_RESTORE_FAIL

日志内容	Failed to restore the UNI configuration of [STRING], because the total UNI bandwidth is greater than the NNI bandwidth.
日志含义	由于带宽保证组的UNI接口配置的下行带宽之和超出上行带宽阈值，UNI接口配置的下行带宽数据恢复失败
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	QOS/4/ QOS_NNIBANDWIDTH_OVERFLOW: Failed to restore the UNI configuration of the interface GigabitEthernet5/1/5, because the total UNI bandwidth is greater than the NNI bandwidth.
对系统的影响	带宽保证组的UNI接口配置的下行带宽限速不生效
日志产生原因	业务板卡重启或重新插入机框等情况下，恢复UNI接口配置数据时，因UNI接口上的带宽限速总和超过上行接口带宽阈值，接口的UNI接口配置数据恢复失败
处理建议	请重新配置带宽保证组中的带宽，例如增加上行接口带宽阈值或降低UNI接口CAR带宽限速，并且执行**qos uni enable**命令重新使能UNI接口的带宽保证组功能

135.25 WRED_TABLE_APPLYFABRIC_FAIL

日志内容	Failed to apply WRED table [STRING] to internal interfaces.Reason: [STRING].
日志含义	在板卡的内联口上应用WRED表失败
参数解释	$1：WRED表的名称 $2：下发和刷新配置失败的详细原因 ○ Hardware resources are insufficient.：业务板上资源不足 ○ ECN is not supported.：业务板内联口不支持应用 WRED 表
日志等级	4 (Warning)
举例	QOS/4/WRED_TABLE_APPLYFABRIC_FAIL: Failed to apply WRED table aaa to internal interfaces.Reason:Hardware resources are insufficient.
对系统的影响	内联口上的网络如果出现拥塞，无法通过WRED表来实现拥塞管理
日志产生原因	某些WRED配置在部分业务板上不支持或者业务板上资源不足
处理建议	**1.** 如果配置失败的详细原因显示为 ECN is not supported.，则在 WRED 表视图下删除 ECN 配置，再重新应用 WRED 表 **2.** 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

135.26 WRED_TABLE_CFG_FAIL

日志内容	Failed to dynamically modify the configuration of WRED table [STRING], because [STRING].
日志含义	修改WRED表中的配置失败
参数解释	$1：WRED表的名称 $2：配置失败的详细原因 ○ ECN is not supported.
日志等级	4 (Warning)
举例	QOS/4/WRED_TABLE_CFG_FAIL: Failed to dynamically modify the configuration of WRED table a, because ECN is not supported.
对系统的影响	修改WRED表中的配置不生效
日志产生原因	由于硬件业务板不支持某些特性，例如ECN功能，修改WRED表中的相应功能配置时失败
处理建议	请勿配置业务板不支持的相关功能或者收集配置文件、日志信息和告警信息，并联系技术支持

136 RADIUS

本节介绍 RADIUS 模块输出的日志信息。

136.1 RADIUS_ACCT_SERVER_DOWN

日志内容	RADIUS accounting server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	RADIUS计费服务器状态为阻塞
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4 (Warning)
举例	RADIUS/4/RADIUS_ACCT_SERVER_DOWN: RADIUS accounting server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	服务器不可达，用户上线失败
日志产生原因	设备发现RADIUS计费服务器状态从active变为block
处理建议	1. 执行命令 **display interface**检查连接RADIUS计费服务器的接口是否为UP。 o 如果是，请执行步骤 2。 o 如果否，请检查物理链路的连接，确保物理链路连接正常。 2. 执行命令 **ping**检查RADIUS计费服务器是否可达。 o 如果是，请执行步骤 3。 o 如果否，请首先检查设备与 RADIUS 计费服务器之间的网络可达性，然后排查网络中是否存在防火墙等设备，确保 RADIUS 计费服务器可达。 3. 执行命令 **display current-configuration**检查设备上RADIUS计费服务器配置是否正确。 o 如果是，请执行步骤 4。 o 如果否，请参考《AAA 命令参考》、《AAA 配置指导》手册修改 RADIUS 计费服务器的配置。 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

136.2 RADIUS_ACCT_SERVER_UP

日志内容	RADIUS accounting server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	RADIUS计费服务器状态变为激活
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6 (Informational)
举例	RADIUS/6/RADIUS_ACCT_SERVER_UP: RADIUS accounting server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	对系统无影响
日志产生原因	设备发现RADIUS计费服务器状态从block变为active
处理建议	系统正常运行时产生的信息，无需处理

136.3 RADIUS_AUTH_FAILURE

日志内容	User [STRING] at [STRING] failed authentication.
日志含义	RADIUS服务器了拒绝用户的认证请求
参数解释	$1：用户名称 $2：IP地址
日志等级	5 (Notification)
举例	RADIUS/5/RADIUS_AUTH_FAILURE: User abc@system at 192.168.0.22 failed authentication.
对系统的影响	用户认证失败
日志产生原因	RADIUS服务器了拒绝用户的认证请求
处理建议	**1.** 检查设备上的 RADIUS 认证相关配置，并联系服务器管理员确认拒绝认证请求的原因，根据具体原因解决。 **2.** 用户重新发起认证后，如果此日志依然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

136.4 RADIUS_AUTH_SERVER_DOWN

日志内容	RADIUS authentication server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	RADIUS认证服务器状态为阻塞
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4 (Warning)
举例	RADIUS/4/RADIUS_AUTH_SERVER_DOWN: RADIUS authentication server was blocked: Server IP= 1.1.1.1, port=1812, VPN instance=public.
对系统的影响	会导致用户上线认证失败，如果没有备份认证服务器可能造成用户下线
日志产生原因	RADIUS认证服务器状态从active变为block
处理建议	**1.** 执行命令 **`display interface`**检查连接RADIUS认证服务器的接口是否为UP。 o 如果是，请执行步骤 2。 o 如果否，请检查物理链路的连接，确保物理链路连接正常。 **2.** 执行命令 **`ping`**检查RADIUS认证服务器是否可达。 o 如果是，请执行步骤 3。 o 如果否，请首先检查设备与 RADIUS 认证服务器之间的网络可达性，然后排查网络中是否存在防火墙等设备，确保 RADIUS 认证服务器可达。 **3.** 执行命令 **`display current-configuration`**检查设备上RADIUS认证服务器配置是否正确。 o 如果是，请执行步骤 4。 o 如果否，请参考《AAA 命令参考》、《AAA 配置指导》手册修改 RADIUS 认证服务器的配置。 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

136.5 RADIUS_AUTH_SERVER_UP

日志内容	RADIUS authentication server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	RADIUS认证服务器状态变为激活
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6 (Informational)
举例	RADIUS/6/RADIUS_AUTH_SERVER_UP: RADIUS authentication server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	对系统无影响
日志产生原因	设备发现RADIUS认证服务器状态从block变为active
处理建议	系统正常运行时产生的信息，无需处理

136.6 RADIUS_AUTH_SUCCESS

日志内容	User [STRING] at [STRING] was authenticated successfully.
日志含义	用户在RADIUS服务器上认证成功
参数解释	$1：用户名称 $2：IP地址
日志等级	6 (Informational)
举例	RADIUS/6/RADIUS_AUTH_SUCCESS: User abc@system at 192.168.0.22 was authenticated successfully.
对系统的影响	对系统无影响
日志产生原因	RADIUS服务器接收了用户的认证请求
处理建议	系统正常运行时产生的信息，无需处理

136.7 RADIUS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
日志含义	删除RADIUS方案中的服务器失败
参数解释	$1：方案名称
日志等级	4 (Warning)
举例	RADIUS/4/RADIUS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	通过命令行删除RADIUS方案中的服务器失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

137 RDDC

本节介绍 RDDC（redundancy）模块输出的日志信息。

137.1 RDDC_ACTIVENODE_CHANGE

日志内容	Redundancy group [STRING] active node changed to [STRING], because of [STRING].
日志含义	冗余组激活节点发生切换
参数解释	$1：冗余组名称 $2：激活节点信息 $3：状态变化原因 ○ manual switchover：表示状态变化由手动切换引起 ○ group's configuration changed：表示状态变化由冗余组配置变化引起 ○ node's weight changed：表示状态变化由冗余组节点权重变化引起
日志等级	5 (Notification)
举例	RDDC/5/RDDC_ACTIVENODE_CHANGE: Redundancy group 1 active node changed to node 1 (chassis 1), because of manual switchover.
对系统的影响	冗余组倒换，业务会在主备设备间进行迁移，对业务运行无影响
日志产生原因	日志产生原因可能为： • 原因一：管理员执行 **switchover**命令，触发手工倒换 • 原因二：冗余组配置变更，例如在冗余组节点视图下执行 **priority**命令修改了节点的优先级，或者执行 **undo node**命令删除冗余组节点等 • 原因三：冗余组节点的权重变换
处理建议	• 如果日志产生原因为原因一和原因二，无需处理 • 如果日志产生原因为原因三，请执行 **display redundancy group**命令查看冗余组关联的Track项，然后执行 **display track**命令查看Track项的信息，找到Track项状态变化的原因，修复该原因，使得冗余组的主备节点能正常运行，主备功能继续生效

138 RESMON

本节介绍 RESMON（RESOURCE MONITER，资源监控）模块输出的日志信息。

138.1 RESMON_MINOR

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource decreased to or below minor threshold [STRING]. [STRING].
日志含义	剩余硬件资源小于或等于硬件资源低级别告警门限
参数解释	$1：资源名称 $2：资源总数 $3：当前已使用的资源数 $4：当前剩余的资源数 $5：低级别告警门限值 $6：资源的补充描述信息，部分资源可能无该描述信息
日志等级	4 (Warning)
举例	RESMON/4/RESMON_MINOR: -Resource=AA-Total=100%-Used=83%-Free=17%; Free resource decreased to or below minor threshold 20%.
对系统的影响	对系统暂无影响，需要留意剩余硬件资源是否持续减少
日志产生原因	当剩余硬件资源小于或等于硬件资源低级别告警门限时，设备转入硬件资源低级别告警状态，并打印该日志
处理建议	请根据具体的资源类型操作设备，使资源得到合理分配

138.2 RESMON_MINOR_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource increased above minor threshold [STRING]. [STRING].
日志含义	剩余硬件资源大于硬件资源低级别告警门限
参数解释	$1：资源名称 $2：资源总数 $3：当前已使用的资源数 $4：当前剩余的资源数 $5：低级别告警门限值 $6：资源的补充描述信息，部分资源可能无该描述信息
日志等级	5 (Notification)
举例	RESMON/5/RESMON_MINOR_RECOVER: -Resource=AA-Total=100%-Used=77%-Free=23%; Free resource increased above minor threshold 20%.
对系统的影响	对系统无影响
日志产生原因	当剩余硬件资源大于硬件资源低级别告警门限时，系统解除硬件资源低级别告警状态，并打印该日志。硬件资源使用率进入正常范围
处理建议	无需处理

138.3 RESMON_SEVERE

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource decreased to or below severe threshold [STRING]. [STRING].
日志含义	剩余硬件资源小于或等于硬件资源高级别告警门限，且硬件资源未被用尽
参数解释	$1：资源名称 $2：资源总数 $3：当前已使用的资源数 $4：当前剩余的资源数 $5：高级别告警门限值 $6：资源的补充描述信息，部分资源可能无该描述信息
日志等级	3 (Error)
举例	RESMON/3/RESMON_SEVERE: -Resource=AA-Total=100%-Used=93%-Free=7%; Free resource decreased to or below severe threshold 10%.
对系统的影响	使用该硬件资源的业务即将受限或不可用
日志产生原因	当剩余硬件资源小于或等于硬件资源高级别告警门限时，且硬件资源未被用尽，则设备转入硬件资源高级别告警状态，并打印该日志
处理建议	请根据具体的资源类型操作设备，使资源得到合理分配

138.4 RESMON_SEVERE_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource increased above severe threshold [STRING]. [STRING].
日志含义	剩余硬件资源大于硬件资源高级别告警门限
参数解释	$1：资源名称 $2：资源总数 $3：当前已使用的资源数 $4：当前剩余的资源数 $5：高级别告警门限值 $6：资源的补充描述信息，部分资源可能无该描述信息
日志等级	5 (Notification)
举例	RESMON/5/RESMON_SEVERE_RECOVER: -Resource=AA-Total=100%-Used=83%-Free=17%; Free resource increased above severe threshold 10%.
对系统的影响	对系统无影响
日志产生原因	当剩余硬件资源大于硬件资源高级别告警门限时，系统解除硬件资源高级别告警状态，并打印该日志
处理建议	无需处理

138.5 RESMON_USEDUP

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Resources used up. [STRING].
日志含义	硬件资源已用尽
参数解释	$1：资源名称 $2：资源总数 $3：当前已使用的资源数 $4：当前剩余的资源数 $5：资源的补充描述信息，部分资源可能无该描述信息
日志等级	2 (Critical)
举例	RESMON/2/RESMON_USEDUP: -Resource=vlaninterface-Total=2048-Used=2048-Free=0; Resources used up.
对系统的影响	使用该硬件资源的业务受限或不可用
日志产生原因	在硬件资源已用尽时，设备转入硬件资源用尽状态，并定期打印该日志
处理建议	请尽快清理资源中不用的数据或者表项，以免对应业务受影响

138.6 RESMON_USEDUP_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; The amount of free resources increased from zero to a non-zero value. [STRING].
日志含义	硬件资源已被释放
参数解释	$1：资源名称 $2：资源总个数，当以绝对值显示时为INT32数值；当以百分比显示时为100% $3：当前使用的资源个数，当以绝对值显示时为INT32数值；当以百分比显示时为xx% $4：当前剩余的资源个数，当以绝对值显示时为INT32数值；当以百分比显示时为xx% $5：产品对资源使用附加信息，可能为空
日志等级	5 (Notification)
举例	RESMON/5/RESMON_USEDUP_RECOVER: -Resource=vlaninterface-Total=2048-Used=2047-Free=1; The amount of free resources increased from zero to a non-zero value.
对系统的影响	对系统无影响
日志产生原因	当硬件资源被释放时，系统硬件解除资源用尽状态，并打印该日志
处理建议	无需处理

139 RIP

本节介绍 RIP 模块输出的日志信息。

139.1 RIPLOG

日志内容	RIP: Interfaces [STRING] [STRING] Multicast group failed, return value [STRING]
日志含义	RIP接口退出或加入组播组失败
参数解释	$1：接口名称 $2：退出或加入组播组失败，取值包括 • Quitting：表示退出组播组失败 • Joining：表示加入组播组失败 $3：错误码，取值包括： • 22：表示无效的参数 • 99：表示组播源地址错误 • 105：表示设备内存不足
日志等级	6 (Informational)
举例	RIP/6/RIPLOG:RIP: Interfaces GigabitEthernet1/0/1 Joining Multicast group failed, return value 22
对系统的影响	无
日志产生原因	接口加入或退出组播组失败，无法正常开始或停止收发RIP组播报文
处理建议	• 重启接口或设备 • 如果问题仍然存在，请收集日志信息并联系技术支持

140 RIPNG

本节介绍 RIPng 模块输出的日志信息。

140.1 RIPNGLOG

日志内容	RIPng: Interfaces [STRING] [STRING] Multicast group failed, return value [STRING].
日志含义	RIPng接口退出或加入组播组失败
参数解释	$1：接口名称 $2：退出或加入组播组失败，取值包括 • Quitting：表示退出组播组失败 • Joining：表示加入组播组失败 $3：错误码，取值包括： • 22：表示无效的参数 • 99：表示组播源地址错误 • 105：表示设备内存不足
日志等级	6 (Informational)
举例	RIPng/6/RIPNGLOG:RIPng: Interfaces GigabitEthernet1/0/1 Joining Multicast group failed, return value 22.
对系统的影响	无
日志产生原因	接口加入或退出组播组失败，无法正常开始或停止收发RIPng组播报文
处理建议	• 重启接口或设备 • 如果问题仍然存在，请收集日志信息并联系技术支持

日志内容	RIPng Socket Set-option failed on [STRING], this packet will be sent next time.
日志含义	RIPng接口在发送报文时设置套接字选项失败，该报文会被重新发送
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	RIPng/6/RIPNGLOG:RIPng Socket Set-option failed on GigabitEthernet1/0/1, this packet will be sent next time.
对系统的影响	无
日志产生原因	RIPng接口在发送报文时设置socket选项失败
处理建议	正常运行信息，无需处理

141 RM

本节介绍 RM 模块输出的日志信息。

141.1 RM_ACRT_REACH_LIMIT

日志内容	Max active [STRING] routes [UINT32] reached in URT of [STRING]
日志含义	指定VPN实例的激活路由数量达到了上限值
参数解释	$1：IPv4或IPv6 $2：最大激活路由数 $3：VPN实例名
日志等级	4 (Warning)
举例	RM/4/RM_ACRT_REACH_LIMIT: Max active IPv4 routes 100000 reached in URT of VPN1
对系统的影响	过多的激活路由数量会占用系统内存等资源
日志产生原因	VPN实例单播路由表中的激活路由数达到了上限值，不支持继续激活新的路由前缀
处理建议	1. 执行命令查看指定 VPN 实例单播路由统计信息： o 对于IPv4 路由，执行 **display ip routing-table vpn-instance** *vpn-instance-name* **statistics**命令。 o 对于IPv6 路由，执行 **display ipv6 routing-table vpn-instance** *vpn-instance-name* **statistics**命令。 2. 分析各协议路由来源，确认当前 VPN 实例是否有多余的路由： o 如果有多余的路由，则删除不必要的路由，并查看路由总数是否低于上限值，如果低于上限值，则处理结束；如果仍高于上限值，请执行步骤 3。 o 如果没有多余的路由，请执行步骤 3。 3. 进入VPN实例IPv4 地址族视图/VPN实例IPv6 地址族视图，执行 **display this**查看本VPN实例的最大激活路由前缀数量，确认配置是否合理： o 如果合理，请收集日志信息和配置信息，并联系技术支持人员。 o 如果不合理，请执行 **routing-table limit**命令，重新配置合理的激活路由数量上限值

141.2 RM_ACRT_REACH_THRESVALUE

日志内容	Threshold value [UINT32] of max active [STRING] routes reached in URT of [STRING]
日志含义	指定VPN实例的激活路由前缀数量达到了本VPN实例的告警阈值，但是没有超过最大值
参数解释	$1：最大激活路由数告警阈值 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4 (Warning)
举例	RM/4/RM_ACRT_REACH_THRESVALUE: Threshold value 50% of max active IPv4 routes reached in URT of vpn1
对系统的影响	设备仍然允许新的激活路由前缀。当VPN实例中的激活路由前缀数达到最多支持激活路由前缀数目时，设备不再激活新的路由前缀
日志产生原因	VPN实例单播路由表中的激活路由数达到了最大路由数告警阈值
处理建议	检查是否需要增加VPN实例的最大路由前缀数量或者最大激活路由数量告警阈值

141.3 RM_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] of active [STRING] routes reached in URT of [STRING]
日志含义	指定VPN实例的激活路由数量达到了本VPN实例的上限值
参数解释	$1：最大激活路由数 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4 (Warning)
举例	RM/4/RM_THRESHLD_VALUE_REACH: Threshold value 10000 of active IPv4 routes reached in URT of vpn1
对系统的影响	过多的激活路由数量会占用的系统内存等资源
日志产生原因	VPN实例单播路由表中的激活路由数达到了上限值，支持继续激活新的路由前缀
处理建议	1. 执行命令查看指定 VPN 实例单播路由统计信息： o 对于IPv4 路由，执行 **display ip routing-table vpn-instance** *vpn-instance-name* **statistics**命令。 o 对于IPv6 路由，执行 **display ipv6 routing-table vpn-instance** *vpn-instance-name* **statistics**命令。 2. 分析各协议路由来源，确认当前 VPN 实例是否有多余的路由： o 如果有多余的路由，则删除不必要的路由，并查看路由总数是否低于上限值，如果低于上限值，则处理结束；如果仍高于上限值，请执行步骤 3。 o 如果没有多余的路由，请执行步骤 3。 3. 进入VPN实例IPv4 地址族视图/VPN实例IPv6 地址族视图，执行 **display this**查看本VPN实例的最大激活路由前缀数量，确认配置是否合理： o 如果合理，请收集日志信息和配置信息，并联系技术支持人员。 o 如果不合理，请执行 **routing-table limit**命令，重新配置合理的激活路由数量上限值

141.4 RM_TOTAL_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] reached for active [STRING] routes in all URTs
日志含义	公网和所有VPN实例的激活路由总数达到了设备支持的最大值
参数解释	$1：最大激活路由数 $2：IPv4或IPv6
日志等级	4 (Warning)
举例	RM/4/ RM_TOTAL_THRESHLD_VALUE_REACH:Threshold value 1000 reached for active IPv4 routes in all URTs
对系统的影响	过多的激活路由数量会占用系统内存等资源
日志产生原因	公网和所有VPN实例的激活路由总数达到了告警值，不支持继续激活新的路由前缀
处理建议	1. 执行命令查看设备单播路由统计信息： o 对于IPv4 路由，执行 **display ip routing-table all-routes statistics**命令。 o 对于IPv6 路由，执行 **display ipv6 routing-table all-routes statistics**命令。 2. 分析各协议路由来源，确认公网或 VPN 实例是否有多余的路由： o 如果有多余的路由，则删除不必要的路由，并查看路由总数是否低于上限值，如果低于上限值，则处理结束；如果仍高于上限值，请执行步骤 3。 o 如果没有多余的路由，请执行步骤 3。 3. 进入RIB IPv4 地址族视图/RIB IPv6 地址族视图，执行 **display this**查看的IPv4/IPv6 最大激活路由前缀数量，确认配置是否合理： o 如果合理，请收集日志信息和配置信息，并联系技术支持人员。 o 如果不合理，请执行 **routing-table limit**命令，重新配置合理的激活路由数量上限值

142 RPR

本节介绍 RPR 模块输出的日志信息。

142.1 RPR_EXCEED_MAX_SEC_MAC

日志内容	A maximum number of secondary MAC addresses exceeded defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环的次级MAC地址的数量超过了最大数量
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	RPR/4/RPR_EXCEED_MAX_SEC_MAC: A maximum number of secondary MAC addresses exceeded defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	影响环网流量转发
日志产生原因	RPR环的次级MAC地址的数量超过了最大数量
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

142.2 RPR_EXCEED_MAX_SEC_MAC_OVER

日志内容	A maximum number of secondary MAC addresses exceeded defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环的次级MAC地址的数量不再超过最大数量
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_EXCEED_MAX_SEC_MAC_OVER: A maximum number of secondary MAC addresses exceeded defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环的次级MAC地址的数量不再超过最大数量
处理建议	无需处理

142.3 RPR_EXCEED_MAX_STATION

日志内容	A maximum number of stations exceeded defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环的站点的数量超过了最大数量
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	RPR/4/RPR_EXCEED_MAX_STATION: A maximum number of stations exceeded defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	影响流量转发
日志产生原因	RPR环的站点的数量超过了最大数量
处理建议	减少RPR环上站点的数量

142.4 RPR_EXCEED_MAX_STATION_OVER

日志内容	A maximum number of stations exceeded defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点的数量正常
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_EXCEED_MAX_STATION_OVER: A maximum number of stations exceeded defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上站点的数量正常
处理建议	系统正常运行时产生的信息，无需处理

142.5 RPR_EXCEED_RESERVED_RATE

日志内容	An excess reserved rate defect is present on [STRING] corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点配置的预留带宽总和超过了环路总带宽
参数解释	$1：RPR环： ○ ringlet0：0 环 ○ ringlet1：1 环 $2：接口名称
日志等级	3 (Error)
举例	RPR/3/RPR_EXCEED_RESERVED_RATE: An excess reserved rate defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
对系统的影响	可能导致预留给特定业务的带宽不足
日志产生原因	RPR环上各站点配置的预留带宽总和超过了环路总带宽
处理建议	修改配置，减少站点的预留带宽，使其总和不大于环路总带宽

142.6 RPR_EXCEED_RESERVED_RATE_OVER

日志内容	An excess reserved rate defect is cleared on [STRING] corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点配置的预留带宽总和不超过环路带宽
参数解释	$1：RPR环： ○ ringlet0：0 环 ○ ringlet1：1 环 $2：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_EXCEED_RESERVED_RATE_OVER: An excess reserved rate defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上各站点配置的预留带宽总和不超过环路带宽
处理建议	系统正常运行时产生的信息，无需处理

142.7 RPR_IP_DUPLICATE

日志内容	A duplicate IP address defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上至少两个站点间的IP地址重复
参数解释	$1：接口名称
日志等级	3 (Error)
举例	RPR/3/RPR_IP_DUPLICATE: A duplicate IP address defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	IP冲突影响流量转发
日志产生原因	RPR环上至少两个站点间的IP地址重复
处理建议	找到IP地址相同的站点，并修改其IP地址

142.8 RPR_IP_DUPLICATE_OVER

日志内容	A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点的IP地址不再相同
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_IP_DUPLICATE_OVER: A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上站点的IP地址不再相同
处理建议	系统正常运行时产生的信息，无需处理

142.9 RPR_JUMBO_INCONSISTENT

日志内容	A jumbo configuration defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上至少两个站点间的Jumbo帧配置不一致
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	RPR/6/RPR_JUMBO_INCONSISTENT: A jumbo configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	影响流量转发
日志产生原因	RPR环上至少两个站点间的Jumbo帧配置不一致
处理建议	找到Jumbo帧配置不一致的站点，并修改其Jumbo帧配置

142.10 RPR_JUMBO_INCONSISTENT_OVER

日志内容	A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点的Jumbo帧配置一致
参数解释	$1：接口名称
日志等级	6 (Informational)
举例	RPR/6/RPR_JUMBO_INCONSISTENT_OVER: A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上站点的Jumbo帧配置一致
处理建议	系统正常运行时产生的信息，无需处理

142.11 RPR_LAGGCONFIG_INCONSISTENT

日志内容	An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上，本站点与邻居站点的RPR逻辑接口的聚合配置不一致
参数解释	$1：RPR逻辑接口名称
日志等级	4 (Warning)
举例	RPR/4/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	本站点与邻居站点的RPR逻辑接口的聚合配置不一致，比如一边加入聚合，另外一边未加入聚合
处理建议	使用**display link-aggregation verbose**命令检查本站点和邻居站点的RPR逻辑接口的聚合配置，确保本站点和邻居站点上的聚合配置保持一致

142.12 RPR_LAGGCONFIG_INCONSISTENT_OVER

日志内容	An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上，本站点与邻居站点的RPR逻辑接口的聚合配置已经更改为一致
参数解释	$1：RPR逻辑接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	本站点与邻居站点的RPR逻辑接口的聚合配置已经更改为一致
处理建议	系统正常运行时产生的信息，无需处理

142.13 RPR_MISCABLING

日志内容	A miscabling defect is present on [STRING] corresponding to RPR logical interface [STRING].
日志含义	站点的西向/东向边连接到了其它站点的西向/东向边
参数解释	$1：RPR环： ○ ringlet0：0 环 ○ ringlet1：1 环 $2：接口名称
日志等级	3 (Error)
举例	RPR/3/RPR_MISCABLING: A miscabling defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
对系统的影响	RPR环无法正常建立，影响环上的流量转发
日志产生原因	站点的西向/东向边连接到了其它站点的西向/东向边
处理建议	检查站点与其它站点间的RPR物理端口是否连接错误

142.14 RPR_MISCABLING_OVER

日志内容	A miscabling defect is cleared on [STRING] corresponding to RPR logical interface [STRING].
日志含义	站点与其它站点间的RPR物理端口连接正确
参数解释	$1：RPR环： ○ ringlet0：0 环 ○ ringlet1：1 环 $2：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_MISCABLING_OVER: A miscabling defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	站点与其它站点间的RPR物理端口连接正确
处理建议	系统正常运行时产生的信息，无需处理

142.15 RPR_PROTECTION_INCONSISTENT

日志内容	A protection configuration defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上至少两个站点间的保护模式配置不一致
参数解释	$1：接口名称
日志等级	3 (Error)
举例	RPR/3/RPR_PROTECTION_INCONSISTENT: A protection configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	影响保护倒换RPR环的流量切换，造成数据帧丢失
日志产生原因	RPR环上至少两个站点间的保护模式配置不一致
处理建议	找到保护模式配置不一致的站点，并修改其保护模式配置

142.16 RPR_PROTECTION_INCONSISTENT_OVER

日志内容	A protection configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点的保护模式配置一致
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_PROTECTION_INCONSISTENT_OVER: A protection configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上站点的保护模式配置一致
处理建议	系统正常运行时产生的信息，无需处理

142.17 RPR_SEC_MAC_DUPLICATE

日志内容	A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上至少两个站点间的次级MAC地址重复
参数解释	$1：接口名称
日志等级	3 (Error)
举例	RPR/3/RPR_SEC_MAC_DUPLICATE: A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上至少两个站点间的次级MAC地址重复
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

142.18 RPR_SEC_MAC_DUPLICATE_OVER

日志内容	A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环上站点的次级MAC地址不再相同
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_SEC_MAC_DUPLICATE_OVER: A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环上站点的次级MAC地址不再相同
处理建议	无需处理

142.19 RPR_TOPOLOGY_INCONSISTENT

日志内容	An inconsistent topology defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	站点上不同端口收集的拓扑信息不一致
参数解释	$1：接口名称
日志等级	3 (Error)
举例	RPR/3/RPR_TOPOLOGY_INCONSISTENT: An inconsistent topology defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	RPR环路异常，影响流量转发
日志产生原因	• RPR 环拓扑组网异常，例如连线异常 • 存在两个站点 MAC 地址重复
处理建议	检查RPR组网和拓扑连接，在链路上依次执行**shutdown**和**undo shutdown**命令，使站点重新收集拓扑信息

142.20 RPR_TOPOLOGY_INCONSISTENT_OVER

日志内容	An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	站点上不同端口收集的拓扑信息已一致
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_TOPOLOGY_INCONSISTENT_OVER: An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	站点上不同端口收集的拓扑信息已一致
处理建议	系统正常运行时产生的信息，无需处理

142.21 RPR_TOPOLOGY_INSTABILITY

日志内容	A topology instability defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环的拓扑不稳定
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	RPR/4/RPR_TOPOLOGY_INSTABILITY: A topology instability defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	影响环上流量转发
日志产生原因	RPR环链路出现问题，RPR环上协议报文转发存在丢包
处理建议	检查链路故障问题并处理

142.22 RPR_TOPOLOGY_INSTABILITY_OVER

日志内容	A topology instability defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	RPR环的拓扑已稳定
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_TOPOLOGY_INSTABILITY_OVER: A topology instability defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	RPR环链路恢复正常
处理建议	系统正常运行时产生的信息，无需处理

142.23 RPR_TOPOLOGY_INVALID

日志内容	A topology invalid defect is present on the ring corresponding to RPR logical interface [STRING].
日志含义	站点收集的拓扑信息无效
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	RPR/4/RPR_TOPOLOGY_INVALID: A topology invalid defect is present on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	RPR环路无效，影响环上流量转发
日志产生原因	RPR拓扑组网无效，没有正确组成环网
处理建议	检查RPR拓扑网络，确保正确组网，在链路上依次执行**shutdown**和**undo shutdown**命令，使站点重新收集拓扑信息

142.24 RPR_TOPOLOGY_INVALID_OVER

日志内容	A topology invalid defect is cleared on the ring corresponding to RPR logical interface [STRING].
日志含义	站点收集的拓扑信息有效
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	RPR/5/RPR_TOPOLOGY_INVALID_OVER: A topology invalid defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
对系统的影响	无
日志产生原因	正确组成RPR环网
处理建议	系统正常运行时产生的信息，无需处理

143 RRPP

本节介绍 RRPP 模块输出的日志信息。

143.1 RRPP_PEERLINK_CHECK

日志内容	An RRPP port can't be configured as a peer-link interface.
日志含义	RRPP环端口不能配置为peer-link接口
参数解释	无
日志等级	6 (Informational)
举例	RRPP/6/RRPP_PEERLINK_CHECK: An RRPP port can't be configured as a peer-link interface.
对系统的影响	RRPP环不能建立
日志产生原因	RRPP环端口不支持配置为peer-link接口
处理建议	将RRPP环端口配置为非peer-link接口

143.2 RRPP_RING_FAIL

日志内容	Ring [UINT32] in Domain [UINT32] failed.
日志含义	RRPP域下的环链路故障
参数解释	$1：环ID $2：域ID
日志等级	4 (Warning)
举例	RRPP/4/RRPP_RING_FAIL: Ring 1 in Domain 1 failed.
对系统的影响	网络拓扑改变，有可能引起业务流量丢失
日志产生原因	RRPP环的链路故障
处理建议	检测RRPP环的各个节点，清除网络故障

143.3 RRPP_RING_RESTORE

日志内容	Ring [UINT32] in Domain [UINT32] recovered.
日志含义	RRPP域下的环故障恢复
参数解释	$1：环ID $2：域ID
日志等级	4 (Warning)
举例	RRPP/4/RRPP_RING_RESTORE: Ring 1 in Domain 1 recovered.
对系统的影响	无
日志产生原因	RRPP环的链路恢复正常
处理建议	无需处理

144 RTM

本节介绍 EAA 的 RTM（Real-Time Management）模块输出的日志信息。

144.1 RTM_EMAIL_SUCCESS

日志内容	Succeed in sending an email with the subject [STRING] to [STRING].
日志含义	EAA自动发送邮件成功
参数解释	$1：邮件主题 $2：邮件接收者
日志等级	6 (Informational)
举例	RTM/6/RTM_EMAIL_SUCCESS: Succeed in sending an email with the subject Interface info to test1@example.com,test2@example.com.
对系统的影响	对系统无影响
日志产生原因	EAA自动发送邮件成功
处理建议	无需处理

144.2 RTM_EMAIL_FAILED

日志内容	Failed to send an email with the subject of [STRING] to [STRING], please check email domain, username password, max size and email server settings.
日志含义	EAA模块自动发送邮件失败
参数解释	$1：邮件主题 $2：邮件接收者
日志等级	4 (Warning)
举例	RTM/4/RTM_EMAIL_FAILED: Failed to send an email with subject of Interface info to test1@example.com, please check email domain, username password, max size and email server settings.
对系统的影响	对系统无影响
日志产生原因	EAA模块自动发送邮件失败，失败原因可能为： • 邮件超大 • 邮件配置不完全 • 设备与发送端邮件服务器之间路由不可达 • 发送端邮件服务器上的邮件服务不可用等
处理建议	请确认： • **rtm email max-size**命令配置的邮件大小限制是否合适 • **rtm email domain**、**rtm email username password**命令的配置是否正确 • Ping 发送端邮件服务器，确认发送邮件服务器是否路由可达 • 使用 NQA HTTP 探测发送端邮件服务器上的邮件服务是否可用 • 发送端邮件服务器上设置的参数是否和设备侧的邮件发送参数匹配 • 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

144.3 RTM_ENVIRONMENT

日志内容	Can't find environment variable [STRING].
日志含义	CLI监控策略替换环境变量时没有找到对应的环境变量
参数解释	$1：环境变量的名字
日志等级	4 (Warning)
举例	RTM/4/RTM_ENVIRONMENT: Can't find environment variable TestEnv.
对系统的影响	CLI监控策略执行失败
日志产生原因	未创建环境变量
处理建议	请在系统视图下使用**rtm environment**命令先创建环境变量再使用环境变量

144.4 RTM_TCL_LOAD_FAILED

日志内容	Failed to load the Tcl script file of policy [STRING].
日志含义	将Tcl监控策略对应的Tcl脚本文件加载到内存失败
参数解释	$1：Tcl监控策略的名称
日志等级	4 (Warning)
举例	RTM/4/RTM_TCL_LOAD_FAILED: Failed to load the Tcl script file of policy [STRING].
对系统的影响	Tcl监控策略不生效
日志产生原因	内存资源不足
处理建议	1. 释放内存。例如：执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源 2. 执行 **display memory**命令查看进程对内存的使用情况： o 如果内存占用率恢复到告警阈值以下，内存告警解除，则无需继续处理 o 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，可以开启或者关闭进程对应的软件功能，来释放内存 3. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

144.5 RTM_TCL_MODIFY

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file had been modified.
日志含义	Tcl监控策略执行失败
参数解释	$1：Tcl监控策略的名称
日志等级	4 (Warning)
举例	RTM/4/RTM_TCL_MODIFY: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file had been modified.
对系统的影响	Tcl监控策略执行失败
日志产生原因	Tcl监控策略对应的Tcl脚本文件被修改了
处理建议	确保Tcl监控策略对应的文件与注册文件相同或者重新创建Tcl监控策略

144.6 RTM_TCL_NOT_EXIST

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file was not found.
日志含义	Tcl监控策略执行失败
参数解释	$1：Tcl监控策略的名称
日志等级	4 (Warning)
举例	RTM/4/RTM_TCL_NOT_EXIST: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file was not found.
对系统的影响	Tcl监控策略执行失败
日志产生原因	Tcl监控策略触发执行时对应的Tcl脚本文件不存在
处理建议	执行**display current-configuration | include "rtm tcl-policy**"命令，查看Tcl监控策略绑定的Tcl脚本文件的名称以及路径，然后将备份的Tcl脚本文件拷贝到**rtm tcl-policy**命令中指定的路径，拷贝后的Tcl脚本文件名称必须和**rtm tcl-policy**命令中指定的Tcl脚本文件名称一致 如果不在需要使用该Tcl监控策略，可在系统视图下执行**undo rtm tcl-policy**命令删除该Tcl监控策略

145 SAVA

本节介绍 SAVA（Source Address Validation Architecture）模块输出的日志信息。

145.1 SAVA_SET_DRV_FAILED

日志内容	Failed to set the driver for enabling IPv6 SAVA on interface [STRING].
日志含义	SAVA功能下硬件驱动失败
参数解释	$1：接口名称
日志等级	5 (Notification)
举例	SAVA/5/SAVA_SET_DRV_FAILED: Failed to set the driver for enabling IPv6 SAVA on interface GigabitEthernet1/0/1.
对系统的影响	SAVA功能无法正常使用
日志产生原因	在接口上开启SAVA功能，功能下硬件驱动失败
处理建议	1. 请稍后在接口视图下重新执行一次 **ipv6 sava enable**命令 2. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

145.2 SAVA_SPOOFING_DETECTED

日志内容	Source IP address [STRING] spoofing packet detected : destination IP [STRING], protocol [STRING], source port [UNIT], destination port [UNIT] on interface [STRING].
日志含义	SAVA检测到了仿冒报文
参数解释	$1：仿冒的源IP地址 $2：目的IP地址 $3：IP报文协议号 $4：源端口号 $5：目的端口号 $6：接口名称
日志等级	6 (Informational)
举例	SAVA/6/SAVA_SPOOFING_DETECTED: Source IP address 2000::1 spoofing packet detected : destination IP 3000::2, protocol 6, source port 200, destination port 3000 on interface GigabitEthernet1/0/1.
对系统的影响	仿冒报文被丢弃
日志产生原因	SAVA检测到仿冒报文（非法主机仿冒合法用户IP）
处理建议	1. 检查报文发送者的合法性： ○ 如果报文确实非法，则无需处理 ○ 如果报文合法，请先执行 **undo ipv6 sava packet-drop enable**命令关闭SAVA丢弃仿冒报文功能，再通过输出的仿冒报文日志的具体内容，分析调整网络配置后再开启SAVA丢弃仿冒报文功能 2. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

146 SAVI

本节介绍 SAVI 模块输出的日志信息。

146.1 SAVI_FILTER_ENTRY_ADD

日志内容	Filter entry add with IP address [STRING], MAC [STRING] on interface [STRING] and VLAN [UINT32].
日志含义	新增SAVI过滤表项
参数解释	$1：IP地址 $2：MAC地址 $3：接口名称 $4：VLAN ID
日志等级	6 (Informational)
举例	SAVI/6/SAVI_FILTER_ENTRY_ADD: Filter entry add with IP address 3000::22, MAC 0011-0231-4520 on interface GigabitEthernet1/0/1 and VLAN 112.
对系统的影响	对系统无影响
日志产生原因	新增SAVI过滤表项
处理建议	无需处理

146.2 SAVI_FILTER_ENTRY_DEL

日志内容	Filter entry delete with IP address [STRING], MAC [STRING] on interface [STRING] and VLAN [UINT32].
日志含义	SAVI过滤表项被删除
参数解释	$1：IP地址 $2：MAC地址 $3：接口名称 $4：VLAN ID
日志等级	6 (Informational)
举例	SAVI/6/ SAVI_FILTER_ENTRY_DEL: Filter entry delete with IP address 3000::22, MAC 0011-0231-4520 on interface GigabitEthernet1/0/1 and VLAN 112.
对系统的影响	对系统无影响
日志产生原因	删除SAVI过滤表项
处理建议	无需处理

146.3 SAVI_SPOOFING_DETECTED

日志内容	Spoofing packet detected: source IP [STRING], MAC [STRING], destination IP [STRING], protocol [UINT32], source port [UINT32], destination port [UINT32], incoming interface [STRING], VLAN [UINT32].
日志含义	SAVI检测到了仿冒报文
参数解释	• $1：仿冒的源 IP 地址 • $2：源 MAC 地址 • $3：目的 IP 地址 • $4：IP 报文协议号 • $5：源端口号 • $6：目的端口号 • $7：接口名称 • $8：VLAN ID
日志等级	6 (Informational)
举例	SAVI/6/SAVI_SPOOFING_DETECTED: Spoofing packet detected: source IP 2000::1, MAC 0011-0231-4520, destination IP 3000::2, protocol 6, source port 299, destination port 399, incoming interface GigabitEthernet1/0/1, VLAN 40.
对系统的影响	系统可能受到仿冒报文攻击
日志产生原因	SAVI检测到仿冒报文（非法主机仿冒合法用户IP）
处理建议	检查报文发送者的合法性： • 如果报文确实非法，则无需处理 • 如果报文合法，则请收集配置文件、日志信息和告警信息，并联系技术支持

147 SCMD

本节介绍 SCMD（服务控制管理）模块输出的日志信息。

147.1 PROCESS_ABNORMAL

日志内容	The process [STRING] exited abnormally. ServiceName=[STRING], ExitCode=[STRING], KillSignal=[STRING], StartTime=[STRING], StopTime=[STRING].
日志含义	进程异常退出
参数解释	$1：进程名 $2：进程脚本里定义的服务名 $3：进程退出码，取值为： • 数字表示进程退出码 • NA 表示无退出码，进程被信号关闭 $4：关闭进程的信号，取值为： • 数字表示关闭进程的信号的数值 • NA 表示没有关闭信号，进程主动退出，并非被信号关闭 $5：进程的创建时间 $6：进程的关闭时间
日志等级	4 (Warning)
举例	SCMD/4/PROCESS_ABNORMAL: The process diagd exited abnormally. ServiceName=DIAG, ExitCode=1, KillSignal=NA, StartTime=2019-03-06 14:18:06, StopTime=2019-03-06 14:35:25.
对系统的影响	• 如果该进程有备进程，则对系统无影响 • 如果该进程无备进程，则设备不能提供该进程对应服务
日志产生原因	进程异常退出
处理建议	1. 通常情况下，进程异常退出后，会立即自动重启。可使用 **display process**命令查看进程是否存在。如果进程存在，则进程已恢复 2. 如果进程未恢复，请搜集以下信息： o 在 probe 视图下，执行 view /var/log/trace.log > trace.log，然后将设备存储目录下的 trace.log 文件通过 FTP 或 TFTP 功能，上传到服务器 o 联系工程师，将上述文件，发送给工程师进行分析，并保留现场，以便工程师进行进一步分析定位 3. 如果进程已恢复，但仍需要定位进程异常退出的原因，请执行（2） 备注：当使用FTP功能将文件上传到服务器时，请使用binary传输模式

147.2 PROCESS_ACTIVEFAILED

日志内容	The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
日志含义	备进程倒换成主进程失败，备进程重启
参数解释	$1：进程名
日志等级	4 (Warning)
举例	SCMD/4/PROCESS_ACTIVEFAILED: The standby process diagd failed to switch to the active process due to uncompleted synchronization, and was restarted.
对系统的影响	• 如果主进程还能继续工作，则对系统无影响 • 如果主进程无法继续工作程，则设备不能提供该进程对应服务
日志产生原因	备用进程还未完成同步时主进程意外退出，导致备进程倒换成主进程失败。备进程重启
处理建议	请收集告警信息和配置信息，并联系技术支持人员

147.3 PROCESS_CORERECORD

日志内容	Exceptions occurred with process [STRING]. A core dump file was generated.
日志含义	进程异常退出产生了core文件。core文件用于记录进程异常退出时的相关信息，以便定位
参数解释	$1：进程名
日志等级	4 (Warning)
举例	SCMD/4/PROCESS_CORERECORD: Exceptions occurred with process diagd. A core dump file was generated.
对系统的影响	• 如果该进程有备进程，则对系统无影响 • 如果该进程无备进程，则设备不能提供该进程对应服务
日志产生原因	进程异常退出
处理建议	1. 请使用 **display exception context**命令搜集进程异常信息，并将该异常信息保存到一个文件中 2. 通过 **display exception filepath**命令查看core文件目录，并通过FTP或TFTP功能，将core文件和记载了异常信息的文件上传到服务器 3. 联系工程师，将上述文件，发送给工程师进行分析，并保留现场，以便工程师进一步分析定位 当使用FTP功能将文件上传到服务器时，请使用binary传输模式

147.4 SCM_ABNORMAL_REBOOT

日志内容	形式一： The process [STRING] can't be restored. Reboot now. 形式二： The process [STRING] can't be restored. Reboot [STRING] now.
日志含义	• 进程恢复失败，立即重启
参数解释	形式一： $1：进程名 形式二： $1：进程名 $2：chassis编号+slot编号或slot编号
日志等级	3 (Error)
举例	SCMD/3/SCM_ABNORMAL_REBOOT: The process ipbased can't be restored. Reboot slot 2 now.
对系统的影响	• 如果该进程有备进程，则对系统无影响 • 如果该进程无备进程，则设备不能提供该进程对应服务
日志产生原因	形式一： 进程在设备启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则自动重启设备。 形式二： 进程在指定slot启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则系统会自动重启指定slot。
处理建议	1. 等单板重启后，使用 **display process**命令查看进程是否恢复 2. 若多次重启后仍不能恢复，请收集告警信息和配置信息，并联系技术支持人员

147.5 SCM_ABNORMAL_REBOOTMDC

日志内容	The process [STRING] in [STRING] [UINT16] can't be restored. Reboot [STRING] [UINT16] now.
日志含义	进程恢复失败，重启MDC或者Context
参数解释	$1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号 $4：取值为MDC或Context $5：MDC或Context的编号
日志等级	3 (Error)
举例	SCMD/3/SCM_ABNORMAL_REBOOTMDC: The process ipbased in MDC 2 can't be restored. Reboot MDC 2 now.
对系统的影响	MDC或者Context无法提供服务
日志产生原因	在主用主控板上的非缺省MDC启动过程中，或者在引擎组中主引擎上的Context启动过程中，进程异常退出，尝试自动重启多次后，仍不能恢复，则重启此MDC或Context。此日志在MDC 1或Context 1中输出
处理建议	1. 等单板重启后，使用 **display process**命令查看进程是否恢复 2. 若多次重启后仍不能恢复，请收集告警信息和配置信息，并联系技术支持人员

147.6 SCM_ABORT_RESTORE

日志内容	The process [STRING] can't be restored, abort it.
日志含义	进程在系统运行中异常退出，尝试自动重启多次后，仍不能恢复，系统放弃恢复该进程
参数解释	$1：进程名
日志等级	3 (Error)
举例	SCMD/3/SCM_ABORT_RESTORE: The process ipbased can't be restored, abort it.
对系统的影响	设备不能提供该进程对应服务
日志产生原因	进程在系统运行中异常退出，尝试自动重启多次后，仍不能恢复
处理建议	1. 任意视图下执行 **display process log**命令查看进程退出详细信息 2. 重启异常进程所在单板或 MDC，尝试恢复 3. 提供 **display process log**命令的显示信息，收集告警信息和配置信息，并联系技术支持人员

147.7 SCM_INSMOD_ADDON_TOOLONG

日志内容	Failed to finish loading [STRING] in [UINT32] minutes.
日志含义	设备启动过程中加载内核文件超时
参数解释	$1：内核文件的名称 $1：已加载时间
日志等级	4 (Warning)
举例	SCMD/4/SCM_INSMOD_ADDON_TOOLONG: Failed to finish loading addon.ko in 30 minutes.
对系统的影响	设备无法正常启动
日志产生原因	设备启动过程中加载内核文件超时
处理建议	**1.** 重启单板，尝试恢复 **2.** 如果问题仍未能解决，请收集告警信息和配置信息，并联系技术支持人员

147.8 SCM_KERNEL_INIT_TOOLONG

日志内容	Kernel init in sequence [STRING] function [STRING] failed to finish in [UINT32] minutes.
日志含义	内核初始化时，某个阶段某函数运行时间过长
参数解释	$1：内核事件的阶段 $2：内核事件阶段对应的函数的地址 $3：所用时间
日志等级	4 (Warning)
举例	SCMD/4/SCM_KERNEL_INIT_TOOLONG: Kernel init in sequence 0x25e7 function 0x6645ffe2 failed to finish in 15 minutes.
对系统的影响	设备无法正常启动
日志产生原因	内核初始化时，某个阶段某函数运行时间过长
处理建议	**1.** 重启单板，尝试恢复 **2.** 如果问题仍未能解决，请收集告警信息和配置信息，并联系技术支持人员

147.9 SCM_KILL_PROCESS

日志内容	形式一： The process [STRING] was killed because it failed to stop within [STRING]. 形式二： The process [STRING] on [STRING] [UINT16] was killed because it failed to stop within [STRING].
日志含义	某进程停止失败，系统强制结束该进程
参数解释	形式一： $1：进程名 $2：进程收到停止信号到打印该日志的时间 形式二： $1：进程名 $2：取值为MDC或context $3：MDC或context的编号 $4：进程收到停止信号到打印该日志的时间
日志等级	6 (Informational)
举例	SCMD/6/SCM_KILL_PROCESS: The process stamgrd was killed because it failed to stop within 30 minutes.
对系统的影响	设备不能提供该进程对应服务甚至导致设备无法正常运行
日志产生原因	某进程超过一定时间没按照指令正常停止，则系统会强制结束该进程
处理建议	1. 系统/MDC/Context稳定后，使用 **display process**命令查看进程是否恢复 2. 如果问题仍未能解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

147.10 SCM_PROCESS_HEALTHY

日志内容	Process [%s] is healthy.
日志含义	进程正常启动，进入健康状态
参数解释	$1：进程名
日志等级	6 (Informational)
举例	SCMD/6/SCM_PROCESS_HEALTHY: Process fsd is healthy.
对系统的影响	对系统无影响
日志产生原因	进程正常启动，进入健康状态
处理建议	无需处理

147.11 SCM_PROCESS_STARTING_TOOLONG

日志内容	The process [STRING] on [STRING] [UINT16] has not finished starting in [UINT32] hours.
日志含义	进程长时间未启动完成
参数解释	$1：进程名 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context的编号（不支持MDC或者Context的设备，不会输出该信息） $4：所用时间
日志等级	4 (Warning)
举例	SCMD/4/ SCM_PROCESS_STARTING_TOOLONG: The process ipbased on MDC 2 has not finished starting in 1 hours.
对系统的影响	设备不能提供该进程对应服务甚至导致设备无法正常运行
日志产生原因	配置太多导致进程启动慢，也可能是进程异常
处理建议	**1.** 大量配置的情况下，设备启动需要较长时间，如果等待 6 小时后，仍提示进程未完成启动，则可以认为进程已经异常 **2.** 重启单板/MDC/Context，尝试恢复。等单板/MDC/Context重启后，使用 **`display process`**命令查看进程是否恢复 **3.** 如果问题仍未能解决，请收集告警信息和配置信息，并联系技术支持人员

147.12 SCM_PROCESS_STILL_STARTING

日志内容	The process [STRING] on [STRING] [UINT16] is still starting for [UINT32] minutes.
日志含义	某进程一直处于启动状态
参数解释	$1：进程的名称 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context编号（不支持MDC或者Context的设备，不会输出该信息） $4：所用时间
日志等级	6 (Informational)
举例	SCMD/6/SCM_PROCESS_STILL_STARTING: The process ipbased on MDC 2 is still starting for 20 minutes.
对系统的影响	对系统无影响
日志产生原因	某进程一直处于启动状态
处理建议	正常运行信息，请继续关注。如果后续出现SCM_PROCESS_STARTING_TOOLONG日志，请参照SCM_PROCESS_STARTING_TOOLONG的处理建议处理

147.13 SCM_PROCESS_UNHEALTHY

日志内容	Process [%s] is unhealthy.
日志含义	进程启动超时，进入非健康状态
参数解释	$1：进程名
日志等级	4 (Warning)
举例	SCMD/4/SCM_PROCESS_UNHEALTHY: Process fsd is unhealthy.
对系统的影响	导致设备/板卡长时间处于启动状态
日志产生原因	设备/板卡启动过程中，有进程启动超时，进入非健康状态。进程处于非健康状态，会导致设备/板卡一直处于启动状态
处理建议	用户无需干预。系统会自动尝试继续启动进程。如果长时间（六小时后）不能正常启动进程，系统会忽略该进程，继续下一步操作

147.14 SCM_SKIP_PROCESS

日志内容	形式一： The process [STRING] was skipped because it failed to start within 6 hours. 形式二： The process [STRING] on [STRING] [UINT16] was skipped because it failed to start within 6 hours.
日志含义	进程超过6小时未启动完成，跳过该进程继续启动
参数解释	$1：进程名 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context的编号（不支持MDC或者Context的设备，不会输出该信息）
日志等级	3 (Error)
举例	SCMD/3/SCM_SKIP_PROCESS: The process ipbased was skipped because it failed to start within 6 hours.
对系统的影响	设备不能提供该进程对应服务
日志产生原因	单板/MDC/Context启动过程中，有进程超过6小时未启动完成，跳过该进程继续启动
处理建议	1. 重启单板/MDC/Context尝试恢复。等单板/MDC/Context重启后，使用 **display process**命令查看进程是否恢复 2. 如果问题仍未能解决，请收集告警信息和配置信息，并联系技术支持人员

148 SCRLSP

本节介绍静态 CRLSP 模块输出的日志信息。

148.1 SCRLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static CRLSP [STRING] is duplicate.
日志含义	静态CRLSP的入标签被占用
参数解释	$1：入标签值 $2：静态CRLSP名称
日志等级	4 (Warning)
举例	SCRLSP/4/SCRLSP_LABEL_DUPLICATE: Incoming label 1024 for static CRLSP aaa is duplicate.
对系统的影响	该静态CRLSP无法转发业务流量
日志产生原因	静态CRLSP的入标签被静态PW或者静态LSP占用。触发该日志的原因可能有： **1.** 在 MPLS 已使能的情况下，配置了一条入标签被静态 PW 或者静态 LSP 占用的静态 CRLSP **2.** 在入标签被静态 PW 或静态 LSP 占用的静态 CRLSP 存在的情况下，使能 MPLS
处理建议	删除该CRLSP，重新配置一条静态CRLSP，并指定一个新的入标签

149 SESSION

本节介绍 SESSION 模块输出的日志信息。

149.1 SESSION_DRV_EXCEED

日志内容	The number of session entries ([UINT32]) supported by hardware already reached.
日志含义	会话数达到产品硬件最大规格数
参数解释	$1：产品硬件支持的最大会话表项的数目
日志等级	2 (Critical)
举例	SESSION/2/SESSION_DRV_EXCEED: The number of session entries (65535) supported by hardware already reached.
对系统的影响	产生新的会话连接无法由硬件进行转发，若新的会话过多可能会消耗大量CPU利用率
日志产生原因	会话表项数目达到硬件支持的最大规格时会发送该日志
处理建议	无需处理

149.2 SESSION_DRV_RECOVERY

日志内容	Session resources supported by hardware had been released.
日志含义	会话数降低至产品硬件最大规格数以下
参数解释	无
日志等级	2 (Critical)
举例	SESSION/2/SESSION_DRV_RECOVERY: Session resources supported by hardware had been released.
对系统的影响	无
日志产生原因	会话表项资源从用尽状态恢复时会发送该日志
处理建议	无需处理

150 SFLOW

本节介绍 sFlow 模块输出的日志信息。

150.1 SFLOW_HARDWARE_ERROR

日志内容	Failed to [STRING] on interface [STRING] due to [STRING].
日志含义	执行流采样模式配置更新失败
参数解释	$1：流采样模式配置，显示为：update sampling mode $2：接口名 $3：失败的原因，目前只有不支持的操作一个原因，显示为：not supported operation
日志等级	4 (Warning)
举例	SFLOW/4/SFLOW_HARDWARE_ERROR: Failed to update sampling mode on interface GigabitEthernet1/0/1 due to not supported operation.
对系统的影响	无法下发新的流采样模式配置
日志产生原因	用户配置了设备不支持的流采样模式
处理建议	**1.** 将流采样模式配置修改为设备支持的模式 **2.** 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

151 SHELL

本节介绍 SHELL 模块输出的日志信息。

151.1 SHELL_CMD

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command is [STRING].
日志含义	用户执行过的命令
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**） $4：命令字符串
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User=**; Command is quit.
对系统的影响	无
日志产生原因	记录设备执行过的命令
处理建议	系统正常运行时产生的信息，无需处理

151.2 SHELL_CMD_CANCEL

日志内容	-Line=[STRING]-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] canceled to be executed. Result=Success.
日志含义	命令取消执行
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：用户名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $4：命令字符串 $5：执行命令的视图
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD_CANCEL: -Line=vty0-IPAddr=**-User=**; Command save in view system canceled to be executed. Result=Success.
对系统的影响	被取消执行的命令不会生效
日志产生原因	用户手工取消命令的执行
处理建议	无需处理

151.3 SHELL_CMD_CONFIRM

日志内容	Confirm option of command [STRING] is [STRING].
日志含义	对于需要确认的命令，记录用户的选择
参数解释	$1：命令字符串 $2：确认选项
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD_CONFIRM: Confirm option of command save is no.
对系统的影响	无
日志产生原因	记录需要用户确认命令的用户选择结果
处理建议	系统正常运行时产生的信息，无需处理

151.4 SHELL_CMD_EXECUTEFAIL

日志内容	-Line=[STRING]-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be executed.Result=Failed.
日志含义	记录执行失败的命令
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：用户名（如果不涉及该参数，显示为**） $3：IP地址（如果不涉及该参数，显示为**） $4：命令字符串 $5：执行命令的视图
日志等级	4 (Warning)
举例	SHELL/4/SHELL_CMD_EXECUTEFAIL: -Line=vty0-User=**-IPAddr=192.168.62.138; Command save in view system failed to be executed.Result=Failed.
对系统的影响	用户无法成功执行命令
日志产生原因	命令执行失败
处理建议	• 重新执行命令 • 检查执行命令的视图是否正确 • 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持

151.5 SHELL_CMD_EXECUTESUCCESS

日志内容	-Line=[STRING]-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] succeed to be executed. Result=Success.
日志含义	命令执行成功
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：用户名（如果不涉及该参数，显示为**） $3：IP地址（如果不涉及该参数，显示为**） $4：命令字符串 $5：执行命令的视图
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD_EXECUTESUCCESS: -Line=vty0-User=**-IPAddr=192.168.62.138; Command save in view system succeed to be executed. Result=Success.
对系统的影响	对系统无影响
日志产生原因	命令成功执行
处理建议	无需处理

151.6 SHELL_CMD_INPUT

日志内容	Input string for the [STRING] command is [STRING].
日志含义	用户执行命令后，为进行下一步操作所输入的信息
参数解释	$1：命令字符串 $2：输入字符串
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD_INPUT: Input string for the save command is startup.cfg. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is CTRL_C. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is the Enter key.
对系统的影响	对系统无影响
日志产生原因	当用户执行命令时，如果需要输入相关信息以进行下一步操作，则输入的字符内容将被记录，并产生日志信息 例如： • 在执行 **save**命令保存配置时，需要用户输入配置文件名和路径，用户输入的该信息将被记录 • 在执行 **save**命令保存配置时，需要用户输入配置文件名和路径，用户输入CTRL_C取消了保存配置操作，则该信息将被记录 • 在执行 **save**命令保存配置时，需要用户输入配置文件名和路径，用户输入回车，则该信息将被记录
处理建议	无需处理

151.7 SHELL_CMD_INPUT_TIMEOUT

日志内容	Operation timed out: Getting input for the [STRING] command.
日志含义	用户执行命令后，输入信息超时，导致无法继续进行下一步操作
参数解释	$1：命令字符串
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD_INPUT_TIMEOUT: Operation timed out: Getting input for the fdisk command.
对系统的影响	用户无法成功执行命令
日志产生原因	当用户执行命令时，如果需要输入额外信息确认操作，而用户在一定时间内未输入信息，则产生输入超时的日志信息
处理建议	重新执行命令，并及时输入为进行下一步操作所需要的信息

151.8 SHELL_CMD_INVALID_CHARACTER

日志内容	Execution failed for the [STRING] command. Reason: The command contains invalid characters (? or \t).
日志含义	指定命令执行失败
参数解释	$1：要执行的命令行
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMD_INVALID_CHARACTER: Execution failed for the sysname abc?? command. Reason: The command contains invalid characters (? or \t).
对系统的影响	该命令无法下发
日志产生原因	当设备使用文本类型的配置文件下发配置时，例如进行配置恢复或配置回滚时，如果配置文件中的命令行里包含无效字符“?”或“\t”，则输出此日志
处理建议	请用户根据需要，将命令行修改为正确形式，进行手动配置

151.9 SHELL_CMD_MATCHFAIL

日志内容	-Line=[STRING]-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be matched.Result=Failed.
日志含义	命令匹配失败
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：用户名（如果不涉及该参数，显示为**） $3：IP地址（如果不涉及该参数，显示为**） $4：命令字符串 $5：执行命令的视图
日志等级	4 (Warning)
举例	SHELL/4/SHELL_CMD_MATCHFAIL: -Line=vty0-User=**-IPAddr=192.168.62.138; Command description 10 in view system failed to be matched.Result=Failed.
对系统的影响	用户无法成功执行命令
日志产生原因	由于命令输入错误，或者当前模式错误等，造成命令匹配错误
处理建议	• 检查输入的命令是否准确完整 • 检查执行命令的视图是否正确 • 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持

151.10 SHELL_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command [STRING] is permission denied.Result=Failed.
日志含义	用户没有执行当前命令所需的权限
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**） $4：命令字符串
日志等级	5 (Notification)
举例	SHELL/5/SHELL_CMDDENY: -Line=vty0-IPAddr=192.168.62.138-User=**; Command vlan 10 is permission denied.Result=Failed.
对系统的影响	用户无法成功执行命令
日志产生原因	命令执行失败。用户权限不够
处理建议	检查用户是否具有执行该命令的权限

151.11 SHELL_CMDFAIL

日志内容	The [STRING] command failed to restore the configuration.
日志含义	恢复文本配置时，执行命令失败
参数解释	$1：命令字符串
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CMDFAIL: The “vlan 1024” command failed to restore the configuration.
对系统的影响	系统无法按指定的配置文件运行
日志产生原因	文本配置恢复操作失败
处理建议	• 确认配置文件是否为当前设备保存的配置文件 • 确认设备是否更换过板卡 • 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持

151.12 SHELL_COMMIT

日志内容	The configuration has been committed.
日志含义	配置成功提交
参数解释	无
日志等级	5 (Notification)
举例	SHELL/5/SHELL_COMMIT: The configuration has been committed.
对系统的影响	对系统无影响
日志产生原因	配置提交成功
处理建议	系统正常运行时产生的信息，无需处理

151.13 SHELL_COMMIT_DELAY

日志内容	A configuration rollback will be performed in [INT32] minutes.
日志含义	用户成功指定配置提交超时时间
参数解释	$1：用户指定的配置提交超时时间
日志等级	5 (Notification)
举例	SHELL/5/SHELL_COMMIT_DELAY: A configuration rollback will be performed in 3 minutes.
对系统的影响	超时系统将按提交前的配置运行
日志产生原因	用户指定配置提交超时时间成功
处理建议	请在超时时间内完成配置并提交，如果不能完成可以再次执行**configuration commit delay**命令延长时间

151.14 SHELL_COMMIT_REDELAY

日志内容	The commit delay has been reset, a configuration rollback will be performed in [INT32] minutes.
日志含义	配置提交超时时间已重置，请在新的配置回滚超时时间内提交
参数解释	$1：用户重新设置的超时时间
日志等级	5 (Notification)
举例	SHELL/5/SHELL_COMMIT_REDELAY: The commit delay has been reset, a configuration rollback will be performed in 3 minutes.
对系统的影响	超时系统将按提交前的配置运行
日志产生原因	用户在指定的超时时间之内再次配置超时时间，提示已经重置超时时间并显示当前超时时间
处理建议	请在用户指定的配置提交超时时间内完成配置并提交

151.15 SHELL_COMMIT_ROLLBACK

日志内容	The configuration commit delay is overtime, a configuration rollback will be performed.
日志含义	用户指定的配置提交超时时间超时未确认提交，触发配置回滚，系统将回滚到提交前的配置
参数解释	无
日志等级	5 (Notification)
举例	SHELL/5/SHELL_COMMIT_ROLLBACK: The configuration commit delay is overtime, a configuration rollback will be performed.
对系统的影响	系统回滚后，将按提交前的配置运行
日志产生原因	达到用户指定的配置提交超时时间后，进行配置回滚
处理建议	请在用户指定的配置提交超时时间内完成配置并提交

151.16 SHELL_COMMIT_ROLLBACKDONE

日志内容	The configuration rollback has been performed.
日志含义	用户指定的配置提交超时时间超时未确认提交，触发配置回滚，系统已回滚到提交前的配置
参数解释	无
日志等级	5 (Notification)
举例	SHELL/5/SHELL_COMMIT_ROLLBACKDONE: The configuration rollback has been performed.
对系统的影响	系统按提交前的配置运行
日志产生原因	配置回滚完成
处理建议	请在用户指定的配置提交超时时间内完成配置并提交

151.17 SHELL_COMMIT_WILLROLLBACK

日志内容	A configuration rollback will be performed in 1 minute. To retain the configuration you have made after executing the configuration commit delay command, execute the commit command.
日志含义	用户指定的配置提交超时时间超时未提交，配置回滚将在1分钟后进行。要保留开启配置延迟提交功能后所做的配置，请执行提交命令
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT_WILLROLLBACK: A configuration rollback will be performed in 1 minute. To retain the configuration you have made after executing the configuration commit delay command, execute the commit command.
对系统的影响	超时系统将按提交前的配置运行
日志产生原因	用户指定的配置提交超时时间超时前1分钟
处理建议	请在超时时间内完成配置并提交，如果不能完成可以再次执行**configuration commit delay**命令延长时间

151.18 SHELL_CRITICAL_CMDFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command is [STRING] .
日志含义	用户执行命令失败
参数解释	$1：用户名 $2：IP地址 $3：命令字符串
日志等级	6 (Informational)
举例	SHELL/6/SHELL_CRITICAL_CMDFAIL: -User=admin-IPAddr=169.254.0.7; Command is save.
对系统的影响	命令执行失败，仅FIPS模式支持
日志产生原因	命令执行失败
处理建议	• 请结合错误提示信息判断失败原因，采取相应处理 • 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持

151.19 SHELL_LOGIN

日志内容	[STRING] logged in from [STRING].
日志含义	用户登录成功
参数解释	$1：用户名 $2：用户线名
日志等级	5 (Notification)
举例	SHELL/5/SHELL_LOGIN: Console logged in from console0.
对系统的影响	无
日志产生原因	用户成功登录 用户线名为“local”时，表示用户登录到备用主控板自身
处理建议	系统正常运行时产生的信息，无需处理

151.20 SHELL_LOGOUT

日志内容	[STRING] logged out from [STRING], reason: [STRING].
日志含义	用户退出登录
参数解释	$1：用户名 $2：用户线名 $3：退出原因（仅FIPS模式下显示） • exit normally：正常退出 • time out：登录超时
日志等级	5 (Notification)
举例	SHELL/5/SHELL_LOGOUT: Console logged out from console0, reason: exit normally.
对系统的影响	对系统无影响
日志产生原因	用户退出登录 用户线名为“local”时，表示用户登录到备用主控板自身 FIPS模式下，显示用户退出登录的原因
处理建议	无需处理

152 SIMMGR

本节介绍 SIMMGR（Simulation Manage，仿真管理）模块输出的日志信息。

152.1 SIMMGR_LIC_EXPIRE

日志内容	Local license is about to expire in [INT32] days.
日志含义	本地License将要过期
参数解释	$1：本地License剩余有效期
日志等级	5 (Notification)
举例	SIMMGR/5/SIMMGR_LIC_EXPIRE: Local license is about to expire in 10 days.
对系统的影响	License授权的特性即将不可用
日志产生原因	本地License即将过期，从距离过期10天开始打印该日志
处理建议	请安装新的正式License，以免影响设备的正常使用

152.2 SIMMGR_NOLIC

日志内容	No license available. [STRING].
日志含义	无可用License
参数解释	$1：动作描述 The packet forwarding function will be disabled in [FLOAT] hours：即将停止报文转发功能 The packet forwarding function was disabled：已停止报文转发 The device will be rebooted in [FLOAT] minutes：即将重启设备 The device will be rebooted immediately：重启设备
日志等级	4 (Warning)
举例	SIMMGR/4/SIMMGR_NOLIC: No license available. The device will be rebooted immediately.
对系统的影响	License授权的特性不可用
日志产生原因	无可用License
处理建议	请安装License

152.3 SIMMGR_REMOTE_LIC_EXPIRE

日志内容	License requested from the license server is about to expire in [INT32] days.
日志含义	License Server获取到的授权即将过期
参数解释	$1：远程License剩余有效期
日志等级	5 (Notification)
举例	SIMMGR/5/SIMMGR_REMOTE_LIC_EXPIRE: License requested from the license server is about to expire in 10 days.
对系统的影响	License授权的特性即将不可用
日志产生原因	License Server获取到的授权即将过期，从距离过期10天开始打印该日志
处理建议	请安装新的正式License，以免影响设备的正常使用

153 SLSP

本节介绍静态 LSP 模块输出的日志信息。

153.1 SLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static LSP [STRING] is duplicate.
日志含义	静态LSP标签冲突
参数解释	$1：入标签值 $2：静态LSP名称
日志等级	4 (Warning)
举例	SLSP/4/SLSP_LABEL_DUPLICATE: Incoming label 1024 for static LSP aaa is duplicate.
对系统的影响	静态LSP不可用，无法基于该静态LSP转发流量
日志产生原因	静态LSP的入标签被静态PW、静态CRLSP或静态SRLSP占用。触发该日志的原因可能有： • 在 MPLS 已使能的情况下，配置了一条入标签被静态 PW、静态 CRLSP 或静态 SRLSP 占用的静态 LSP • 设备上已存在入标签被静态 PW、静态 CRLSP 或静态 SRLSP 占用的静态 LSP 的情况下，使能 MPLS
处理建议	删除该静态LSP，重新配置一条静态LSP，并指定一个新的入标签

154 SMARTMC

本节介绍 SMARTMC（Smart Management Center，智能管理中心）模块输出的日志信息。

154.1 ERROR

日志内容	Failed to set a password for device [UNIT].
日志含义	为成员设备配置密码失败
参数解释	$1：成员设备的ID
日志等级	3 (Error)
举例	SMARTMC/3/ERROR: Failed to set a password for device 10.
对系统的影响	TM将无法管理该TC
日志产生原因	执行**smartmc tc password**命令设置成员设备的密码失败
处理建议	• 执行 **display password-control**命令，查看显示信息中Password length、Password composition、Password complexity三个字段的取值，了解密码设置要求，重新设置密码 • 执行 **password-control length**、**password-control composition** 和 **password-control complexity**命令修改密码复杂度要求

155 SMLK

本节介绍 Smart Link 模块输出的日志信息。

155.1 SMLK_PORT_INACTIVE

日志内容	形式一： Not all the members in smart link group [UINT16] are M-LAG interfaces. 形式二： A peer-link interface can't be a member of a smart link group.
日志含义	形式一： 不是所有成员接口都是M-LAG接口 形式二： 成员接口不能为peer-link接口
参数解释	$1：Smart Link组ID
日志等级	4 (Warning)
举例	SMLK/4/SMLK_PORT_INACTIVE: -MDC=1; Not all the members in smart link group 1 are M-LAG interfaces.
对系统的影响	Smart Link组成员接口不生效
日志产生原因	形式一： Smart Link组成员接口为M-LAG接口与非M-LAG接口 形式二： Smart Link组成员接口为peer-link接口
处理建议	配置Smart Link组成员接口都为M-LAG接口或非M-LAG接口或非peer-link接口

155.2 SMLK_LINK_SWITCH

日志内容	Status of port [STRING] in smart link group [UINT16] changes to active.
日志含义	Smart Link组的端口变为转发状态
参数解释	$1：端口名称 $2：Smart Link组ID
日志等级	4 (Warning)
举例	SMLK/4/SMLK_LINK_SWITCH: Status of port GigabitEthernet0/1/4 in smart link group 1 changes to active.
对系统的影响	业务流量切换到当前端口
日志产生原因	另一个成员端口接替故障端口转发流量
处理建议	清除网络故障

156 SNMP

本节介绍 SNMP 模块输出的日志信息。

156.1 SNMP_ACL_RESTRICTION

日志内容	SNMP [STRING] from [STRING] is rejected due to ACL restriction.
日志含义	因为被ACL规则限制，NMS无法访问设备
参数解释	$1：SNMP 团体名/用户名/组名 $2：NMS的IP地址
日志等级	3 (Error)
举例	SNMP/3/SNMP_ACL_RESTRICTION: SNMP community public from 192.168.1.100 is rejected due to ACL restriction.
对系统的影响	NMS无法访问设备
日志产生原因	NMS的IP地址等参数未能匹配SNMP ACL
处理建议	请确认提示信息中NMS的IP地址是否为合法NMS的IP地址： • 如果 IP 地址为合法 NMS 的 IP 地址，则需要检查 ACL 的配置是否正确 • 请执行 **display snmp-agent community**命令查看日志中提示的SNMP团体名引用的ACL编号，执行 **display snmp-agent group**和 **display snmp-agent usm-user**命令查看日志中提示的SNMP用户名/组名引用的ACL编号；再执行 **display acl**命令查看ACL的内容。如果ACL的配置有误，请在ACL视图下，执行 **rule**命令修改ACL的过滤规则 • 如果 IP 地址为非法 NMS 的 IP 地址，则无需处理

156.2 SNMP_AUTHENTICATION_FAILURE

日志内容	Failed to authenticate SNMP message.
日志含义	NMS因为认证失败，无法访问设备（作为SNMP Agent）
参数解释	无
日志等级	4 (Warning)
举例	SNMP/4/SNMP_AUTHENTICATION_FAILURE: Failed to authenticate SNMP message.
对系统的影响	NMS无法访问设备
日志产生原因	NMS向设备发起SNMP请求，NMS未通过认证
处理建议	执行**display snmp-agent sys-info**命令查看设备使用的SNMP版本号，不同版本的SNMP支持的安全认证方式不同： • 对于SNMPv1 和SNMPv2c版本，SNMP协议不支持认证和加密，使用团体名进行安全认证，设备和NMS上使用的团体名必须一致。在设备上执行 **display snmp-agent community**命令查看设备使用的团体名，在NMS上使用相同的团体名访问设备即可，或者在设备上执行 **snmp-agent community**命令创建新的团体名，使团体名和NMS上使用的团体名一致 • 对于SNMPv3 版本，SNMP协议支持认证和加密，设备和NMS上必须使用相同的安全认证参数（包括用户名、是否进行认证、是否进行加密以及进行认证的认证密码、进行加密时的加密密码）。在设备上执行 **display snmp-agent group**和 **display snmp-agent usm-user**命令查看设备的安全认证参数，如果设备和NMS上使用的安全认证参数不同，请修改NMS上的安全认证参数，或者使用 **snmp-agent group**、**snmp-agent usm-user v3**命令修改认证参数

156.3 SNMP_GET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=GET-node=[STRING]-value=[STRING]; The agent received a message.
日志含义	设备收到NMS发送的Get请求报文
参数解释	$1：SNMP操作日志的序列号 $2：NMS的IP地址 $3：Get操作的MIB节点名及对应的OID $4：请求报文的取值字段
日志等级	6 (Informational)
举例	SNMP/6/SNMP_GET: -seqNO=1-srcIP=192.168.28.28-op=GET-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=; The agent received a message.
对系统的影响	对系统无影响
日志产生原因	设备开启了SNMP日志功能，且收到NMS发送的Get请求报文
处理建议	无需处理

156.4 SNMP_INFORM_LOST

日志内容	Inform failed to reach NMS through [STRING]: Inform [STRING][STRING].
日志含义	设备向NMS发送Inform报文失败 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
参数解释	$1：NMS主机地址及端口号 $2：告警名称及对应的OID $3：告警携带的MIB节点名称、OID及相应的值 o 如果告警未携带 MIB 节点，此参数部分不会出现 o 如果告警携带有 MIB 节点，此参数部分以“ with ”（空格 with 空格）开头，节点间以“;”（分号）作为分隔符
日志等级	3 (Error)
举例	SNMP/3/SNMP_INFORM_LOST: Inform failed to reach NMS through 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
对系统的影响	对系统无影响
日志产生原因	设备给NMS发送Inform报文，直到Inform报文超时仍未收到NMS的响应，日志产生原因可能有： • 原因一：NMS 路由不可达 • 原因二：NMS 的 SNMP 服务不可用 • 原因三：配置错误 • 原因四：设备到 NMS 的双向网络时延太大，超出了 Inform 报文的超时时间
处理建议	请根据不同原因，进行相应处理 • 针对原因一：根据日志信息中提示的NMS的IP地址，执行 **ping**命令。如果Ping失败，则说明NMS路由不可达，请先解决路由不可达问题 • 针对原因二：在设备上配置 NQA SNMP 测试，测试 NMS 服务是否可用。如果测试失败，请解决 NMS 的 SNMP 服务不可用问题 • 针对原因三：请执行 **display current-configuration | include "snmp-agent inform source"**命令，并查看显示信息： o 查看显示信息中的 **snmp-agent target-host inform**命令配置是否正确，NMS的IP地址、UDP端口号、VPN、SNMP版本号、安全认证参数都必须和NMS侧适配，否则，请执行 **snmp-agent target-host inform**命令修改 o 查看显示信息中是否存在 **snmp-agent inform source**命令为Inform报文配置了源接口。如果配置了源接口，则要求接口处于up状态，接口IP地址和NMS的IP地址可以路由可达。否则，需要解决源接口不可用问题或者切换源接口 • 针对原因四：对NMS执行Ping命令，查看双向延迟时间和丢包率，如果延迟时间过大（可通过 **snmp-agent trap periodical-interval**命令配置，缺省值为 60 秒）或者丢包率超过 20%，说明网络质量不好，请处理网络质量问题，或者切换到备份链路

156.5 SNMP_NOTIFY

日志内容	Notification [STRING][STRING].
日志含义	设备将产生的告警信息（Trap和Inform）以日志的形式在本地输出 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
参数解释	$1：告警名称及对应的OID $2：告警携带的MIB节点名称、OID及相应的值 o 如果告警未携带 MIB 节点，此参数部分不会出现 o 如果告警携带有 MIB 节点，此参数部分以“ with ”（空格 with 空格）开头，节点间以“;”（分号）作为分隔符
日志等级	6 (Informational)
举例	未拆分的日志举例： SNMP/6/SNMP_NOTIFY: Notification hh3cLogIn(1.3.6.1.4.1.25506.2.2.1.1.3.0.1) with hh3cTerminalUserName(1.3.6.1.4.1.25506.2.2.1.1.2.1.0)=;hh3cTerminalSource(1.3.6.1.4.1.25506.2.2.1.1.2.2.0)=Console. 被拆分的日志举例： SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=1; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgFacility(1.3.6.1.2.1.192.1.2.1.2.1)=23;syslogMsgSeverity(1.3.6.1.2.1.192.1.2.1.3.1)=6;syslogMsgVersion(1.3.6.1.2.1.192.1.2.1.4.1)=1;syslogMsgTimeStamp(1.3.6.1.2.1.192.1.2.1.5.1)=07-e2-04-12-12-26-35-00-00-00-2d-00-00[hex];syslogMsgHostName(1.3.6.1.2.1.192.1.2.1.6.1)=H3C;syslogMsgAppName(1.3.6.1.2.1.192.1.2.1.7.1)=SHELL;syslogMsgProcID(1.3.6.1.2.1.192.1.2.1.8.1)=-;syslogMsgMsgID(1.3.6.1.2.1.192.1.2.1.9.1)=SHELL_CMD;syslogMsgSDParams(1.3.6.1.2.1.192.1.2.1.10.1)=4;syslogMsgMsg(1.3.6.1.2.1.192.1.2.1.11.1)= Command is snmp-agent trap enable syslog;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.1.12.83.121.115.76.111.99.64.50.53.53.48.54.3.77.68.67)=1;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.2.12.65.112.112.76.111.99.64.50.53.53.48.54.4.76.105.110.101)=con0. SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=2; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.3.12.65.112.112.76.111.99.64.50.53.53.48.54.6.73.80.65.100.100.114)=**;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.4.12.65.112.112.76.111.99.64.50.53.53.48.54.4.85.115.101.114)=**.
对系统的影响	对系统无影响
日志产生原因	设备开启了SNMP告警日志功能，且设备发送告警信息给NMS
处理建议	无需处理

156.6 SNMP_SET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=SET-errorIndex=[UINT32]-errorStatus=[STRING]-node=[STRING]-value=[STRING]; The agent received a message.
日志含义	设备收到NMS发送的Set请求报文
参数解释	$1：SNMP操作日志的序列号 $2：NMS的IP地址 $3：Set操作的差错索引 $4：Set操作的差错状态 $5：Set操作的MIB节点名及对应的OID $6：Set操作设置的MIB节点的值
日志等级	6 (Informational)
举例	SNMP/6/SNMP_SET: -seqNO=3-srcIP=192.168.28.28-op=SET-errorIndex=0-errorStatus=noError-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=Hangzhou China; The agent received a message.
对系统的影响	对系统无影响
日志产生原因	设备开启了SNMP日志功能，且收到NMS发送的Set请求报文
处理建议	无需处理

156.7 SNMP_USM_NOTINTIMEWINDOW

日志内容	-User=[STRING]-IPAddr=[STRING]; SNMPv3 message is not in the time window.
日志含义	超时时间到达，设备仍未收到SNMPv3响应报文
参数解释	$1：用户名 $2：NMS的IP地址
日志等级	4 (Warning)
举例	SNMP/4/SNMP_USM_NOTINTIMEWINDOW: -User=admin-IPAddr=169.254.0.7; SNMPv3 message is not in the time window.
对系统的影响	对系统无影响
日志产生原因	超时时间到达，设备仍未收到SNMPv3响应报文
处理建议	**1.** 重新发送 SNMPv3 请求 **2.** 重连建立 SNMPv3 连接后，再重新发送 SNMPv3 请求。如果能收到对端的响应，则无需继续处理；否则，执行步骤 3 **3.** Ping 网管的 IP 地址。如果 Ping 失败，请先定位 Ping 不通问题 **4.** 检查网管侧的 SNMP server 能否正常工作。如果不能正常工作，请重启网管的 SNMP server 功能 **5.** 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

157 SOCKET

本节介绍 SOCKET 模块输出的日志信息。

157.1 SOCKET_TCP_UNREAD

日志内容	Data stays in the receive buffer for [INTEGER] secs. Owner=[STRING], VRF index=[INTEGER], local address/port=[STRING]/[INTEGER], remote address/port=[STRING]/[INTEGER], buffered sent bytes=[INTEGER], buffered received bytes=[INTEGER].
日志含义	TCP数据在接收缓冲区超过30秒未被读取
参数解释	$1：时间 $2：进程名 $3：VPN索引 $4：本地IP地址 $5：TCP本地端口 $6：对端IP地址 $7：TCP对端端口 $8：发送缓冲区的字节数 $9：接收缓冲区的字节数
日志等级	6 (Informational)
举例	SOCKET/6/SOCKET_TCP_UNREAD: Data stays in the receive buffer for 40 secs. Owner=bgpd, VRF index=0, local address/port=1.1.1.1/179, remote address/port=1.1.1.2/12345, buffered sent bytes=1000, buffered received bytes=50.
对系统的影响	无
日志产生原因	上层业务不活跃，两次读取TCP数据缓冲区的时间间隔超过30秒
处理建议	无需处理

158 SSHC

本节介绍 SSHC（SSH Client，SSH 客户端）模块输出的日志信息。

158.1 SSHC_ALGORITHM_MISMATCH

日志内容	The SSH client failed to log in because of [STRING] algorithm mismatch.
日志含义	SSH客户端和服务器端算法不匹配
参数解释	$1：算法类型： • encryption：加密算法 • key exchange：密钥交换算法 • MAC：HMAC 算法 • public key：主机签名算法
日志等级	5 (Notification)
举例	SSHC/5/SSHC_ALGORITHM_MISMATCH: The SSH client failed to log in because of encryption algorithm mismatch.
对系统的影响	SSH客户端无法正常登录服务器
日志产生原因	SSH客户端与服务器端算法不匹配
处理建议	修改算法，使SSH客户端和服务器使用相同类型的算法

158.2 SSHC_AUTH_PASSWORD_FAIL

日志内容	SSH user [STRING] failed to pass password authentication because of invalid username or wrong password.
日志含义	用户名无效或者密码错误导致认证失败
参数解释	$1：SSH用户名
日志等级	5 (Notification)
举例	SSHC/5/SSHC_AUTH_PASSWORD_FAIL: SSH user aaa failed to pass password authentication because of invalid username or wrong password.
对系统的影响	SSH用户登录失败
日志产生原因	• SSH 用户登录用户名无效或不存在 • SSH 用户登录密码错误
处理建议	**1.** 检查 SSH 登录用户名是否存在： o 如果不存在，请在 SSH 服务器上创建相应的 SSH 用户 o 如果存在，请执行步骤 2 或 3 **2.** 若服务器采用本地认证，请确认当前用户登录的密码是否与设备上设备管理类本地用户视图下配置的密码一致： o 如果不一致，请请重新输入正确的密码 o 如果一致，请执行步骤 4 **3.** 若服务器采用远程认证，请确认当前用户登录的密码是否与认证服务器上配置的一致： o 如果不一致，请重新输入正确的密码。若忘记密码，可以在服务器上为登录用户重新设置密码，确保登录密码与认证服务器上配置的一致。 o 如果一致，请执行步骤 4 **4.** 请收集配置文件、日志信息和告警信息，并联系技术支持

158.3 SSHC_AUTH_PUBLICKEY_FAIL

日志内容	SSH user [STRING] failed to pass publickey authentication.
日志含义	SSH用户没有通过公钥认证
参数解释	$1：SSH用户名
日志等级	5 (Notification)
举例	SSHC/5/SSHC_AUTH_PUBLICKEY_FAIL: SSH user abc failed to pass publickey authentication.
对系统的影响	SSH用户登录失败
日志产生原因	SSH服务器主机密钥与SSH客户端上缓存的密钥不匹配
处理建议	1. 检查服务器主机密钥与客户端上缓存的服务器主机密钥对是否一致： o 如果不一致，请在客户端上执行 **delete ssh client server-public-key** 命令，删除客户端保存的旧的服务端主机密钥 o 如果一致，请执行步骤 2 2. 请收集配置文件、日志信息和告警信息，并联系技术支持

158.4 SSHC_CERT_VERIFY_FAIL

日志内容	Failed to verify the certificate because [STRING].
日志含义	证书验证失败
参数解释	$1：失败原因： • null certificate：证书为空 • null certificate name：证书名字为空 • unable to get issuer certificate：获取颁发者证书失败 • unable to get certificate CRL：无法获取证书的 CRL • unable to decrypt CRL's signature：无法解密 CRL 的签名 • certificate signature failure：证书签名错误 • CRL signature failure：CRL 签名失败 • unable to decrypt certificate's signature：解密证书签名失败 • certificate is not yet valid：证书尚未生效 • certificate has expired：证书已失效 • CRL is not yet valid：CRL 尚未生效 • CRL has expired：CRL 已经失效 • format error in certificate's notBefore field：证书的起始时间格式错误 • format error in certificate's notAfter field：证书的结束时间格式错误 • format error in CRL's lastUpdate field：CRL 的上次更新时间格式错误 • format error in CRL's nextUpdate field：CRL 的下次更新时间格式错误 • out of memory：内存不足 • self signed certificate：自签名证书 • self signed certificate in certificate chain：证书链中存在自签名证书 • unable to verify the first certificate：验证首个证书失败 • certificate chain too long：证书链过长 • certificate revoked：证书被撤回 • invalid CA certificate：无效的 CA 证书 • invalid non-CA certificate (has CA markings)：无效的非 CA 证书 • path length constraint exceeded：超过路径深度约束 • proxy path length constraint exceeded：超过代理路径深度约束 • proxy certificates not allowed, please set the appropriate flag：代理证书不通过，请设置合适的标记 • unsupported certificate purpose：不支持的证书用途 • certificate not trusted：证书不被信任 • certificate rejected：证书被拒绝 • application verification failure：证书应用验证失败 • subject issuer mismatch：证书主题颁发者不匹配 • authority and subject key identifier mismatch：授权和主题密钥标识不匹配 • authority and issuer serial number mismatch：授权和颁发者序列号不匹配

	• key usage does not include certificate signing：密钥用途不包括证书签名 • unable to get CRL issuer certificate：获取 CRL 颁发者证书失败 • unhandled critical extension：不受控的决定性的扩展 • key usage does not include CRL signing：密钥用途不包括 CRL 签名 • key usage does not include digital signature：密钥用途不包括数字签名 • unhandled critical CRL extension：不受控的决定性的 CRL 扩展 • invalid or inconsistent certificate extension：无效或不一致的证书扩展 • invalid or inconsistent certificate policy extension：无效或不一致的证书策略扩展 • no explicit policy：不存在明确的策略 • Different CRL scope：CRL 范围不同 • CRL path validation error：CRL 路径检验失败 • unsupported or invalid name syntax：不支持的或无效的名字语法 • unsupported or invalid name constraint syntax：不支持的或无效的名字约束语法 • Suite B: certificate version invalid：Suite B：证书版本号无效 • Suite B: invalid public key algorithm：Suite B：无效的公钥算法 • Suite B: invalid ECC curve：Suite B：无效的 ECC 曲线 • Suite B: invalid signature algorithm：Suite B：无效的签名算法 • Suite B: curve not allowed for this LOS：Suite B：曲线不被本 LOS 准许 • Suite B: cannot sign P-384 with P-256：Suite B：不能使用 P-256 给 P-384 签名 • Invalid certificate verification context：无效的证书认证上下文 • Issuer certificate lookup error：颁发者证书查找失败 • proxy subject name violation：代理主题名称不规范
日志等级	5 (Notification)
举例	SSHC/5/SSHC_CERT_VERIFY_FAIL: Failed to verify the certificate because null certificate.
对系统的影响	SSH用户登录失败或者SSH用户掉线
日志产生原因	SSH客户端证书验证失败，具体原因见【参数解释】
处理建议	根据日志中具体提示的失败原因，进行相应处理

158.5 SSHC_CONNECT_FAIL

日志内容	The SSH client failed to connect to SSH server [STRING] port [UINT32].
日志含义	SSH客户端与服务器端建立连接失败
参数解释	$1：SSH服务器端IP地址 $2：SSH服务器的端口号
日志等级	5 (Notification)
举例	SSHC/5/SSHC_CONNECT_FAIL: The SSH client failed to connect to SSH server 1.1.1.1 port 2000.
对系统的影响	SSH用户登录失败
日志产生原因	• SSH 客户端与服务器端之间路由不通，无法建立 TCP 连接 • SSH 服务器端未开启 SSH 服务
处理建议	**1.** 检查客户端能否 Ping 通服务器端： o 如果 Ping 不通，请定位网络问题，确保 SSH 客户端能 Ping 通服务器端 o 如果 Ping 通，请执行步骤 2 **2.** 检查 SSH 服务器端是否开启 SSH 服务： o 如果未开启，请开启 o 如果已开启，请执行步骤 3 **3.** 请收集配置文件、日志信息和告警信息，并联系技术支持

158.6 SSHC_DECRYPT_FAIL

日志内容	The SSH client failed to use [STRING] to decrypt the packet received from the SSH server.
日志含义	解密SSH服务器端的报文失败
参数解释	$1：加密算法（比如aes256-cbc）
日志等级	5 (Notification)
举例	SSHC/5/SSHC_DECRYPT_FAIL: The SSH client failed to use aes256-cbc to decrypt the packet received from the SSH server.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	来自SSH服务器端的报文解密失败
处理建议	请SSH用户重新登录进行尝试，如果还不能解决，请收集配置文件、日志信息和告警信息，并联系技术支持

158.7 SSHC_DISCONNECT

日志内容	The SSH client was disconnected from the SSH server because the network was not available.
日志含义	SSH客户端与服务器由于网络问题断开连接
参数解释	无
日志等级	5 (Notification)
举例	SSHC/5/SSHC_DISCONNECT: The SSH client was disconnected from the SSH server because the network was not available.
对系统的影响	SSH用户登录失败或者登录掉线
日志产生原因	SSH客户端与服务器端之间网络存在问题
处理建议	请定位网络问题，确保SSH客户端能Ping通服务器端

158.8 SSHC_ENCRYPT_FAIL

日志内容	The SSH client failed to use [STRING] to encrypt the packet sent to the SSH server.
日志含义	SSH客户端发给SSH服务器的报文加密失败
参数解释	$1：加密算法（比如aes256-cbc）
日志等级	5 (Notification)
举例	SSHC/5/SSHC_ENCRYPT_FAIL: The SSH client failed to use aes256-cbc to encrypt the packet sent to the SSH server.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	发往SSH服务器的报文加密失败
处理建议	请SSH用户重新登录进行尝试，如果还不能解决，请收集配置文件、日志信息和告警信息，并联系技术支持

158.9 SSHC_HOST_NAME_ERROR

日志内容	The SSH server host name [STRING] is incorrect.
日志含义	指定的SSH服务器主机名错误
参数解释	$1：主机名
日志等级	5 (Notification)
举例	SSHC/5/SSHC_HOST_NAME_ERROR: The SSH server host name AAA is incorrect.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	SSH服务器主机名指定错误
处理建议	检查指定的SSH服务器主机名，确保主机名指定正确

158.10 SSHC_KEY_EXCHANGE_FAIL

日志内容	The SSH client failed to exchange keys with the SSH server.
日志含义	SSH客户端与SSH服务器端交换密钥失败
参数解释	无
日志等级	5 (Notification)
举例	SSHC/5/SSHC_KEY_EXCHANGE_FAIL: The SSH client failed to exchange keys with the SSH server.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	在密钥交换过程中出现错误

处理建议	以我司设备作为SSH服务器为例，通过**display ssh2 algorithm**命令查看当前SSH2协议使用的算法列表，检查客户端支持的算法是否包含在算法列表中：
	• 如果客户端使用的算法与服务器端上的算法不匹配，可通过如下两种方式进行修改：
	  ○ 服务器端可以通过执行 **ssh2 algorithm cipher**、**ssh2 algorithm key-exchange**、**ssh2 algorithm mac**或**ssh2 algorithm public-key**命令修改相关算法列表，增加客户端支持的算法；
	  ○ 客户端可添加服务端支持的相关算法
	• 如果客户端使用的算法与服务器端上的算法匹配，请收集配置文件、日志信息和告警信息，并联系技术支持

158.11 SSHC_MAC_ERROR

日志内容	The SSH client received from the SSH server a packet with incorrect message authentication code.
日志含义	SSH客户端校验SSH服务器端报文完整性失败
参数解释	无
日志等级	5 (Notification)
举例	SSHC/5/SSHC_MAC_ERROR: The SSH client received from the SSH server a packet with incorrect message authentication code.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	SSH客户端校验SSH服务器端报文完整性失败
处理建议	请SSH用户重新登录进行尝试，如果还不能解决，请收集配置文件、日志信息和告警信息，并联系技术支持

158.12 SSHC_PUBLICKEY_NOT_EXIST

日志内容	The public key of the SSH server does not exist.
日志含义	指定的服务器端公钥不存在
参数解释	无
日志等级	5 (Notification)
举例	SSHC/5/SSHC_PUBLICKEY_NOT_EXIST: The public key of the SSH server does not exist.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	用户登录过程中指定的服务器端公钥不存在
处理建议	以我司设备作为SSH服务器为例，通过在服务器上执行**display public-key peer**命令查看保存在设备上的客户端公钥信息，判断是否与正在登录用户使用的私钥类型一致： • 如果不一致，请执行 **public-key local create**命令在服务器上生成相应类型的密钥对 • 如果一致，请收集配置文件、日志信息和告警信息，并联系技术支持

158.13 SSHC_VERSION_MISMATCH

日志内容	The SSH client failed to log in because of version mismatch.
日志含义	SSH客户端版本与服务器端不兼容
参数解释	无
日志等级	5 (Notification)
举例	SSHC/5/SSHC_VERSION_MISMATCH: The SSH client failed to log in because of version mismatch.
对系统的影响	SSH客户端登录失败
日志产生原因	SSH客户端版本与服务器端不兼容
处理建议	检查服务器的SSH版本与客户端版本是否兼容，确保SSH客户端版本与服务器端兼容

159 SSHS

本节介绍 SSHS（SSH server，SSH 服务器）模块输出的日志信息。

159.1 SSHS_ACL_DENY

日志内容	The SSH Connection [IPADDR]([STRING]) request was denied according to ACL rules.
日志含义	SSH客户端的IP地址不在ACL定义的permit规则范围内
参数解释	$1：SSH客户端IP地址 $2：SSH客户端IP地址所在VPN
日志等级	5 (Notification)
举例	SSHS/5/SSH_ACL_DENY: The SSH Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
对系统的影响	SSH客户端登录失败
日志产生原因	设备上配置了对SSH客户端的访问控制，且客户端的IP地址不在ACL定义的permit规则范围内
处理建议	请确认该IP地址对应的用户是否为非法用户： • 如果是，则无需处理 • 如果不是，请修改 ACL 配置，使得客户端的 IP 地址在 ACL 的 permit 规则中

159.2 SSHS_ALGORITHM_MISMATCH

日志内容	SSH client [STRING] failed to log in because of [STRING] algorithm mismatch.
日志含义	SSH客户端和服务器端算法不匹配
参数解释	$1：SSH客户端IP地址 $2：算法类型： ○ encryption：加密 ○ key exchange：密钥交换 ○ MAC：MAC 算法 ○ public key：公钥
日志等级	6 (Informational)
举例	SSHS/6/SSHS_ALGORITHM_MISMATCH: SSH client 192.168.30.117 failed to log in because of encryption algorithm mismatch.
对系统的影响	SSH客户端登录失败
日志产生原因	SSH客户端和服务器端算法不匹配
处理建议	修改算法，使SSH客户端和服务器使用相同类型的算法

159.3 SSHS_AUTH_EXCEED_RETRY_TIMES

日志内容	SSH user [STRING] (IP: [STRING]) failed to log in, because the number of authentication attempts exceeded the upper limit.
日志含义	SSH用户认证尝试的最大次数达到上限
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_AUTH_EXCEED_RETRY_TIMES: SSH user David (IP: 192.168.30.117) failed to log in, because the number of authentication attempts exceeded the upper limit.
对系统的影响	系统可能在被非法用户攻击
日志产生原因	SSH用户认证尝试的最大次数达到上限
处理建议	**1.** 通过日志检查该用户是否为非法用户： ○ 如果是，请通过请修改 ACL 配置，使得非法客户端的 IP 地址不在 ACL 的 permit 规则中 ○ 如果不是，请联系管理员获取正确的用户名和密码。若告警依然存在，请执行步骤 2 **2.** 请收集配置文件、日志信息和告警信息，并联系技术支持

159.4 SSHS_AUTH_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass public key authentication for [STRING].
日志含义	SSH用户未通过publickey认证
参数解释	$1：用户名 $2：SSH客户端IP地址 $3：失败原因： • wrong public key algorithm：公钥算法错误 • wrong public key：公钥错误 • wrong digital signature：数字签名错误
日志等级	5 (Notification)
举例	SSHS/5/SSHS_AUTH_FAIL: SSH user David (IP: 192.168.30.117) didn't pass public key authentication for wrong public key algorithm.
对系统的影响	SSH客户端登录失败
日志产生原因	SSH用户没有通过公钥认证
处理建议	原因1：wrong public key algorithm 1. 检查 FIPS 模式下，SSH 客户端认证是否使用了 DSA 算法： o 如果是，请重新更换其他支持的算法。 o 如果不是，请收集配置文件、日志信息和告警信息，并联系技术支持。 原因2：wrong public key 2. 请通过 **display ssh user-information**命令检查指定的SSH用户是否配置了 **publickey**： o 如果没有，请通过 **ssh user**命令进行配置。 o 如果有，请执行步骤 2。 3. 请通过 **display public-key peer**命令查看已配置的 **publickey**是否与客户端上指定的一致： o 如果不一致，请将客户端上指定的 **publickey**导入到设备，并通过 **ssh user**命令配置给指定的用户。 o 如果一致，可能是由于 SSH 客户端的公钥和私钥不匹配，请在 SSH 客户端上重新生成密钥对。 4. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持。 原因3：wrong digital signature 5. 请检查服务器端 CA 证书和客户端本地证书的有效性。 6. 执行以上操作后，若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持。

159.5 SSHS_AUTH_KBDINT_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass keyboard-interactive authentication.
日志含义	SSH用户没有通过keyboard-interactive认证
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_AUTH_KBDINT_FAIL: SSH user David (IP: 192.168.30.117) didn't pass keyboard-interactive authentication.
对系统的影响	SSH用户登录失败（keyboard-interactive认证）
日志产生原因	SSH用户没有通过keyboard-interactive认证
处理建议	请SSH用户重新登录，如果问题还未解决，请收集配置文件、日志信息和告警信息，并联系技术支持

159.6 SSHS_AUTH_PWD_FAIL

日志内容	Authentication failed for user [STRING] from [STRING] port [INT32] because of invalid username or wrong password.
日志含义	用户名无效或者密码错误导致认证失败
参数解释	$1：用户名 $2：SSH客户端IP地址 $3：端口号
日志等级	6 (Informational)
举例	SSHS/6/SSHS_AUTH_PWD_LOG: Authentication failed for user David from 140.1.1.46 port 16266 because of invalid username or wrong password.
对系统的影响	SSH用户登录失败
日志产生原因	• SSH 用户登录用户名无效或不存在 • SSH 用户登录密码错误
处理建议	**1.** 检查 SSH 登录用户名是否存在： o 如果不存在，请在 SSH 服务器上创建相应的 SSH 用户 o 如果存在，请执行步骤 2 或 3 **2.** 若服务器采用本地认证，请确认当前用户登录的密码是否与设备上设备管理类本地用户视图下配置的密码一致： o 如果不一致，请请重新输入正确的密码 o 如果一致，请执行步骤 4 **3.** 若服务器采用远程认证，请确认当前用户登录的密码是否与认证服务器上配置的一致： o 如果不一致，请重新输入正确的密码。若忘记密码，可以在服务器上为登录用户重新设置密码，确保登录密码与认证服务器上配置的一致。 o 如果一致，请执行步骤 4 **4.** 请收集配置文件、日志信息和告警信息，并联系技术支持

159.7 SSHS_AUTH_SUCCESS

日志内容	SSH user [STRING] from [IPADDR] port [INTEGER] passed [STRING] authentication.
日志含义	SSH用户通过SSH认证
参数解释	$1：用户名 $2：用户IP地址 $3：TCP源端口 $4：认证方法，取值为keyboard-interactive、password和publickey
日志等级	6 (Informational)
举例	SSHS/6/SSHS_AUTH_SUCCESS: SSH user ABC from 1.1.1.1 port 55361 passed keyboard-interactive authentication.
对系统的影响	对系统无影响
日志产生原因	SSH用户认证通过
处理建议	无需处理

159.8 SSHS_AUTH_TIMEOUT

日志内容	Authentication timed out for [IPADDR].
日志含义	SSH用户认证超时
参数解释	$1：用户IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_AUTH_TIMEOUT: Authentication timed out for 1.1.1.1.
对系统的影响	SSH用户登录认证失败
日志产生原因	SSH用户在设置的认证超时时间内没有完成认证
处理建议	通过**display ssh server status**命令查看SSH用户认证超时时间是否设置过短： • 如果没有过短，请及时输入用户信息，完成认证 • 如果设置过短，请通过**ssh server authentication-timeout**命令将认证超时时间调大

159.9 SSHS_AUTHOR_FAIL

日志内容	Authorization failed for user [STRING] from [STRING] port [INT32].
日志含义	SSH用户授权失败
参数解释	$1：用户名 $2：SSH客户端IP地址 $3：端口号
日志等级	6 (Informational)
举例	SSHS/6/SSHS_AUTHOR_FAIL: Authorization failed for user David from 140.1.2.46 port 15000.
对系统的影响	SSH用户登录失败
日志产生原因	SSH用户授权失败
处理建议	检查本地用户配置或者认证服务器配置

159.10 SSHS_CERT_VERIFY_FAIL

日志内容	Failed to verify the certificate because [STRING].
日志含义	证书验证失败
参数解释	$1：失败原因： • null certificate：证书为空 • null certificate name：证书名字为空 • unable to get issuer certificate：获取颁发者证书失败 • unable to get certificate CRL：无法获取证书的 CRL • unable to decrypt CRL's signature：无法解密 CRL 的签名 • certificate signature failure：证书签名错误 • CRL signature failure：CRL 签名失败 • unable to decrypt certificate's signature：解密证书签名失败 • certificate is not yet valid：证书尚未生效 • certificate has expired：证书已失效 • CRL is not yet valid：CRL 尚未生效 • CRL has expired：CRL 已经失效 • format error in certificate's notBefore field：证书的起始时间格式错误 • format error in certificate's notAfter field：证书的结束时间格式错误 • format error in CRL's lastUpdate field：CRL 的上次更新时间格式错误 • format error in CRL's nextUpdate field：CRL 的下次更新时间格式错误 • out of memory：内存不足 • self signed certificate：自签名证书 • self signed certificate in certificate chain：证书链中存在自签名证书 • unable to verify the first certificate：验证首个证书失败 • certificate chain too long：证书链过长 • certificate revoked：证书被撤回 • invalid CA certificate：无效的 CA 证书 • invalid non-CA certificate (has CA markings)：无效的非 CA 证书 • path length constraint exceeded：超过路径深度约束 • proxy path length constraint exceeded：超过代理路径深度约束 • proxy certificates not allowed, please set the appropriate flag：代理证书不通过，请设置合适的标记 • unsupported certificate purpose：不支持的证书用途 • certificate not trusted：证书不被信任 • certificate rejected：证书被拒绝 • application verification failure：证书应用验证失败 • subject issuer mismatch：证书主题颁发者不匹配 • authority and subject key identifier mismatch：授权和主题密钥标识不匹配 • authority and issuer serial number mismatch：授权和颁发者序列号不匹配

	• key usage does not include certificate signing：密钥用途不包括证书签名 • unable to get CRL issuer certificate：获取 CRL 颁发者证书失败 • unhandled critical extension：不受控的决定性的扩展 • key usage does not include CRL signing：密钥用途不包括 CRL 签名 • key usage does not include digital signature：密钥用途不包括数字签名 • unhandled critical CRL extension：不受控的决定性的 CRL 扩展 • invalid or inconsistent certificate extension：无效或不一致的证书扩展 • invalid or inconsistent certificate policy extension：无效或不一致的证书策略扩展 • no explicit policy：不存在明确的策略 • Different CRL scope：CRL 范围不同 • CRL path validation error：CRL 路径检验失败 • unsupported or invalid name syntax：不支持的或无效的名字语法 • unsupported or invalid name constraint syntax：不支持的或无效的名字约束语法 • Suite B: certificate version invalid：Suite B：证书版本号无效 • Suite B: invalid public key algorithm：Suite B：无效的公钥算法 • Suite B: invalid ECC curve：Suite B：无效的 ECC 曲线 • Suite B: invalid signature algorithm：Suite B：无效的签名算法 • Suite B: curve not allowed for this LOS：Suite B：曲线不被本 LOS 准许 • Suite B: cannot sign P-384 with P-256：Suite B：不能使用 P-256 给 P-384 签名 • Invalid certificate verification context：无效的证书认证上下文 • Issuer certificate lookup error：颁发者证书查找失败 • proxy subject name violation：代理主题名称不规范
日志等级	5 (Notification)
举例	SSHS/5/SSHS_CERT_VERIFY_FAIL: Failed to verify the certificate because null certificate.
对系统的影响	SSH用户登录失败或者SSH用户掉线
日志产生原因	SSH客户端证书验证失败，具体原因见【参数解释】
处理建议	根据日志中提示的具体失败原因，进行相应处理

159.11 SSHS_CONNECT

日志内容	SSH user [STRING] (IP: [STRING]) connected to the server successfully.
日志含义	SSH用户成功登录SSH服务器
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_CONNECT: SSH user David (IP: 192.168.30.117) connected to the server successfully.
对系统的影响	对系统无影响
日志产生原因	SSH用户成功登录服务器
处理建议	无需处理

159.12 SSHS_DECRYPT_FAIL

日志内容	The packet from [STRING] failed to be decrypted with [STRING].
日志含义	解密SSH客户端的报文失败
参数解释	$1：SSH客户端IP地址 $2：加密算法（比如aes256-cbc）
日志等级	5 (Notification)
举例	SSHS/5/SSHS_DECRYPT_FAIL: The packet from 192.168.30.117 failed to be decrypted with aes256-cbc.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	来自SSH客户端的报文解密失败
处理建议	请SSH用户重新登录进行尝试，如果还不能解决，请收集配置文件、日志信息和告警信息，并联系技术支持

159.13 SSHS_DISCONNECT

日志内容	SSH user [STRING] (IP: [STRING]) disconnected from the server.
日志含义	SSH用户退出登录
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_DISCONNECT: SSH user David (IP: 192.168.30.117) disconnected from the server.
对系统的影响	对系统无影响
日志产生原因	SSH用户退出登录
处理建议	检查该SSH客户端是否为非法客户端： • 如果是，请通过请修改 ACL 配置，使得非法客户端的 IP 地址不在 ACL 的 permit 规则中，并修改该客户端所使用的用户认证配置 • 如果不是，无需处理

159.14 SSHS_ENCRYPT_FAIL

日志内容	The packet to [STRING] failed to be encrypted with [STRING].
日志含义	SSH服务器端发给客户端的报文加密失败
参数解释	$1：SSH客户端IP地址 $2：加密算法（比如aes256-cbc）
日志等级	5 (Notification)
举例	SSHS/5/SSHS_ENCRYPT_FAIL: The packet to 192.168.30.117 failed to be encrypted with aes256-cbc.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	发往SSH客户端的报文加密失败
处理建议	请SSH用户重新登录进行尝试，如果还不能解决，请收集配置文件、日志信息和告警信息，并联系技术支持

159.15 SSHS_LOG

日志内容	Authentication failed for user [STRING] from [STRING] port [INT32] because of invalid username or wrong password. Authorization failed for user [STRING] from [STRING] port [INT32].
日志含义	用户名无效或者登录密码错误导致认证失败 SSH用户授权失败
参数解释	$1：SSH客户端IP地址 $2：用户名 $3：端口号
日志等级	6 (Informational)
举例	SSHS/6/SSHS_LOG: Authentication failed for user David from 140.1.1.46 port 16266 because of invalid username or wrong password. SSHS/6/SSHS_LOG: Authorization failed for user David from 140.1.2.46 port 15000.
对系统的影响	SSH用户无法登录SSH服务器
日志产生原因	• SSH 用户名无效 • SSH 用户登录密码错误
处理建议	**1.** 检查用户名是否符合格式要求： o 如果不符合，请重新输入正确符合格式要求的用户名 o 如果符合，请执行步骤 2 **2.** 检查登录密码是否正确： o 如果不正确，请重新输入正确的密码。 o 如果正确，请执行步骤 3 **3.** 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

159.16 SSHS_MAC_ERROR

日志内容	SSH server received a packet with wrong message authentication code (MAC) from [STRING].
日志含义	SSH服务器端校验SSH客户端报文完整性失败
参数解释	$1：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_MAC_ERROR: SSH server received a packet with wrong message authentication code (MAC) from 192.168.30.117.
对系统的影响	可能导致SSH用户登录失败或者登录掉线
日志产生原因	SSH服务器端校验SSH客户端报文完整性失败
处理建议	请SSH用户重新登录进行尝试，如果还不能解决，请收集配置文件、日志信息和告警信息，并联系技术支持

159.17 SSHS_REACH_SESSION_LIMIT

日志内容	SSH client [STRING] failed to log in. The current number of SSH sessions is [NUMBER]. The maximum number allowed is [NUMBER].
日志含义	设备允许建立的SSH会话总数或各类SSH子会话总数达到了允许的最大值
参数解释	$1：SSH客户端IP地址 $2：SSH/Stelnet/SFTP/SCP/NETCONF $3：SSH会话总数或各类SSH子会话数（Stelnet/SFTP/SCP/NETCONF over SSH） $4：设备允许建立的SSH会话总数或各类SSH子会话总数（Stelnet/SFTP/SCP/NETCONF over SSH）
日志等级	6 (Informational)
举例	SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The current number of SSH sessions is 10. The maximum number allowed is 10.
对系统的影响	SSH客户端登录服务器端失败
日志产生原因	SSH客户端登录失败，SSH会话总数达到了最大值
处理建议	1. 通过执行 **aaa session-limit ssh**命令调大上限 2. 如果配置的最大用户连接数已为可配置的最大值，可将空闲的客户端下线，使得新的 SSH 用户能够上线 3. 若问题仍未解决，则请收集配置文件、日志信息和告警信息，并联系技术支持

159.18 SSHS_REACH_USER_LIMIT

日志内容	SSH client [STRING] failed to log in, because the number of users reached the upper limit.
日志含义	登录服务器的SSH用户数达到了允许用户数的上限
参数解释	$1：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_REACH_USER_LIMIT: SSH client 192.168.30.117 failed to log in, because the number of users reached the upper limit.
对系统的影响	SSH客户端登录失败
日志产生原因	SSH服务器上VTY用户数已达到允许用户数的上限
处理建议	通过**display users**命令查看处于空闲状态的用户线，再通过**free line vty**命令强制释放空闲的VTY用户线，使得新的SSH用户能够上线

159.19 SSHS_SCP_DISCONNECT

日志内容	SCP user [STRING] (IP: [STRING]) disconnected from the server, reason: [STRING].
日志含义	SCP客户端退出登录
参数解释	$1：用户名 $2：SCP客户端IP地址 $3：连接断开原因： • User logout：用户主动退出登录 • Forced logout by admin：管理员强制登录用户退出
日志等级	6 (Informational)
举例	SSHS/6/SSHS_SCP_DISCONNECT: SCP user David (IP: 192.168.30.117) disconnected from the server, reason: User logout.
对系统的影响	对系统无影响
日志产生原因	SCP客户端退出登录
处理建议	检查该SCP客户端是否为非法客户端： • 如果是，请通过请修改 ACL 配置，使得非法客户端的 IP 地址不在 ACL 的 permit 规则中，并修改该客户端所使用的用户认证配置 • 如果不是，无需处理

159.20 SSHS_SCP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
日志含义	SCP服务器收到SCP用户的请求操作
参数解释	$1：用户名称. $2：用户IP地址. $3：用户请求内容，包括文件操作信息 • get file "*name*"：下载名为 *name*的文件 • put file "*name*"：上传名为 *name*的文件
日志等级	6 (Informational)
举例	SSHS/6/SSHS_SCP_OPER: -MDC=1; User user1 at 1.1.1.1 requested operation: put file "aa".
对系统的影响	对系统无影响
日志产生原因	SCP服务器收到SCP用户请求执行相关操作
处理建议	无需处理

159.21 SSHS_SFTP_DISCONNECT

日志内容	SFTP user [STRING] (IP: [STRING]) disconnected from the server, reason: [STRING].
日志含义	SFTP客户端退出登录
参数解释	$1：用户名 $2：SFTP客户端IP地址 $3：连接断开原因： • User logout：用户主动退出登录 • Timeout：用户登录超时 • Forced logout by admin：管理员强制登录用户退出
日志等级	6 (Informational)
举例	SSHS/6/SSHS_SFTP_DISCONNECT: SFTP user David (IP: 192.168.30.117) disconnected from the server, reason: Timeout.
对系统的影响	对系统无影响
日志产生原因	SFTP客户端退出登录
处理建议	检查该SFTP客户端是否为非法客户端： • 如果是，请通过请修改 ACL 配置，使得非法客户端的 IP 地址不在 ACL 的 permit 规则中，并修改该客户端所使用的用户认证配置 • 如果不是，无需处理

159.22 SSHS_SFTP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
日志含义	SFTP服务器收到SFTP用户的请求操作
参数解释	$1：用户名称. $2：用户IP地址. $3：用户请求内容，包括文件操作和目录操作等信息 • open dir "*path*"：打开目录 *path* • open "*file*" (attribute code *code*) in *MODE* mode：在 *MODE*模式下，打开文件 *file*，该文件的属性代码为 *code* • remove file "*path*"：删除文件 *path* • mkdir "*path*" (attribute code *code*)：创建新目录 *path*，该目录的属性代码为 *code* • rmdir "*path*"：删除目录 *path* • rename old "*old-name*" to new "*new-name*"：改变旧文件或文件夹的名称 *old-name* 为 *new-name*
日志等级	6 (Informational)
举例	SSHS/6/SSHS_SFTP_OPER: User user1 at 1.1.1.1 requested operation: open dir "flash:/".
对系统的影响	对系统无影响
日志产生原因	SFTP服务器收到SFTP用户请求执行相关操作
处理建议	无需处理

159.23 SSHS_SRV_UNAVAILABLE

日志内容	The [STRING] server is disabled or the [STRING] service type is not supported.
日志含义	SSH服务不可用或者服务类型不支持
参数解释	$1：服务类型，包括Stelnet、SCP、SFTP、NETCONF
日志等级	6 (Informational)
举例	SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type is not supported.
对系统的影响	服务器正在断开连接，SSH用户登录SSH服务器失败
日志产生原因	Stelnet/SCP/SFTP/NETCONF over SSH服务不可用或者服务类型不支持
处理建议	1. 请检查对应的 SSH 服务类型是否开启： ○ 如果没开启，请开启相应的服务。 ○ 如果已开启，请执行步骤 2 2. 请在设备系统视图下执行 **ssh user**命令，修改SSH用户的服务类型与客户端类型相匹配

159.24 SSHS_VERSION_MISMATCH

日志内容	SSH client [STRING] failed to log in because of version mismatch.
日志含义	SSH服务器端版本与客户端不兼容
参数解释	$1：SSH客户端IP地址
日志等级	6 (Informational)
举例	SSHS/6/SSHS_VERSION_MISMATCH: SSH client 192.168.30.117 failed to log in because of version mismatch.
对系统的影响	对系统无影响
日志产生原因	SSH客户端和服务器的SSH版本号不匹配
处理建议	1. 请在设备上执行 **display ssh server status**命令查看SSH version字段确认SSH版本： ○ 如果 SSH version 显示为 1.99，则表示设备可以兼容 SSH1 版本的客户端，请执行步骤 2 ○ 如果SSH version显示为 2.0，请在设备上执行 **ssh server compatible-ssh1x enable**命令设置设备兼容SSH1 版本的客户端 2. 请收集配置文件、日志信息和告警信息，并联系技术支持

160 STAMGR

本节介绍 STAMGR 模块输出的日志信息。

160.1 STAMGR_ADD_FAILVLAN

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Added a user to the Fail VLAN [STRING].
日志含义	用户加入Fail-VLAN
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址 $3：用户加入的Fail-VLAN的VLAN ID
日志等级	5 (Notification)
举例	STAMGR/5/STAMGR_ADD_FAILVLAN:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Added a user to the Fail VLAN 5.
对系统的影响	无
日志产生原因	用户认证失败加入Fail-VLAN时，打印该日志
处理建议	无需处理

160.2 STAMGR_AUTHORACL_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign an ACL. Reason: [STRING].
日志含义	下发ACL失败
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址 $3：授权ACL失败的原因 • The ACL doesn't exist：指定的 ACL 不存在 • ACL type not supported：不支持指定的 ACL 类型 • Not enough hardware resources：内存不足 • The ACL conflicts with other ACLs：指定的 ACL 与其他 ACL 冲突 • The ACL doesn't contain any rules：指定 ACL 没有包含任何规则 • Unknown error：未知错误
日志等级	5 (Notification)
举例	STAMGR/5/STAMGR_AUTHORACL_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Failed to assign an ACL.Reason: The ACL doesn’t exist.
对系统的影响	无法授权指定ACL规则
日志产生原因	参见打印的授权ACL失败原因

处理建议	• 根据打印的失败原因修改 ACL 配置
	• 内存不足时，释放内存资源。例如，执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源，然后执行 **display memory**命令查看内存使用情况：
	  ◦ 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，可以开启或者关闭进程对应的软件功能，来释放内存
	  ◦ 如果内存占用率恢复到告警阈值以下，内存告警解除，Tcl 监控策略会继续生效，无需额外处理
	• 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

160.3 STAMGR_AUTHORUSERPROFILE_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign a user profile
日志含义	下发User Profile失败
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址
日志等级	5 (Notification)
举例	STAMGR/5/STAMGR_AUTHORUSERPROFILE_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Failed to assign a user profile
对系统的影响	无发授权指定User Profile
日志产生原因	内存不足或User Profile配置错误

处理建议	• 内存不足时，释放内存资源。例如，执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源，然后执行 **display memory**命令查看内存使用情况：
	  ○ 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，可以开启或者关闭进程对应的软件功能，来释放内存
	  ○ 如果内存占用率恢复到告警阈值以下，内存告警解除，Tcl 监控策略会继续生效，无需额外处理
	• 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

160.4 STAMGR_CLIENT_OFFLINE

日志内容	Client [STRING] went offline from BSS [STRING] with [STRING]. State changed to Unauth.
日志含义	客户端下线
参数解释	$1：客户端的MAC地址 $2：BSSID $3：服务模板的SSID
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_CLIENT_OFFLINE: Client 0023-8933-2147 went offline from BSS 0023-12ef-78dc with SSID abc. State changed to Unauth.
对系统的影响	无
日志产生原因	客户端在BSS下线，状态变为未认证状态
处理建议	• 若客户端主动下线，则不用排查问题 • 若客户端异常下线，需要查看 AP 和 Radio 是否处于正常工作状态，若有异常根据调试信息定位并解决问题

160.5 STAMGR_CLIENT_ONLINE

日志内容	Client [STRING] went online from BSS [STRING] with SSID [STRING]. State changed to Run.
日志含义	客户端上线
参数解释	$1：客户端的MAC地址 $2：BSSID $3：无线服务模板的SSID
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_CLIENT_ONLINE: Client 0023-8933-2147 went online from BSS 0023-12ef-78dc with SSID abc. State changed to Run.
对系统的影响	无
日志产生原因	客户端在BSS上线，状态变为运行状态时打印该日志
处理建议	无需处理

160.6 STAMGR_DOT1X_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication.
日志含义	用户802.1X认证失败
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID
日志等级	5 (Notification)
举例	STAMGR/5/STAMGR_DOT1X_LOGIN_FAILURE:-Username= Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11; A user failed 802.1X authentication.
对系统的影响	802.1X认证失败
日志产生原因	AAA服务器不可用、用户名或密码设置不正确
处理建议	• 检查设备与 AAA 服务器的网络连接是否正常 • 检查 AAA 服务器是否正常工作 • 检查用户名和密码设置是否和 AAA 服务器上的设置一致

160.7 STAMGR_DOT1X_LOGIN_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user passed 802.1X authentication and came online.
日志含义	用户802.1X认证成功
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_DOT1X_LOGIN_SUCC:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11; A user passed 802.1X authentication and came online.
对系统的影响	无
日志产生原因	用户通过802.1X认证
处理建议	无需处理

160.8 STAMGR_DOT1X_LOGOFF

日志内容	Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; Session for an 802.1X user was terminated.
日志含义	802.1X用户下线
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_DOT1X_LOGOFF:Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11; Session for an 802.1X user was terminated.
对系统的影响	无
日志产生原因	802.1X用户下线
处理建议	无需处理

160.9 STAMGR_MACA_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user failed MAC authentication.
日志含义	用户MAC地址认证失败
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID $5：用户名格式 • fixed：固定用户名格式 • MAC address：MAC 地址格式
日志等级	5 (Notification)
举例	STAMGR/5/STAMGR_MACA_LOGIN_FAILURE:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; A user failed MAC authentication.
对系统的影响	MAC地址认证不可用
日志产生原因	AAA服务器不可用、用户名或密码设置不正确
处理建议	• 检查设备与 AAA 服务器的网络连接是否正常 • 检查 AAA 服务器是否正常工作 • 检查用户名和密码设置是否和 AAA 服务器上的设置一致

160.10 STAMGR_MACA_LOGIN_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user passed MAC authentication and came online.
日志含义	用户MAC地址认证成功
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID $5：用户名格式 • fixed：固定用户名格式 • MAC address：MAC 地址格式
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_MACA_LOGIN_SUCC:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; A user passed MAC authentication and came online.
对系统的影响	无
日志产生原因	用户通过MAC地址认证
处理建议	无需处理

160.11 STAMGR_MACA_LOGOFF

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; Session for a MAC authentication user was terminated.
日志含义	MAC地址认证用户下线
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID $5：用户名格式 • fixed：固定用户名格式 • MAC address：MAC 地址格式
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_MACA_LOGOFF:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; Session for a MAC authentication user was terminated.
对系统的影响	无
日志产生原因	用户下线
处理建议	无需处理

160.12 STAMGR_STAIPCHANGE_INFO

日志内容	IP address of client [STRING] changed to [STRING].
日志含义	客户端更新IP地址
参数解释	$1：客户端的MAC地址 $2：客户端更新的IP地址
日志等级	6 (Informational)
举例	STAMGR/6/STAMGR_STAIPCHANGE_INFO: IP address of client 3ce5-a616-28cd changed to 4.4.4.4.
对系统的影响	无
日志产生原因	客户端更新IP地址
处理建议	无需处理

160.13 STAMGR_TRIGGER_IP

日志内容	-SSID=[STRING]-UserMAC=[STRING]-VLANID=[STRING]; Intrusion protection triggered, the intrusion protection action: [STRING].
日志含义	触发入侵检测，并显示入侵检测模式
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址 $3：用户上线的VLAN ID $4：入侵检测模式 • Added the user to the blocked MAC address list：将用户加入 Block-MAC 表中 • Closed the user's BSS temporarily：关闭用户所在 BSS 一段时间 • Closed the user's BSS permanently：永久关闭用户所在的 BSS
日志等级	5 (Notification)
举例	STAMGR/5/STAMGR_TRIGGER_IP:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-VLAN ID=11; Intrusion protection triggered, the intrusion protection action: added a user to the list of Block-MAC.
对系统的影响	无
日志产生原因	设备检测到一个未通过认证的用户试图访问网络
处理建议	无需处理

161 STM

本节介绍 STM（IRF）模块输出的日志信息。

161.1 STM_AUTO_UPDATE_FAILED

日志内容	形式一： Slot [UINT32] auto-update failed. Reason: [STRING]. 形式二： Chassis [UINT32] slot [UINT32] auto-update failed. Reason: [STRING].
日志含义	某设备加入IRF时，自动升级软件版本失败
参数解释	形式一： $1：成员设备编号 $2：失败原因： ○ Timeout when loading：加载超时 ○ Wrong description when loading：软件包中记录的文件描述信息和软件包当前的属性不一致 ○ Disk full when writing to disk：备设备存储介质上的空间不够 形式二： $1：成员设备编号 $2：主控板槽位号 $3：失败原因： ○ Timeout when loading：加载超时 ○ Wrong description when loading：软件包中记录的文件描述信息和软件包当前的属性不一致 ○ Disk full when writing to disk：主控板存储介质上的空间不够
日志等级	4 (Warning)
举例	STM/4/STM_AUTO_UPDATE_FAILED: Slot 5 auto-update failed. Reason: Timeout when loading.
对系统的影响	该设备无法加入IRF
日志产生原因	形式一： 在加入IRF时，设备从主设备自动加载启动软件包失败 形式二： 在加入IRF时，备用主控板从全局主用主控板自动加载启动软件包失败
处理建议	1. 如果失败原因为 Timeout when loading，请检查 IRF 链路是否畅通 2. 如果失败原因为 Wrong description when loading，可能是软件包被损坏了，请重新下载软件包 3. 如果失败原因为 Disk full when writing to disk，请先清理备设备的存储介质，删除一些暂时不用的文件 4. 请手动升级即将加入 IRF 的设备的软件包后，再将该设备和 IRF 相连

161.2 STM_AUTO_UPDATE_FINISHED

日志内容	形式一： File loading finished on slot [UINT32]. 形式二： File loading finished on chassis [UINT32] slot [UINT32].
日志含义	某设备加入IRF时，自动升级软件版本成功
参数解释	形式一： $1：成员设备编号 形式二： $1：成员设备编号 $2：主控板槽位号
日志等级	5 (Notification)
举例	STM/5/STM_AUTO_UPDATED_FINISHED: File loading finished on slot 3.
对系统的影响	对系统无影响
日志产生原因	形式一： 成员设备完成启动文件加载 形式二： 主控板完成启动文件加载
处理建议	无需处理

161.3 STM_AUTO_UPDATING

日志内容	形式一： Don't reboot the slot [UINT32]. It is loading files. 形式二： Don't reboot the chassis [UINT32] slot [UINT32]. It is loading files.
日志含义	
参数解释	形式一： $1：成员设备编号 形式二： $1：成员设备编号 $2：主控板槽位号
日志等级	5 (Notification)
举例	STM/5/STM_AUTO_UPDATING: Don't reboot the slot 2. It is loading files.
对系统的影响	
日志产生原因	形式一： 如果成员设备正在加载文件，请不要重启该设备 形式二： 如果主控板正在加载文件，请不要重启该主控板
处理建议	无需处理

161.4 STM_BRIDGE_MAC_CHANGE

日志内容	Bridge MAC on IRF member [UINT32] changed.
日志含义	IRF桥MAC地址变化
参数解释	$1：桥MAC变化的成员的编号
日志等级	5 (Notification)
举例	STM/5/STM_BRIDGE_MAC_CHANGE: Bridge MAC on IRF member 1 changed.
对系统的影响	对系统无影响
日志产生原因	IRF桥MAC地址变化，变成新主设备的桥MAC
处理建议	无需处理 如果不需要修改IRF桥MAC地址，可通过**irf mac-address persistent**命令修改桥MAC地址的变更时间

161.5 STM_HELLOPKT_NOTRCV

日志内容	Hello thread hasn't received packets for [UINT] seconds.
日志含义	Hello报文接收超时
参数解释	$1：时间值
日志等级	5 (Notification)
举例	STM/5/STM_HELLOPKT_NOTRCV: Hello thread hasn't received packets for 10 seconds.
对系统的影响	可能会导致IRF分裂
日志产生原因	Hello线程收包时间超过10秒，记录收包超时的时间
处理建议	检查IRF链路是否故障。登录本设备，执行**display irf link**命令，查看设备使用的IRF物理端口。针对这些物理端口可以进行以下处理： **1.** 确认对端设备是否正常运行。执行**display device**命令查看设备状态，如果设备处于非正常工作状态，请先定位设备故障 **2.** 在对端设备执行**display irf link**命令，查看对端IRF端口的配置是否正确。如果配置错误，请在IRF端口视图下，重新绑定IRF物理端口 **3.** 确保物理连线正确。本端IRF端口 1 需要和对端的IRF端口 2 连接，本端IRF端口 2 需要和对端的IRF端口 1 连接。两台设备组成的IRF系统，请使用链型拓扑，不要使用环形拓扑。确保物理连线正确后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **4.** 更换接口。在IRF端口视图下执行**port group interface**命令将IRF端口和其它物理端口绑定，并将IRF连线插入新绑定的物理端口。更换接口后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **5.** 更换网线或光纤。更换网线或光纤后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **6.** 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

161.6 STM_HELLOPKT_NOTSEND

日志内容	Hello thread hasn't sent packets for [UINT32] seconds.
日志含义	Hello报文发包超时
参数解释	$1：时间值
日志等级	5 (Notification)
举例	STM/5/STM_HELLOPKT_NOTSEND: Hello thread hasn't sent packets for 10 seconds.
对系统的影响	可能会导致IRF分裂
日志产生原因	Hello线程发包时间间隔超过10秒，记录发包超时时间
处理建议	1. 执行 **display cpu-usage**查看系统是不是暂时的CPU利用率增高，例如受到攻击或者处理其他较耗费CPU资源的任务 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

161.7 STM_LINK_DOWN

日志内容	IRF port [UINT32] went down.
日志含义	IRF端口状态变成down
参数解释	$1：IRF端口名
日志等级	3 (Error)
举例	STM/3/STM_LINK_DOWN: IRF port 2 went down.
对系统的影响	导致IRF分裂
日志产生原因	IRF端口绑定的所有物理端口都关闭了
处理建议	登录本设备，执行**display irf link**命令，查看设备使用的IRF物理端口。针对这些物理端口可以进行以下处理： 1. 确认对端设备是否正常运行。执行 **display device**命令查看设备状态，如果设备处于非正常工作状态，请先定位设备故障 2. 在对端设备执行 **display irf link**命令，查看对端IRF端口的配置是否正确。如果配置错误，请在IRF端口视图下，重新绑定IRF物理端口 3. 确保物理连线正确。本端IRF端口 1 需要和对端的IRF端口 2 连接，本端IRF端口 2 需要和对端的IRF端口 1 连接。两台设备组成的IRF系统，请使用链型拓扑，不要使用环形拓扑。确保物理连线正确后，再次执行 **display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 4. 更换接口。在IRF端口视图下执行 **port group interface**命令将IRF端口和其它物理端口绑定，并将IRF连线插入新绑定的物理端口。更换接口后，再次执行 **display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 5. 更换网线或光纤。更换网线或光纤后，再次执行 **display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 6. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

161.8 STM_LINK_TIMEOUT

日志内容	IRF port [UINT32] went down because the heartbeat timed out.
日志含义	由于IRF心跳检测超时，IRF端口关闭
参数解释	$1：IRF端口名
日志等级	2 (Critical)
举例	STM/2/STM_LINK_TIMEOUT: IRF port 1 went down because the heartbeat timed out.
对系统的影响	导致IRF分裂
日志产生原因	IRF心跳检测超时
处理建议	检查IRF链路是否故障。登录本设备，执行**display irf link**命令，查看设备使用的IRF物理端口。针对这些物理端口可以进行以下处理： **1.** 确认对端设备是否正常运行。执行**display device**命令查看设备状态，如果设备处于非正常工作状态，请先定位设备故障 **2.** 在对端设备执行**display irf link**命令，查看对端IRF端口的配置是否正确。如果配置错误，请在IRF端口视图下，重新绑定IRF物理端口 **3.** 确保物理连线正确。本端IRF端口 1 需要和对端的IRF端口 2 连接，本端IRF端口 2 需要和对端的IRF端口 1 连接。两台设备组成的IRF系统，请使用链型拓扑，不要使用环形拓扑。确保物理连线正确后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **4.** 更换接口。在IRF端口视图下执行**port group interface**命令将IRF端口和其它物理端口绑定，并将IRF连线插入新绑定的物理端口。更换接口后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **5.** 更换网线或光纤。更换网线或光纤后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 **6.** 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

161.9 STM_LINK_UP

日志内容	IRF port [UINT32] came up.
日志含义	IRF端口状态变成up
参数解释	$1：IRF端口名
日志等级	6 (Informational)
举例	STM/6/STM_LINK_UP: IRF port 1 came up.
对系统的影响	导致IRF合并
日志产生原因	IRF链路恢复
处理建议	无需处理

161.10 STM_LOGIC_PORT_LINK_ERR

日志内容	Link error detected on the IRF port. Reason: [STRING].
日志含义	堆叠建立时，发现IRF逻辑端口链接错误
参数解释	$1：导致逻辑端口链接错误的原因，取值包括： **1.** Both ends of a link are local physical interfaces：IRF 端口的物理连线出现了环路 **2.** The IRF-port contains links connected to two remote IRF-ports：本设备同一个 IRF 端口连接到了对端设备的两个不同 IRF 端口 **3.** The IRF-port contains links connected to different IRF member devices：本设备同一个 IRF 端口连接到了不同设备的 IRF 端口 **4.** The IRF-port contains links connected to non-IRF network ports：IRF 物理端口与对端设备的普通业务口相连 **5.** Inconsistent system-working-mode (if configurable) settings between peer devices or inconsistent switch-mode (if configurable) settings between peer IRF-connect cards：两端设备系统工作模式（如果可配置）设置不一致，或两端设备的交换机模式（如果可配置）设置不一致
日志等级	3 (Error)
举例	STM/3/STM_LOGIC_PORT_LINK_ERR: Link error detected on the IRF port. Reason: Both ends of a link are local physical interfaces.
对系统的影响	对系统无影响
日志产生原因	堆叠建立时，发现IRF逻辑端口链接错误
处理建议	**1.** 执行 **display irf link**和 **display irf topology**命令查看IRF端口的连接信息以及拓扑信息，确认IRF端口配置是否正确。本设备的IRF端口 1 只能和对端设备的IRF端口 2 连接，本设备的IRF端口 2 只能和对端设备的IRF端口 1 连接。当成员设备只有两台时，只支持链型拓扑，不支持环形拓扑 **2.** 根据提示的错误原因，正确地连接 IRF 端口 **3.** 如果问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持人员

161.11 STM_LOGIC_PORT_LINK_ERR_RECOVER

日志内容	Link error removed from the IRF port. Removed error: [STRING].
日志含义	IRF链接故障恢复正常
参数解释	$1：导致逻辑端口链接错误的原因
日志等级	3 (Error)
举例	STM/3/STM_LOGIC_PORT_LINK_ERR_RECOVER: Link error removed from the IRF port. Removed error: [STRING].
对系统的影响	对系统无影响
日志产生原因	IRF链接故障恢复正常
处理建议	无需处理

161.12 STM_MEMBER_JOIN

日志内容	IRF member [UINT32] added.
日志含义	IRF系统中有新成员加入
参数解释	$1：设备在IRF中的成员编号
日志等级	6 (Informational)
举例	STM/6/STM_MEMBER_JOIN: IRF member 1 added.
对系统的影响	对系统无影响
日志产生原因	IRF系统中有新成员加入
处理建议	无需处理

161.13 STM_MEMBER_LEAVE

日志内容	IRF member [UINT32] left.
日志含义	IRF系统中有成员离开
参数解释	$1：设备在IRF中的成员编号
日志等级	6 (Informational)
举例	STM/6/STM_MEMBER_LEAVE: IRF member 1 left.
对系统的影响	对系统无影响
日志产生原因	IRF系统中有成员离开
处理建议	• 如果是管理员主动将成员设备从 IRF 中移除，则无需处理 • 如果是成员设备突然离开，请检查该设备物理链路状态是否正常

161.14 STM_MEMBER_LIMIT

日志内容	The number of members has reached the limit ([UINT32]). No new members can be added.
日志含义	IRF系统成员设备的个数已经达到了产品支持的最大值，新设备加入失败
参数解释	$1：IRF系统阈值
日志等级	5 (Notification)
举例	STM/5/STM_MEMBER_LIMIT: The number of members has reached the limit (32). No new members can be added.
对系统的影响	对系统无影响
日志产生原因	IRF系统成员设备的个数已经达到了产品支持的最大值，再加入成员设备，打印该日志
处理建议	增加设备前，必须先移除一台成员

161.15 STM_MERGE

日志内容	IRF merge occurred.
日志含义	IRF合并事件发生
参数解释	无
日志等级	4 (Warning)
举例	STM/4/STM_MERGE: IRF merge occurred.
对系统的影响	对系统无影响
日志产生原因	IRF链路状态恢复到up
处理建议	无需处理

161.16 STM_MERGE_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system needs a reboot.
日志含义	IRF发生合并，本地IRF系统需要重启
参数解释	无
日志等级	4 (Warning)
举例	STM/4/STM_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
对系统的影响	本地IRF系统重启期间无法提供服务
日志产生原因	IRF链路状态恢复到up，导致IRF发生合并，且本地IRF系统在角色选举中失败
处理建议	重启本地IRF系统。本地IRF系统重启后，本地IRF系统的所有成员设备会以备设备的身份加入竞选成功的IRF系统中

161.17 STM_MERGE_NOT_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system does not need to reboot.
日志含义	IRF发生合并时，本地IRF系统无需重启
参数解释	无
日志等级	5 (Notification)
举例	STM/5/STM_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
对系统的影响	对系统无影响
日志产生原因	IRF链路状态恢复到up，导致IRF发生合并，且本地IRF系统在角色选举中成功
处理建议	无需处理

161.18 STM_PHY_DOWN

日志内容	Physical interface [STRING] of IRF port [UINT32] went down.
日志含义	IRF物理端口状态变为down
参数解释	$1：IRF物理端口名 $2：IRF端口名
日志等级	3 (Error)
举例	STM/3/STM_PHY_DOWN: Physical interface Ten-GigabitEthernet1/0/1 of IRF port 1 went down.
对系统的影响	导致IRF分裂
日志产生原因	IRF物理端口状态变为down
处理建议	登录本设备，执行**display irf link**命令，查看设备使用的IRF物理端口。针对这些物理端口可以进行以下处理： 1. 确认对端设备是否正常运行。执行**display device**命令查看设备状态，如果设备处于非正常工作状态，请先定位设备故障 2. 在对端设备执行**display irf link**命令，查看对端IRF端口的配置是否正确。如果配置错误，请在IRF端口视图下，重新绑定IRF物理端口 3. 确保物理连线正确。本端IRF端口 1 需要和对端的IRF端口 2 连接，本端IRF端口 2 需要和对端的IRF端口 1 连接。两台设备组成的IRF系统，请使用链型拓扑，不要使用环形拓扑。确保物理连线正确后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 4. 更换接口。在IRF端口视图下执行**port group interface**命令将IRF端口和其它物理端口绑定，并将IRF连线插入新绑定的物理端口。更换接口后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 5. 更换网线或光纤。更换网线或光纤后，再次执行**display irf link**命令，如果端口状态为Up，则说明故障被修复；如果端口状态不是Up，请继续定位 6. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

161.19 STM_PHY_UP

日志内容	Physical interface [STRING] of IRF port [UINT32] came up.
日志含义	IRF物理端口状态变为UP
参数解释	$1：IRF物理端口名 $2：IRF端口名
日志等级	6 (Informational)
举例	STM/6/STM_PHY_UP: Physical interface Ten-GigabitEthernet1/0/1 of IRF port 1 came up.
对系统的影响	导致IRF合并
日志产生原因	IRF物理端口状态变为UP
处理建议	IRF合并时，会进行Master设备竞选，竞选失败的IRF会打印日志STM_MERGE_NEED_REBOOT，请重启竞选失败的IRF。竞选失败的IRF重启后会自动和竞选成功的IRF合并

161.20 STM_PORT_LOOP_ALARM

日志内容	Traffic loop detected on IRF port [UINT32] on IRF member [UINT32].
日志含义	IRF端口出现报文环路现象
参数解释	$1：IRF端口编号 $2：成员编号
日志等级	5 (Notification)
举例	STM/5/STM_PORT_LOOP_ALARM: Traffic loop detected on IRF port 1 on IRF member 1.
对系统的影响	可能会出现报文风暴，导致正常报文无法及时被处理
日志产生原因	IRF端口出现报文环路现象，即该IRF端口发送出去的报文，再从该IRF端口回到本设备
处理建议	1. 执行 **display irf link**和 **display irf topology**命令查看IRF端口的连接信息以及拓扑信息，确认IRF端口配置是否正确。本设备的IRF端口 1 只能和对端设备的IRF端口 2 连接，本设备的IRF端口 2 只能和对端设备的IRF端口 1 连接。当成员设备只有两台时，建议采用链型拓扑 2. 确认 IRF 物理端口的连线是否符合网络规划拓扑，如果不符合，请重新连线 3. 如果问题仍未解决，请收集告警信息、日志信息和配置信息，并联系技术支持人员

161.21 STM_PORT_LOOP_ALARM_RECOVER

日志内容	Traffic loop removed on IRF port [UINT32] on IRF member [UINT32].
日志含义	IRF端口报文环路问题解除
参数解释	$1：IRF端口编号 $2：成员编号
日志等级	5 (Notification)
举例	STM/5/STM_PORT_LOOP_ALARM_RECOVER: Traffic loop removed on IRF port 1 on IRF member 1.
对系统的影响	对系统无影响
日志产生原因	IRF端口报文环路问题解除
处理建议	无需处理

161.22 STM_SAMEMAC

日志内容	Failed to stack because of the same bridge MAC addresses.
日志含义	新设备加入IRF时，因为桥MAC地址相同，无法加入IRF
参数解释	无
日志等级	4 (Warning)
举例	STM/4/STM_SAMEMAC: Failed to stack because of the same bridge MAC addresses.
对系统的影响	对系统无影响
日志产生原因	新设备和IRF中已有成员设备的桥MAC地址相同
处理建议	设备会出厂携带桥MAC地址，无法通过命令行修改。请收集告警信息和配置信息，并联系技术支持人员

161.23 STM_SET_UP_FAILED

日志内容	IRF stacking failed on device with member ID [UINT32].
日志含义	新设备加入IRF失败
参数解释	$1：加入IRF失败的设备编号
日志等级	3 (Error)
举例	STM/3/STM_SET_UP_FAILED: IRF stacking failed on device with member ID 1.
对系统的影响	对系统无影响
日志产生原因	新设备的硬件不符合IRF的要求，导致加入IRF失败。在加入失败的设备上打印该日志
处理建议	1. 检查成员设备的硬件是否符合 IRF 的要求 2. 请使用符合产品要求的硬件组建IRF，例如设备型号、主控板、接口板、IRF物理接口的类型必须符合要求。在设备上执行 **display version**命令可以通过如下方式查看当前设备的型号、主控板型号等，以判断设备硬件是否符合IRF要求 3. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

161.24 STM_SOMER_CHECK

日志内容	Neighbor of IRF port [UINT32] cannot be stacked.
日志含义	IRF口连接的设备无法加入本设备所在的IRF
参数解释	$1：IRF端口名
日志等级	3 (Error)
举例	STM/3/STM_SOMER_CHECK: Neighbor of IRF port 1 cannot be stacked.
对系统的影响	对系统无影响
日志产生原因	IRF口连接的设备无法加入本设备所在的IRF
处理建议	请检查以下事项： • 设备型号是否允许组成 IRF • IRF 配置是否正确 要获取更多信息，请参见该型号设备的IRF配置指导

162 STP

本节介绍生成树模块输出的日志信息。

162.1 STP_BLACK_HOLE_DISCARDING

日志内容	Port [STRING] set to discarding state due to black hole detected.
日志含义	端口的生成树工作状态被置为Discarding
参数解释	$1：接口名
日志等级	6 (Informational)
举例	STP/6/STP_BLACK_HOLE_DISCARDING: Port GigabitEthernet1/0/1 set to discarding state due to black hole detected.
对系统的影响	被置为Discarding状态的端口无法转发用户流量
日志产生原因	生成树黑洞探测功能在端口上检测到BPDU报文黑洞，阻塞该端口，将该端口的生成树工作状态置为Discarding
处理建议	无需处理，或修改物理拓扑以消除BPDU报文黑洞

162.2 STP_BLACK_HOLE_FORWARDING

日志内容	Port [STRING] set to forwarding state due to black hole eliminated.
日志含义	端口的生成树状态被置为Forwarding
参数解释	$1：接口名
日志等级	6 (Informational)
举例	STP/6/STP_BLACK_HOLE_DISCARDING: Port GigabitEthernet1/0/1 set to forwading state due to black hole eliminated.
对系统的影响	被置为Forwarding状态的端口可以正常转发用户流量
日志产生原因	被生成树黑洞探测功能阻塞的端口在经过**stp timer rx-blackhole-timeout**或**stp global timer rx-blackhole-timeout**命令指定的超时时间内，未再次收到生成树黑洞探测报文，则说明BPDU报文黑洞消除，该端口恢复正常转发状态
处理建议	无需处理，或修改物理拓扑以消除BPDU报文黑洞

162.3 STP_BPDU_PROTECTION

日志内容	BPDU-Protection port [STRING] received BPDUs.
日志含义	开启了BPDU保护功能的端口收到BPDU
参数解释	$1：接口名
日志等级	4 (Warning)
举例	STP/4/STP_BPDU_PROTECTION: BPDU-Protection port GigabitEthernet1/0/1 received BPDUs.
对系统的影响	该端口被设备关闭
日志产生原因	开启了BPDU保护功能的接口收到BPDU
处理建议	被关闭的端口在经过一定时间间隔之后将被重新激活，如果开启了BPDU保护功能的端口因为受到BPDU而频繁被关闭，请检查该端口上BPDU报文是否来自恶意攻击： • 如果是，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员 • 如果否，请在该端口上执行 **stp port bpdu-protection disable**命令关闭该端口的BPDU保护功能

162.4 STP_BPDU_RECEIVE_EXPIRY

日志内容	[STRING] [UINT32]'s port [STRING] received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
日志含义	非指定端口因在BPDU超时之前没有收到任何BPDU，端口状态发生改变
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	5 (Notification)
举例	STP/5/STP_BPDU_RECEIVE_EXPIRY: Instance 0's port GigabitEthernet1/0/1 received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
对系统的影响	生成树网络的拓扑发生变化
日志产生原因	端口对应的对端设备生成树功能未开启或与对端设备之间的链路发生故障
处理建议	1. 在通过该端口相连的对端设备上执行 **display stp**命令，检查该设备的生成树功能是否开启： ○ 如果是，请执行步骤 2 ○ 如果否，请在对端设备上通过 **stp global enable**命令以及 **stp enable**命令开启全局和端口上的生成树功能。对端设备开启生成树功能后若本端仍不能收到BPDU，请执行步骤 2 2. 检查本设备与对端设备间的链路是否存在故障： ○ 如果是，请修复设备间的链路故障，如果无法定位故障原因或无法自行修复链路故障，请执行步骤 3 ○ 如果否，请执行和步骤 3 3. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.5 STP_CONSISTENCY_CHECK

日志内容	M-LAG role assignment finished. Please verify that the local device and the peer device have consistent global and mlag-interface-specific STP settings.
日志含义	M-LAG设备角色已设定，请确保M-LAG系统中两台M-LAG设备上生成树全局和M-LAG接口上的配置一致
参数解释	无
日志等级	5 (Notification)
举例	STP/5/STP_CONSISTENCY_CHECK: M-LAG role assignment finished. Please verify that the local device and the peer device have consistent global and mlag-interface-specific STP settings.
对系统的影响	如果M-LAG系统中两台M-LAG设备上的生成树配置不一致，可能导致M-LAG系统无法正常运行
日志产生原因	设备上同时配置了M-LAG和生成树功能
处理建议	在M-LAG 系统的两台设备上均执行**display current-configuration**命令，查看两台设备的全局和M-LAG接口上的生成树配置是否一致： • 如果一致，则无需处理 • 如果不一致，则请在两台 M-LAG 设备上将生成树配置修改为一致

162.6 STP_CONSISTENCY_RESTORATION

日志内容	Consistency restored on VLAN [UINT32]'s port [STRING].
日志含义	PVID或端口类型不一致的保护状态解除
参数解释	$1：VLAN ID $2：接口名
日志等级	6 (Informational)
举例	STP/6/STP_CONSISTENCY_RESTORATION: Consistency restored on VLAN 10's port GigabitEthernet1/0/1.
对系统的影响	对系统无影响
日志产生原因	链路两端端口的PVID或端口类型变为一致
处理建议	无需处理

162.7 STP_DETECTED_TC

日志内容	[STRING] [UINT32]'s port [STRING] detected a topology change.
日志含义	端口所在实例或VLAN的生成树拓扑发生变化
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6 (Informational)
举例	STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.
对系统的影响	生成树拓扑发生变化，引发生成树协议重新计算
日志产生原因	设备上的端口状态发生变化
处理建议	检查拓扑变化是否正常： • 如果是，无需处理 • 如果否，请排查相关故障，恢复生成树拓扑。如果无法排查故障，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.8 STP_DISABLE

日志内容	STP is now disabled on the device.
日志含义	设备的全局生成树协议状态处于关闭状态
参数解释	无
日志等级	6 (Informational)
举例	STP/6/STP_DISABLE: STP is now disabled on the device.
对系统的影响	设备无法使用生成树功能，无法处理和发送BPDU
日志产生原因	用户执行**undo stp global enable**命令全局关闭生成树协议
处理建议	无需处理

162.9 STP_DISCARDING

日志内容	[STRING] [UINT32]'s port [STRING] has been set to discarding state.
日志含义	MSTP实例内的端口状态变为discarding
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6 (Informational)
举例	STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/0/1 has been set to discarding state.
对系统的影响	该端口无法转发用户流量
日志产生原因	MSTP实例内的端口所在的生成树拓扑发生变化
处理建议	1. 检查网络拓扑中的设备或链路是否发生变化： o 如果是，请执行步骤 2 o 如果否，请执行步骤 3 2. 查看网络拓扑中的设备或链路变化是否符合需要： o 如果是，请执行步骤 3 o 如果否，请指示步骤 4 3. 执行 **display stp**命令，查看当前各个端口的状态计算结果是否符合需要： o 如果是，则无需处理 o 如果否，请执行步骤 4 4. 请正确部署网络拓扑。如果正确部署网络拓扑后问题仍未解决，请执行步骤 5 5. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.10 STP_DISPUTE

日志内容	[STRING] [UINT32]'s port [STRING] received an inferior BPDU from a designated port which is in forwarding or learning state. The designated bridge ID contained in the BPDU is [STRING], and the designated port ID contained in the BPDU is [STRING].
日志含义	端口触发Dispute保护
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名 $4：低优先级BPDU携带的指定桥ID $5：低优先级BPDU携带的指定端口ID
日志等级	4 (Warning)
举例	STP/4/STP_DISPUTE: Instance 0's port GigabitEthernet1/0/2 received an inferior BPDU from a designated port which is in forwarding or learning state. The designated bridge ID contained in the BPDU is 32768.9a5c-5e0b-0300, and the designated port ID contained in the BPDU is 128.1293.
对系统的影响	触发Dispute保护的端口将被阻塞
日志产生原因	在生成树实例或VLAN内，端口收到了指定端口发出的低优先级BPDU报文，且发送端口处于Forwarding或Learning状态
处理建议	可通过如下方法进行处理： • 执行 **display stp abnormal-port**命令查看处于Dispute保护的阻塞端口信息。检查链路上是否存在对端接收不到本端所发报文的单通故障。确保两端的端口VLAN配置一致后，可以尝试down/up链路恢复或更换连线 • 根据接收到的低优先级报文携带的指定桥 ID 和指定端口 ID，排查设备与生成树拓扑中该 BPDU 所属的设备之间的链路 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.11 STP_DISPUTE_RESTORATION

日志内容	[STRING] [UINT32]'s port [STRING] exited the dispute state.
日志含义	在生成树实例或VLAN内，端口退出Dispute保护状态
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名称
日志等级	6 (Informational)
举例	STP/6/STP_DISPUTE_RESTORATION: Instance 0's port GigabitEthernet1/0/2 exited the dispute state.
对系统的影响	对系统无影响
日志产生原因	在生成树实例或VLAN内，端口从dispute状态恢复端口恢复收到正常优先级的BPDU，或用户手动执行**undo stp dispute-protection**命令关闭了Dispute保护功能
处理建议	无正常运行产生的日志信息，无需处理

162.12 STP_EDGEPORT_INACTIVE

日志内容	Port [STRING] became a non-edge port after receiving a BPDU.
日志含义	边缘端口收到BPDU报文，成为非边缘端口
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	STP/4/STP_EDGEPORT_INACTIVE: Port GigabitEthernet1/0/1 became a non-edge port after receiving a BPDU.
对系统的影响	生成树网络拓扑发生变化
日志产生原因	边缘端口收到了STPBPDU报文，成为了非边缘端口
处理建议	1. 检查是否有恶意用户伪造 BPDU 攻击网络判断该端口是否应该被规划为边缘端口： o 如果是，请执行步骤 2 o 如果否，请执行步骤 3 2. 判断该端口上收到的 BPDU 报文是否来自于恶意攻击： o 如果是，请执行步骤 4 o 如果否，请执行步骤 3 3. 在该端口下，执行 **undo stp edged-port**命令，将该端口配置为非边缘端口 4. 如果问题仍未解决，请收集日志打印信息和配置信息，并联系 H3C 技术支持工程师请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.13 STP_ENABLE

日志内容	STP is now enabled on the device.
日志含义	设备的全局生成树协议处于开启状态
参数解释	无
日志等级	6 (Informational)
举例	STP/6/STP_ENABLE: STP is now enabled on the device.
对系统的影响	部分端口可能会由于生成树协议的计算结果被阻塞
日志产生原因	设备上执行了**stp global enable**命令已开启全局的生成树协议
处理建议	无需处理

162.14 STP_FORWARDING

日志内容	[STRING] [UINT32]'s port [STRING] has been set to forwarding state.
日志含义	生成树实例内的端口变为Forwarding状态
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6 (Informational)
举例	STP/6/STP_FORWARDING: Instance 0's port GigabitEthernet1/0/1 has been set to forwarding state.
对系统的影响	对系统无影响
日志产生原因	网络拓扑发生变化
处理建议	1. 执行 **display stp**命令，查看当前各个端口的状态计算结果是否符合需要： ○ 如果是，则无需处理 ○ 如果否，请执行步骤 2 2. 请正确部署网络拓扑。如果正确部署网络拓扑后问题仍未解决，请执行步骤 3 3. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.15 STP_LOOP_PROTECTION

日志内容	[STRING] [UINT32]'s LOOP-Protection port [STRING] failed to receive configuration BPDUs.
日志含义	开启了环路保护功能的端口长时间未收到BPDU报文
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	4 (Warning)
举例	STP/4/STP_LOOP_PROTECTION: Instance 0's LOOP-Protection port GigabitEthernet1/0/1 failed to receive configuration BPDUs.
对系统的影响	开启了环路保护功能的端口将一直处于Discarding状态，直到收到BPDU
日志产生原因	原因一：开启了环路保护功能的端口的对端设备生成树功能未开启 原因二：开启了环路保护功能的端口链路发生故障
处理建议	1. 在通过该端口相连的对端设备上执行 **display stp**命令，检查该设备的生成树功能是否开启： o 如果是，请执行步骤 2 o 如果否，请在对端设备上通过 **stp global enable**命令以及 **stp enable**命令开启全局和端口上的生成树功能。对端设备开启生成树功能后若本端仍不能收到BPDU，请执行步骤 2 2. 检查本设备与对端设备间的链路是否存在故障： o 如果是，请修复设备间的链路故障，如果无法定位故障原因或无法自行修复链路故障，请执行步骤 3 o 如果否，请执行和步骤 3 3. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.16 STP_LOOPBACK_PROTECTION

日志内容	[STRING] [UINT32]'s port [STRING] received its own BPDU.
日志含义	设备上的端口触发自环保护
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	4 (Warning)
举例	STP/4/STP_LOOPBACK_PROTECTION: Instance 0's port GigabitEthernet1/0/2 received its own BPDU.
对系统的影响	网络中存在的环路可能造成广播风暴
日志产生原因	在生成树实例或VLAN中，端口收到自己发出的BPDU报文
处理建议	**1.** 检查是否有恶意用户伪造 BPDU 攻击网络： o 如果是，请执行步骤 3 o 如果否，请执行步骤 2 **2.** 检查网络中是否存在物理环路，如果存在，则请手动破除环路。如果问题仍未解决，请执行步骤 3 **3.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.17 STP_NOT_ROOT

日志内容	The current switch is no longer the root of instance [UINT32].
日志含义	设备不再是根桥角色
参数解释	$1：生成树实例编号
日志等级	5 (Notification)
举例	STP/5/STP_NOT_ROOT: The current switch is no longer the root of instance 0.
对系统的影响	设备角色重新计算，可能导致业务的短暂中断
日志产生原因	可能的原因包括： • 生成树的网络拓扑中新加入了根桥 ID 更小的设备 • 修改了原有生成树网络拓扑中的设备优先级

处理建议	对于生成树的网络拓扑中新加入了根桥ID更小的设备：
	1. 在新加入的设备上，执行 **display stp root**命令，查看该设备的根桥ID是否为最小的根桥ID：
	  ○ 如果是，请执行步骤 2
	  ○ 如果否，请执行步骤 4
	2. 请确认新加入设备的根桥 ID 是否应该规划为最小的根桥 ID：
	  ○ 如果是，则无需处理
	  ○ 如果否，请执行步骤 3
	3. 请修改新加入设备的优先级等配置，使得根桥角色变更为用户规划的设备。如果问题仍未解决，请执行步骤 4
	4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员
	对于修改了原有生成树网络拓扑中的设备优先级：
	5. 执行 **display stp**命令，查看生成树网络拓扑中的设备优先级修改配置是否正常：
	  ○ 如果是，则无需处理
	  ○ 如果否，请执行步骤 2
	6. 执行 **stp priority**命令将各设备的优先级修改为用户需要规划的值。如果问题仍未解决，请执行步骤 3
	7. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.18 STP_NOTIFIED_TC

日志内容	[STRING] [UINT32]'s port [STRING] was notified a topology change.
日志含义	生成树实例或VLAN中的端口收到对端设备发送的通知拓扑变化的通知
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6 (Informational)
举例	STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/0/1 was notified a topology change.
对系统的影响	生成树拓扑发生变化，引发生成树协议重新计算
日志产生原因	设备接收到TC标记置位的BPDU
处理建议	检查拓扑变化是否正常： • 如果是，无需处理 • 如果否，请排查相关故障，恢复生成树拓扑。如果无法排查故障，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.19 STP_PORT_TYPE_INCONSISTENCY

日志内容	Access port [STRING] in VLAN [UINT32] received PVST BPDUs from a trunk or hybrid port.
日志含义	端口收到了来自与本端口类型不一致的端口的BPDU
参数解释	$1：接口名 $2：VLAN ID
日志等级	4 (Warning)
举例	STP/4/STP_PORT_TYPE_INCONSISTENCY: Access port GigabitEthernet1/0/1 in VLAN 10 received PVST BPDUs from a trunk or hybrid port.
对系统的影响	由于Access端口与Trunk以及Hybrid端口发送的BPDU格式存在差别，可能导致生成树协议计算发生错误
日志产生原因	Access端口收到了来自Trunk或Hybrid端口发出的PVST格式的BPDU
处理建议	**1.** 检查日志指定的端口与其对端端口的类型是否一致： o 如果是，请执行步骤 2 o 如果否，请修改两端的端口类型为相同的类型。如果问题仍未解决，请执行步骤 2 **2.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.20 STP_PVID_INCONSISTENCY

日志内容	Port [STRING] with PVID [UINT32] received PVST BPDUs from a port with PVID [UINT32].
日志含义	端口收到了与本端口PVID不同的对端端口发布的BPDU
参数解释	$1：接口名 $2：VLAN ID $3：VLAN ID
日志等级	4 (Warning)
举例	STP/4/STP_PVID_INCONSISTENCY: Port GigabitEthernet1/0/1 with PVID 10 received PVST BPDUs from a port with PVID 20.
对系统的影响	PVST的计算可能出现错误
日志产生原因	本端端口与对端端口的PVID不一致
处理建议	请判断两端端口PVID不一致的情况是否符合网络的规划需求： • 如果是，请执行 **stp ignore-pvid-inconsistency**命令关闭PVST的PVID不一致保护功能 • 如果否，请将两端端口的 PVID 修改为一致

162.21 STP_PVST_BPDU_PROTECTION

日志内容	PVST BPDUs were received on port [STRING], which is enabled with PVST BPDU protection.
日志含义	在MSTP工作模式下，开启了PVST报文保护功能的端口收到了PVST报文
参数解释	$1：接口名
日志等级	4 (Warning)
举例	STP/4/STP_PVST_BPDU_PROTECTION: PVST BPDUs were received on port GigabitEthernet1/0/1, which is enabled with PVST BPDU protection.
对系统的影响	收到了PVST报文的端口被关闭
日志产生原因	在MSTP工作模式下，开启了PVST报文保护功能的端口收到了PVST报文

处理建议	1. 判断发布 PVST 报文的设备是否需要发布 PVST 报文：
	  ○ 如果是，则无需处理
	  ○ 如果否，请修改该设备上的配置，使其不再发布 PVST 报文。如果问题仍未解决，请执行步骤 2
	2. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.22 STP_ROOT_PROTECTION

日志内容	[STRING] [UINT32]'s ROOT-Protection port [STRING] received superior BPDUs.
日志含义	开启了根保护功能的端口收到了更高优先级的BPDU
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	4 (Warning)
举例	STP/4/STP_ROOT_PROTECTION: Instance 0's ROOT-Protection port GigabitEthernet1/0/1 received superior BPDUs.
对系统的影响	收到了更高优先级BPDU的端口转变为侦听状态，不再转发用户报文。当两倍的Forward Delay时间内没有收到更优的BPDU时，端口会恢复原来的正常状态
日志产生原因	生成树网络拓扑中加入了新的设备或者现有的设备发生了优先级变化
处理建议	1. 在生成树网络中的其他设备上执行 **display stp**命令，查看当前的各根桥计算结果以及各端口计算结果是否符合网络规划： ○ 如果是，请执行步骤 2 ○ 如果否，请执行步骤 3 2. 在开启了根保护功能的端口上执行 **undo stp root-protection**命令，关闭该端口的根保护功能。如果问题仍未解决，请执行步骤 4 3. 根据实际需要重新配置网络中各设备的优先级，使得开启了根保护功能的设备成为根桥设备。如果问题仍未解决，请执行步骤 4 4. 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

162.23 STP_STG_NUM_DETECTION

日志内容	STG count [UINT32] is smaller than the MPU's STG count [UINT32].
日志含义	检测到指定单板上的STG个数小于主控板上的STG个数
参数解释	$1：指定单板STG个数 $2：主控板STG个数
日志等级	4 (Warning)
举例	STP/4/STP_STG_NUM_DETECTION: STG count 64 is smaller than the MPU's STG count 65.
对系统的影响	生成树协议无法正常运行
日志产生原因	检测到指定单板上的STG个数小于主控板上的STG个数
处理建议	主控板上配置的STP实例个数不能大于所有单板的STG个数的最小值。例如：配置STP实例数是m，所有单板中，STG个数最小的一块单板的STG数是n，m不能大于n

163 SYSEVENT

本节介绍系统事件模块输出的日志信息。

163.1 EVENT_TIMEOUT

日志内容	Module [UINT32]'s processing for event [UINT32] timed out. Module [UINT32]'s processing for event [UINT32] on [STRING] timed out.
日志含义	应用模块处理事件超时
参数解释	$1：模块ID $2：事件ID $3：MDC *MDC-ID*或Context *Context-ID*
日志等级	6 (Informational)
举例	SYSEVENT/6/EVENT_TIMEOUT: -MDC=1; Module 0x1140000's processing for event 0x20000010 timed out. SYSEVENT/6/EVENT_TIMEOUT: -Context=1; Module 0x33c0000's processing for event 0x20000010 on Context 16 timed out.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	应用模块处理事件超时 非缺省MDC/Context上打印的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 缺省MDC/Context上打印的本MDC/Context的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 缺省MDC/Context上打印的其它MDC/Context的日志信息包含MDC *MDC-ID*或Context *Context-ID*
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

164 SYSLOG

本节包含 syslog（信息中心）模块输出的日志消息。

164.1 SYSLOG_LOGBUFFER_FAILURE

日志内容	Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
日志含义	日志无法输出到日志缓冲区，因为Syslog进程和DBM进程通信超时
参数解释	无
日志等级	4 (Warning)
举例	SYSLOG/4/SYSLOG_LOGBUFFER_FAILURE: Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
对系统的影响	日志缓冲区无法存储日志
日志产生原因	Syslog进程和DBM进程通信超时
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

164.2 SYSLOG_LOGFILE_CREATE

日志内容	Going to create new logfile [%s].
日志含义	设备将创建新的日志文件用于存储新的日志
参数解释	$1：日志文件的名称
日志等级	6 (Informational)
举例	SYSLOG/6/SYSLOG_LOGFILE_CREATE: Going to create new logfile flash:/logfile/logfile2.log.
对系统的影响	对系统无影响
日志产生原因	当前无日志文件或者现有的日志文件已经存满，设备需要创建新的日志文件用于存储新的日志
处理建议	无需处理

164.3 SYSLOG_LOGFILE_FULL

日志内容	Log file space is full.
日志含义	日志文件已满
参数解释	无
日志等级	4 (Warning)
举例	SYSLOG/4/SYSLOG_LOGFILE_FULL: Log file space is full.
对系统的影响	新日志无法存储到日志文件
日志产生原因	日志文件已满
处理建议	1. 备份日志文件后将日志文件删除 2. 执行 **undo info-center logfile overwrite-protection**命令关闭日志文件的写满保护功能，以便当日志文件被写满时，新日志可以覆盖保存到日志文件中 3. 执行 **info-center logfile size-quota**命令修改单个日志文件最大能占用的存储空间的大小

164.4 SYSLOG_LOGFILE_OVERWRITE

日志内容	The logfile [%s] will be overwritten.
日志含义	日志文件将要被覆盖写
参数解释	$1：日志文件的名称
日志等级	6 (Informational)
举例	SYSLOG/6/SYSLOG_LOGFILE_OVERWRITE: The logfile flash:/logfile/logfile.log will be overwritten.
对系统的影响	日志文件中时间最久远的日志将要被新日志覆盖
日志产生原因	日志文件已经写满，设备存储下一条日志时，将对日志文件进行覆盖操作
处理建议	请及时备份日志文件，以免旧日志被新日志覆盖。或者配置**info-center logfile overwrite-protection**命令开启日志文件的写满保护功能。如果日志文件的写满保护功能处于开启状态，则日志将从当前日志文件的尾部开始进行记录。在记录日志的过程中，如果日志文件的个数达到设备支持的最大值或者设备可用存储介质的空间不足，不再覆盖旧日志或删除最旧的日志文件，而是停止记录日志文件

164.5 SYSLOG_NO_SPACE

日志内容	Failed to save log file due to lack of space resources.
日志含义	存储介质空间不足，将日志保存到日志文件失败
参数解释	无
日志等级	4 (Warning)
举例	SYSLOG/4/SYSLOG_NO_SPACE: -MDC=1; Failed to save log file due to lack of space resources.
对系统的影响	新生成的日志无法保存到日志文件
日志产生原因	存储介质空间不足
处理建议	1. 请将日志文件备份到远程服务器 2. 使用 **delete /unreserved** *file*命令删除暂时不用的文件 3. 执行 **reset recycle-bin**命令清除回收站中的文件来清理存储介质上的存储空间

164.6 SYSLOG_RESTART

日志内容	System restarted -- [STRING] [STRING] Software.
日志含义	系统重启
参数解释	$1：公司名称 $2：软件名称
日志等级	6 (Informational)
举例	SYSLOG/6/SYSLOG_RESTART: System restarted -- H3C Comware Software.
对系统的影响	系统重启，设备无法工作
日志产生原因	重启设备
处理建议	无需处理

164.7 SYSLOG_RTM_EVENT_BUFFER_FULL

日志内容	In the last minute, [String] syslog logs were not monitored because the buffer was full.
日志含义	过去1分钟内，EAA监控的日志缓冲区被占满，有多条日志没来得及匹配便被丢弃了
参数解释	$1：过去1分钟内SYSLOG模块没有发送给EAA模块的日志的条数
日志等级	5 (Notification)
举例	SYSLOG/5/SYSLOG_RTM_EVENT_BUFFER_FULL: In the last minute, 100 syslog logs were not monitored because the buffer was full.
对系统的影响	可能会影响EAA监控策略的执行
日志产生原因	设备在短时间内产生大量日志，导致EAA监控的日志缓冲区被占满，有多条日志没来得及匹配便被丢弃了
处理建议	1. 执行 **display logbuffer**命令找到短时间内产生的大量日志，找到生成日志的业务模块，根据日志信息判断业务模块功能是否异常或者是否受到攻击，先解决业务模块异常问题或者被攻击问题，减少日志的生成 2. 使用 **rtm event syslog buffer-size**命令增大EAA监控的日志缓冲区的大小

164.8 SYSLOG_START

日志内容	System started --[STRING] Software.
日志含义	系统启动完成
参数解释	$1：公司名称
日志等级	6 (Informational)
举例	SYSLOG/6/SYSLOG_START: System started --*XXXX* Software
对系统的影响	对系统无影响
日志产生原因	系统启动完成（本日志的支持情况与设备的型号有关，请以设备的实际情况为准）
处理建议	无需处理

165 TACACS

本节介绍 TACACS 模块输出的日志信息。

165.1 TACACS_ACCT_SERVER_DOWN

日志内容	TACACS accounting server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	TACACS计费服务器状态为阻塞
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4 (Warning)
举例	TACACS/4/TACACS_ACCT_SERVER_DOWN: TACACS accounting server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	服务器不可达，用户上线失败
日志产生原因	设备发现TACACS计费服务器状态从active变为block
处理建议	**1.** 执行命令 **`display interface`**检查连接TACACS计费服务器的接口是否为UP。 o 如果是，请执行步骤 2。 o 如果否，请检查物理链路的连接，确保物理链路连接正常。 **2.** 执行命令 **`ping`**检查TACACS计费服务器是否可达。 o 如果是，请执行步骤 3。 o 如果否，请首先检查设备与 TACACS 计费服务器之间的网络可达性，然后排查网络中是否存在防火墙等设备，确保 TACACS 计费服务器可达。 **3.** 执行命令 **`display current-configuration`**检查设备上TACACS计费服务器配置是否正确。 o 如果是，请执行步骤 4。 o 如果否，请参考《AAA 命令参考》、《AAA 配置指导》手册修改 TACACS 计费服务器的配置。 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

165.2 TACACS_ACCT_SERVER_UP

日志内容	TACACS accounting server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	TACACS计费服务器状态变为激活
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6 (Informational)
举例	TACACS/6/TACACS_ACCT_SERVER_UP: TACACS accounting server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	对系统无影响
日志产生原因	设备发现TACACS计费服务器状态从block变为active
处理建议	系统正常运行时产生的信息，无需处理

165.3 TACACS_AUTH_FAILURE

日志内容	User [STRING] at [STRING] failed authentication.
日志含义	TACACS认证失败
参数解释	$1：用户名称 $2：IP地址
日志等级	5 (Notification)
举例	TACACS/5/TACACS_AUTH_FAILURE: User cwf@system at 192.168.0.22 failed authentication.
对系统的影响	用户认证失败
日志产生原因	TACACS服务器了拒绝用户的认证请求
处理建议	**1.** 检查设备上的 TACACS 认证相关配置，并联系服务器管理员确认拒绝认证请求的原因，根据具体原因解决。 **2.** 用户重新发起认证后，如果此日志依然存在，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

165.4 TACACS_AUTH_SERVER_DOWN

日志内容	TACACS authentication server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	TACACS认证服务器状态为阻塞
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4 (Warning)
举例	TACACS/4/TACACS_AUTH_SERVER_DOWN: TACACS authentication server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	会导致用户上线认证失败，如果没有备份认证服务器可能造成用户下线
日志产生原因	设备发现TACACS认证服务器状态从active变为block
处理建议	**1.** 执行命令 **`display interface`**检查连接TACACS认证服务器的接口是否为UP。 o 如果是，请执行步骤 2。 o 如果否，请检查物理链路的连接，确保物理链路连接正常。 **2.** 执行命令 **`ping`**检查TACACS认证服务器是否可达。 o 如果是，请执行步骤 3。 o 如果否，请首先检查设备与 TACACS 认证服务器之间的网络可达性，然后排查网络中是否存在防火墙等设备，确保 TACACS 认证服务器可达。 **3.** 执行命令 **`display current-configuration`**检查设备上TACACS认证服务器配置是否正确。 o 如果是，请执行步骤 4。 o 如果否，请参考《AAA 命令参考》、《AAA 配置指导》手册修改 TACACS 认证服务器的配置。 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

165.5 TACACS_AUTH_SERVER_UP

日志内容	TACACS authentication server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	TACACS认证服务器状态变为激活
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6 (Informational)
举例	TACACS/6/TACACS_AUTH_SERVER_UP: TACACS authentication server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	对系统无影响
日志产生原因	设备发现TACACS认证服务器状态从block变为active
处理建议	系统正常运行时产生的信息，无需处理

165.6 TACACS_AUTH_SUCCESS

日志内容	User [STRING] at [STRING] was authenticated successfully.
日志含义	TACACS认证成功
参数解释	$1：用户名称 $2：IP地址
日志等级	6 (Informational)
举例	TACACS/6/TACACS_AUTH_SUCCESS: User cwf@system at 192.168.0.22 was authenticated successfully.
对系统的影响	对系统无影响
日志产生原因	TACACS服务器接收了用户的认证请求
处理建议	系统正常运行时产生的信息，无需处理

165.7 TACACS_AUTHOR_SERVER_DOWN

日志内容	TACACS authorization server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	TACACS授权服务器状态为阻塞
参数解释	$1：授权服务器IP地址 $2：授权服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4 (Warning)
举例	TACACS/4/TACACS_AUTHOR_SERVER_DOWN: TACACS authorization server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	会导致用户上线认证失败，如果没有备份认证服务器可能造成用户下线
日志产生原因	设备发现TACACS授权服务器状态从active变为block
处理建议	**1.** 执行命令 **`display interface`**检查连接TACACS授权服务器的接口是否为UP。 o 如果是，请执行步骤 2。 o 如果否，请检查物理链路的连接，确保物理链路连接正常。 **2.** 执行命令 **`ping`**检查TACACS授权服务器是否可达。 o 如果是，请执行步骤 3。 o 如果否，请首先检查设备与 TACACS 授权服务器之间的网络可达性，然后排查网络中是否存在防火墙等设备，确保 TACACS 授权服务器可达。 **3.** 执行命令 **`display current-configuration`**检查设备上TACACS授权服务器配置是否正确。 o 如果是，请执行步骤 4。 o 如果否，请参考《AAA 命令参考》、《AAA 配置指导》手册修改 TACACS 授权服务器的配置。 **4.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

165.8 TACACS_AUTHOR_SERVER_UP

日志内容	TACACS authorization server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
日志含义	TACACS授权服务器状态变为激活
参数解释	$1：授权服务器IP地址 $2：授权服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6 (Informational)
举例	TACACS/6/TACACS_AUTHOR_SERVER_UP: TACACS authorization server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
对系统的影响	对系统无影响
日志产生原因	设备发现TACACS授权服务器状态从block变为active
处理建议	系统正常运行时产生的信息，无需处理

165.9 TACACS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
日志含义	删除TACACS方案中的服务器失败
参数解释	$1：方案名称
日志等级	4 (Warning)
举例	TACACS/4/TACACS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	通过命令行删除TACACS方案中的服务器失败
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

166 TCSM

本节介绍 TCSM（Trusted Computing Services Management，可信计算服务管理）模块输出的日志信息。

166.1 TCSM_CERT_BROKEN

日志内容	Certificate [STRING] is missing or corrupted.
日志含义	证书文件已丢失或损坏
参数解释	$1：证书的名称
日志等级	3 (Error)
举例	TCSM/3/TCSM_CERT_BROKEN: Certificate ak1-cert is missing or corrupted.
对系统的影响	指定证书无法使用
日志产生原因	保存在存储介质中的证书文件已丢失或损坏
处理建议	1. 建议更换存储介质 2. 通过管理端为设备的 TCSM 密钥重新签发证书 3. 如果丢失/损坏的是系统预置证书（以 default 为前缀的证书），请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

166.2 TCSM_KEY_BROKEN

日志内容	Key [STRING] is corrupted or missing.
日志含义	密钥文件已丢失或损坏
参数解释	$1：密钥的名称
日志等级	3 (Error)
举例	TCSM/3/TCSM_KEY_BROKEN: Key abc is corrupted or missing.
对系统的影响	指定密钥无法使用
日志产生原因	保存在存储介质中的密钥文件已丢失或损坏
处理建议	1. 如果该密钥还存在，删除该密钥（相关命令为 **key destroy**） 2. 建议更换存储介质 3. 如果丢失/损坏的是系统预置密钥，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

166.3 TCSM_KEY_HIERARCHY_BROKEN

日志内容	Key hierarchy of [STRING] is corrupted.
日志含义	密钥层级已损坏
参数解释	$1：密钥的名称
日志等级	3 (Error)
举例	TCSM/3/TCSM_KEY_HIERARCHY_BROKEN: Key hierarchy of abc is corrupted.
对系统的影响	指定密钥无法使用
日志产生原因	指定密钥的上层密钥已损坏
处理建议	1. 删除该密钥及其上层密钥（相关命令为 **key destroy**） 2. 建议更换存储介质

166.4 TCSM_TSS_SVC_DOWN

日志内容	TSS service is down.
日志含义	TSS进程down
参数解释	无
日志等级	3 (Error)
举例	TCSM/3/TCSM_TSS_SVC_DOWN: TSS service is down.
对系统的影响	可信计算相关服务无法使用
日志产生原因	TSS进程down
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

166.5 TCSM_TSS_SVC_UP

日志内容	TSS service is up.
日志含义	TSS进程up
参数解释	无
日志等级	5 (Notification)
举例	TCSM/5/TCSM_TSS_SVC_UP: TSS service is up.
对系统的影响	无
日志产生原因	TSS进程up
处理建议	无需处理

167 TELNETD

本节介绍 TELNETD（Telnet Daemon）模块输出的日志信息。

167.1 TELNETD_ACL_DENY

日志内容	The Telnet Connection [IPADDR]([STRING]) request was denied according to ACL rules.
日志含义	Telnet ACL规则限制登录IP地址
参数解释	$1：Telnet客户端IP地址 $2：Telnet客户端IP地址所在VPN
日志等级	5 (Notification)
举例	TELNETD/5/TELNETD_ACL_DENY: The Telnet Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
对系统的影响	系统可能受到攻击
日志产生原因	该日志在Telnet服务端检测到非法客户端尝试登录时输出
处理建议	联系技术支持工程师查看ACL规则，保证该Telnet连接符合该ACL访问规则

167.2 TELNETD_REACH_SESSION_LIMIT

日志内容	Telnet client [STRING] failed to log in. The current number of Telnet sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
日志含义	Telnet登录数用户达到上限，登录失败
参数解释	$1：Telnet客户端IP地址 $2：当前的Telnet会话数 $3：设备允许建立的Telnet会话数
日志等级	6 (Informational)
举例	TELNETD/6/TELNETD_REACH_SESSION_LIMIT: Telnet client 1.1.1.1 failed to log in. The current number of Telnet sessions is 10. The maximum number allowed is (10).
对系统的影响	Telnet登录用户无法正常访问系统
日志产生原因	该日志在Telnet服务端检测到登录客户端数达到上限时输出
处理建议	• 请使用 **display current-configuration | include sesion-limit**命令查看设备当前允许的Telnet最大登录用户数（如果执行该 **display**命令后没有显示，则表示使用的是缺省配置） • 请根据需要使用命令 **aaa session-limit**配置允许的Telnet最大登录用户数

168 TRACK

本节介绍 TRACK 模块输出的日志信息。

168.1 TRACK_STATE_CHANGE

日志内容	The state of track entry [UINT32] changed from [STRING] to [STRING].
日志含义	Track项的状态发生改变
参数解释	$1：Track项的序号，取值范围为1～1024 $2：先前状态，取值为Positive、Negative和NotReady $3：当前状态，取值为Positive、Negative和NotReady
日志等级	6 (Informational)
举例	TRACK/6/TRACK_STATE_CHANGE: -MDC=1; The state of track entry 1 changed from Negative to Positive.
对系统的影响	如果有业务模块关联了该Track，Track项状态的变化可能会导致业务模块执行相应的动作（例如主备接口倒换、路由是否生效等）
日志产生原因	Track项的状态： • 如果监测结果为监测对象工作正常（如接口处于 up 状态、网络可达），则对应 Track 项的状态为 Positive • 如果监测结果为监测对象出现异常（如接口处于 down 状态、网络不可达），则对应 Track 项的状态为 Negative • 如果监测结果无效（如 NQA 作为监测模块时，与 Track 项关联的 NQA 测试组不存在），则对应 Track 项的状态为 NotReady
处理建议	执行**display track**命令查询Track项关联的对象，然后再进一步定位关联的对象是否工作正常

169 TRILL

本节介绍 TRILL 模块输出的日志信息。

169.1 TRILL_DUP_SYSTEMID

日志内容	Duplicate System ID [STRING] in [STRING] PDU sourced from RBridge 0x[HEX].
日志含义	收到的System ID与本地RBridge的System ID相同
参数解释	$1：System ID $2：PDU类型 $3：源RBridge的Nickname
日志等级	5 (Notification)
举例	TRILL/5/TRILL_DUP_SYSTEMID: Duplicate System ID 0011.2200.1501 in LSP PDU sourced from RBridge 0xc758.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	本地RBridge收到的LSP或者IIH PDU中的System ID和本地RBridge的System ID相同。可能的原因包括： • 为本地 RBridge 和远端 RBridge 分配了相同的 System ID • 本地 RBridge 收到了一个自己产生、携带了旧的 Nickname 的 LSP PDU
处理建议	检查TRILL网络中上RBridge的System ID

169.2 TRILL_INTF_CAPABILITY

日志内容	The interface [STRING] does not support TRILL.
日志含义	不支持TRILL的端口被加入到了聚合组中
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	TRILL/4/TRILL_INTF_CAPABILITY: The interface GigabitEthernet0/1/3 does not support TRILL.
对系统的影响	该接口无法使用TRILL的相关功能
日志产生原因	不支持TRILL的端口被加入到了聚合组中
处理建议	将不支持TRILL的端口从聚合组中删除

169.3 TRILL_LICENSE_EXPIRED

日志内容	The TRILL feature is being disabled, because its license has expired.
日志含义	TRILL的License已经过期
参数解释	无
日志等级	5 (Notification)
举例	TRILL/5/TRILL_LICENSE_EXPIRED: The TRILL feature is being disabled, because its license has expired.
对系统的影响	无法使用TRILL功能
日志产生原因	TRILL的License已经过期
处理建议	请更换有效的License

169.4 TRILL_LICENSE_EXPIRED_TIME

日志内容	The TRILL feature will be disabled in [ULONG] days.
日志含义	TRILL的License即将失效
参数解释	$1：功能还可使用的天数
日志等级	5 (Notification)
举例	TRILL/5/TRILL_LICENSE_EXPIRED_TIME: The TRILL feature will be disabled in 2 days.
对系统的影响	License失效后，将无法使用TRILL功能
日志产生原因	TRILL的License不可用，TRILL功能将在2天后失效 说明 主备倒换后新的主控板上没有可用的 TRILL License，会启动 30 天临时可用定时器
处理建议	若要继续使用TRILL功能，请准备新的License

169.5 TRILL_LICENSE_UNAVAILABLE

日志内容	The TRILL feature has no available license.
日志含义	未找到TRILL对应的License
参数解释	无
日志等级	3 (Error)
举例	TRILL/3/TRILL_LICENSE_UNAVAILABLE: The TRILL feature has no available license.
对系统的影响	无法使用TRILL功能
日志产生原因	进程启动时，没有找到TRILL对应的License
处理建议	请为TRILL安装有效的License

169.6 TRILL_MEM_ALERT

日志内容	TRILL process receive system memory alert [STRING] event.
日志含义	TRILL从系统收到一个内存告警事件
参数解释	$1：内存告警事件的类型
日志等级	5 (Notification)
举例	TRILL/5/TRILL_MEM_ALERT: TRILL process receive system memory alert start event.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	TRILL从系统收到一个内存告警事件
处理建议	检查系统内存

169.7 TRILL_NBR_CHG

日志内容	TRILL [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
日志含义	TRILL邻居的状态发生改变
参数解释	$1：TRILL进程ID $2：邻居级别 $3：邻居的System ID $4：接口名 $5：当前邻居状态 o up：表示邻居关系已建立，可以正常工作 o initializing：表示初始状态 o down：表示邻居关系结束
日志等级	5 (Notification)
举例	TRILL/5/TRILL_NBR_CHG: TRILL 1, Level-1 adjacency 0011.2200.1501 (GigabitEthernet0/1/3), state changed to down.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	一个TRILL邻居的状态发生改变
处理建议	当邻居状态变为down或者initializing时，请根据状态变化的原因检查TRILL配置和网络状态

170 TSTREAM

本节介绍 Telemetry Stream 模块输出的日志信息。

170.1 TELEMETRY_STREAM_ENCAP_FAIL

日志内容	Failed to set telemetry stream addressing parameters. Reason: [STRING].
日志含义	Telemetry Stream的寻址参数设置失败
参数解释	$1：失败原因 • Driver encapsulation error：驱动封装功能错误 • The output interface index is an invalid value：根据封装信息查到的出接口是无效值 • The operation is not supported：单板不支持 Telemetry Stream 功能 • Not enough resources to complete the operation：资源不足
日志等级	4 (Warning)
举例	TSTREAM/4/TELEMETRY_STREAM_ENCAP_FAIL: Failed to set telemetry stream addressing parameters. Reason: The operation is not supported.
对系统的影响	**telemetry stream collector**命令下发失败
日志产生原因	通过**telemetry stream collector**命令配置上送采集器报文的封装信息时出错，出错原因请参见日志的Reason字段
处理建议	建议收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

171 USBDPY

本节介绍自动配置模块中 U 盘开局输出的日志信息。

171.1 USBDPY_START

日志内容	Deployment via USB is starting.
日志含义	U盘开局开始执行
参数解释	无
日志等级	6 (Informational)
举例	USBDPY/6/USBDPY_START: Deployment via USB is starting.
对系统的影响	对系统无影响
日志产生原因	U盘开局开始执行
处理建议	无需处理

171.2 USBDPY_SUCCEEDED

日志内容	Deployment via USB succeeded.
日志含义	U盘开局执行成功
参数解释	无
日志等级	6 (Informational)
举例	USBDPY/6/USBDPY_SUCCEEDED: Deployment via USB succeeded.
对系统的影响	对系统无影响
日志产生原因	U盘开局执行成功
处理建议	无需处理

171.3 USBDPY_FAILED

日志内容	Failed to run deployment via USB. Please see the usbload_error.txt file for failure reason.
日志含义	U盘开局执行失败，请在usbload_error.txt文件中查看执行失败的原因
参数解释	无
日志等级	4 (Warning)
举例	USBDPY/4/USBDPY_FAILED: Failed to run deployment via USB. Please see the usbload_error.txt file for failure reason.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	常见的执行失败原因有： • Failed to parse smart config.ini（解析 smart_config.ini 文件失败） • No matching device was found in smart config.ini（无法在 smart_config.ini 找到与开局设备匹配的设备信息）
处理建议	请收集配置文件、日志信息和告警信息，并联系技术支持

171.4 USBDPY_DPY

日志内容	Set startup file: [STRING]
日志含义	U盘开局开始前提示开局使用到的软件包和配置文件
参数解释	$1：开局使用到的软件包或配置文件
日志等级	5 (Notification)
举例	USBDPY/5/USBDPY_DPY: Set startup file: S12600G.ipe.
对系统的影响	对系统无影响
日志产生原因	U盘开局开始前提示开局使用到的软件包和配置文件
处理建议	无需处理

172 VCF

本节介绍 VCF Fabric 模块输出的日志信息。

172.1 VCF_AGGR_CREAT

日志内容	Phase [STRING], Device [STRING] created Layer 2 aggregation group [INT32]: member ports=[STRING].
日志含义	自动化部署进程将端口加入到聚合组
参数解释	$1：阶段 $2：设备MAC地址 $3：二层聚合组ID $4：二层聚合组成员端接口列表
日志等级	6 (Informational)
举例	VCF/6/VCF_AGGR_CREAT: Phase 2.0.5, Device 0000-0000-0000 created Layer 2 aggregation group 10: member ports=Ten-GigabitEthernet1/0/2, Ten-GigabitEthernet1/0/10.
对系统的影响	无
日志产生原因	创建二层聚合组，并将端口加入对应的聚合组
处理建议	无需处理

172.2 VCF_AGGR_DELETE

日志内容	Phase [STRING], Device [STRING] deleted Layer 2 aggregation group [INT32].
日志含义	自动化部署进程删除聚合组
参数解释	$1：阶段 $2：设备MAC地址 $3：二层聚合组ID
日志等级	6 (Informational)
举例	VCF/6/VCF_AGGR_DELETE: Phase 2.0.6, Device 0000-0000-0000 deleted Layer 2 aggregation group 10.
对系统的影响	业务流量无法使用该聚合链路转发
日志产生原因	二层聚合组中仅包含一条Up状态的链路时，删除聚合组
处理建议	无需处理

172.3 VCF_AGGR_FAILED

日志内容	Phase [STRING], Device [STRING] failed to create Layer 2 aggregation group [INT32].
日志含义	自动化部署进程创建聚合组失败
参数解释	$1：阶段 $2：设备MAC地址 $3：聚合组ID
日志等级	3 (Error)
举例	VCF/3/ VCF_AGGR_FAILED: Phase 2.0.7, Device 0000-0000-0000 failed to create Layer 2 aggregation group 10.
对系统的影响	无法使用该聚合组
日志产生原因	创建聚合组失败
处理建议	请管理员排查是否因为资源不足等原因造成聚合组创建失败

172.4 VCF_AUTO_ANALYZE_USERDEF

日志内容	Phase [STRING], Device [STRING] started to parse template file.
日志含义	自动化部署处于开始解析模板文件中的用户自定义配置阶段
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	6 (Informational)
举例	VCF/6/VCF_AUTO_ANALYZE_USERDEF: Phase 1.2.2, Device 0000-0000-0000 started to parse template file.
对系统的影响	无
日志产生原因	开始解析模板文件中的用户自定义配置
处理建议	无需处理

172.5 VCF_AUTO_NO_USERDEF

日志内容	Phase [STRING], Device [STRING] found undefined variable [STRING] in command [STRING] on line [INTEGER].
日志含义	模板文件中存在无法识别的用户定义变量
参数解释	$1：阶段 $2：设备的MAC地址 $3：未定义的用户变量 $4：出错的命令行 $5：出错的命令行行号
日志等级	3 (Error)
举例	VCF/3/VCF_AUTO_NO_USERDEF: Phase 1.2.3, Device 0000-0000-0000 found undefined variable $$_ABC in command interface $$_ABC on line 192.
对系统的影响	系统无法正常解析模板文件
日志产生原因	解析模板文件过程中，若模板文件中存在无法识别的用户定义变量时，输出此日志信息，提示未找到用户定义的变量。若存在多个无法识别的用户定义变量，则打印多条此日志信息
处理建议	需管理员确认模板文件中定义的变量是否正确，修改后重新部署

172.6 VCF_AUTO_START

日志内容	Phase [STRING], Device [STRING] (Role [STRING]) started VCF automated deployment.
日志含义	自动化部署开始
参数解释	$1：阶段 $2：设备的MAC地址 $3：设备的角色，spine、leaf或access
日志等级	5 (Notification)
举例	VCF/5/VCF_AUTO_START: Phase 1.0.1, Device 0000-0000-0000 (Role leaf) started VCF automated deployment.
对系统的影响	无
日志产生原因	自动化部署开始
处理建议	无需处理

172.7 VCF_AUTO_STATIC_CMD

日志内容	Phase [STRING], Device [STRING] automatically executed static commands.
日志含义	自动化部署处于执行模板中的静态配置命令阶段
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	6 (Informational)
举例	VCF/6/VCF_AUTO_STATIC_CMD: Phase 1.2.4, Device 0000-0000-0000 automatically executed static commands.
对系统的影响	无
日志产生原因	执行模板中的静态配置命令，静态配置命令是指与VCF拓扑等动态信息无关的配置命令
处理建议	无需处理

172.8 VCF_BGP

日志内容	Phase [STRING], Device [STRING] established a BGP session with peer [STRING] in AS [INT32]. Phase [STRING], Device [STRING] established a BGP session with peers [[STRING]] in AS [INT32].
日志含义	自动化部署处于成功与对等体建立BGP会话阶段
参数解释	$1：阶段 $2：设备的MAC地址 $3：peer地址（三层组网时，主Spine节点可能一次为设备配置多个peer，不同peer地址之间用逗号分隔） $4：BGP的AS号
日志等级	6 (Informational)
举例	VCF/6/VCF_BGP: Phase 3.0.5, Device 0000-0000-0000 established a BGP session with peer 1.1.1.1 in AS 100. VCF/6/VCF_BGP: Phase 3.0.5, Device 0000-0000-0000 established a BGP session with peers [‘1.1.1.1’ , ‘1.1.1.2’] in AS 100.
对系统的影响	无
日志产生原因	VCF成功与对等体建立BGP会话 在三层组网中，仅主Spine节点上会记录该日志信息
处理建议	无需处理

172.9 VCF_DOWN_LINK

日志内容	Phase [STRING], Device [STRING] discovered downlink interface [STRING].
日志含义	自动化部署处于发现下行接口并下发配置阶段
参数解释	$1：阶段 $2：设备MAC地址 $3：下行接口名
日志等级	6 (Informational)
举例	VCF/6/VCF_DOWN_LINK: Phase 2.0.8, Device 0000-0000-0000 discovered downlink interface Ten-GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	VCF发现下行接口（Spine设备上连接Leaf的接口或leaf设备连接下游接入设备的接口），并下发配置
处理建议	无需处理

172.10 VCF_DRIVER_INIT

日志内容	Phase [STRING], failed to find driver [STRING]. Driver initialization failed.
日志含义	驱动初始化失败
参数解释	$1：阶段 $2：驱动名称
日志等级	3 (Error)
举例	VCF/3/VCF_DRIVER_INIT: Phase 3.0.8, failed to find driver 6820. Driver initialization failed.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	设备驱动不存在时，提示驱动初始化失败。
处理建议	请检查模板对应驱动名称是否正确，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员确认VCF是否支持该驱动

172.11 VCF_FAILED_ADD_IRFPORT

日志内容	Phase [STRING], failed to bind IRF physical interface [STRING] on device with MAC address [STRING] to an IRF port three times.
日志含义	IRF物理端口绑定IRF端口失败
参数解释	$1：阶段 $2：IRF物理端口 $3：MAC地址
日志等级	4 (Warning)
举例	VCF/4/VCF_FAILED_ADD_IRFPORT: Phase 2.0.10, failed to bind IRF physical interface [STRING] on device with MAC address 4c85-5206-0100 to an IRF port three times.
对系统的影响	需结合实际情况，综合判断对系统的影响
日志产生原因	设备自动化上线时，如果指定IRF物理端口绑定IRF端口失败三次，则VCF不再尝试将该IRF物理端口与IRF端口绑定，同时打印此日志
处理建议	建议检查IRF连线

172.12 VCF_GET_IMAGE

日志内容	Phase [STRING], Device [STRING] obtained information about update startup image file [STRING]: new version=[STRING], current version=[STRING].
日志含义	自动化部署处于通过模板文件获取新版本的文件名和版本号阶段
参数解释	$1：阶段 $2：设备的MAC地址 $3：新版本文件名 $4：新版本的产品外部版本号 $5：设备当前产品外部版本号
日志等级	6 (Informational)
举例	VCF/6/VCF_GET_IMAGE: Phase 1.3.1, Device 0000-0000-0000 obtained information about update startup image file s6800.ipe: new version=V300R009B01D002, current version=V300R009B01D001.
对系统的影响	无
日志产生原因	通过模板文件获取新版本的文件名和版本号
处理建议	无需处理

172.13 VCF_GET_TEMPLATE

日志内容	Phase [STRING], Device [STRING] downloaded template file [STRING].
日志含义	自动化部署处于将模板文件下载到本地设备阶段
参数解释	$1：阶段 $2：设备的MAC地址 $3：模板文件名
日志等级	6 (Informational)
举例	VCF/6/VCF_GET_TEMPLATE: Phase 1.2.1, Device 0000-0000-0000 downloaded template file /mnt/flash:/vxlan_spine.template.
对系统的影响	无
日志产生原因	将自动部署的模板文件下载到本地设备
处理建议	无需处理

172.14 VCF_INSTALL_IMAGE

日志内容	Phase [STRING], Device [STRING] started to install the [STRING] version of startup image.
日志含义	自动化部署处于开始安装新版本阶段
参数解释	$1：阶段 $2：设备的MAC地址 $3：设备的版本号
日志等级	6 (Informational)
举例	VCF/6/VCF_INSTALL_IMAGE: Phase 1.3.3, Device 0000-0000-0000 started to install the V700R001B70D001 version of startup image.
对系统的影响	无
日志产生原因	设备开始安装新版本
处理建议	无需处理

172.15 VCF_IRF_FINISH

日志内容	Phase [STRING], Device [STRING] finished IRF configuration: result=[INT32].
日志含义	自动化部署完成IRF配置下发
参数解释	$1：阶段 $2：本设备的MAC地址 $3：执行IRF配置的结果 (成功=0, 失败=-1)
日志等级	5 (Notification)
举例	VCF/5/VCF_IRF_FINISH: Phase 2.0.3, Device 0000-0000-0000 finished IRF configuration: result=0.
对系统的影响	无
日志产生原因	完成IRF配置下发
处理建议	如果配置下发失败，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

172.16 VCF_IRF_FOUND

日志内容	Phase [STRING], Device [STRING] (Role [STRING]) found a peer ([STRING]) with the same role, IRF stackability check result: [INT32].
日志含义	自动化部署处于发现需要搭建IRF设备的阶段
参数解释	$1：阶段 $2：本设备的MAC地址 $3：角色名字 $4：对端设备的MAC地址 $5：检查结果，取值包括： ○ 0：表示可配置 IRF ○ 1：表示 MAC 地址冲突
日志等级	5 (Notification)
举例	VCF/5/VCF_IRF_FOUND: Phase 2.0.1, Device 0000-0000-0000 (Role leaf) found a peer with the same role, IRF stackability check result: 0.
对系统的影响	无
日志产生原因	VCF通过拓扑变化发现对端需要搭建IRF的设备，检查是否能够开始进行IRF配置
处理建议	无需处理

172.17 VCF_IRF_START

日志内容	Phase [STRING], Device [STRING] started IRF configuration: current member ID=[INT32], new member ID=[INT32], priority=[INT32], IRF-port 1's member ports=[STRING], IRF-port 2's member ports=[STRING].
日志含义	设备开始下发IRF配置
参数解释	$1：阶段 $2：本设备的MAC地址 $3：设备当前的成员编号 $4：设备新的成员编号 $5：设备新的优先级 $6：设备IRF-Port1绑定的物理端口列表，没有为none $7：设备IRF-Port2绑定的物理端口列表，没有为none
日志等级	5 (Notification)
举例	VCF/5/VCF_IRF_START: Phase 2.0.2, Device 0000-0000-0000 started IRF configuration: current member ID=2, new member ID=1, priority=2, IRF-port 1's member ports=GigabitEthernet1/0/1, IRF-port 2's member ports=none.
对系统的影响	无
日志产生原因	开始下发IRF配置
处理建议	无需处理

172.18 VCF_LOOPBACK_START

日志内容	Phase [STRING], IP address assignment started for [STRING] on other nodes.
日志含义	VCF主节点开始为其他节点的接口分配IP地址
参数解释	$1：阶段 $2：接口名称
日志等级	5 (Notification)
举例	VCF/5/VCF_LOOPBACK_START: Phase 3.0.1, IP address assignment started for Loopback0 on other nodes.
对系统的影响	无
日志产生原因	VCF主节点开始为其他节点的接口分配IP地址
处理建议	无需处理

172.19 VCF_LOOPBACK_START_FAILED

日志内容	Phase [STRING], failed to assign IP addresses to [STRING] on other nodes: reason=[STRING].
日志含义	主节点未能开始为其他节点的接口分配IP地址
参数解释	$1：阶段 $2：接口名称 $3：启动失败的原因 ○ -1：表示没有指定 IP 范围 ○ -2：表示 IP 地址无效
日志等级	5 (Notification)
举例	VCF/5/VCF_LOOPBACK_START_FAILED: Phase 3.0.1, failed to assign IP addresses to Loopback0 on other nodes: reason=-1.
对系统的影响	其他节点未获取到主节点分配的IP地址
日志产生原因	VCF Fabric组网中，由于以下原因之一，主节点没能开始为其他节点的接口分配IP地址： • 没有指定 IP 范围 • IP 地址无效
处理建议	管理员检查模板中IP范围是否有问题

172.20 VCF_LOOPBACK_ALLOC

日志内容	Phase [STRING], assigned IP [STRING] to [STRING] on Device [STRING]: result=[INT32].
日志含义	VCF主节点为指定设备的接口分配IP地址
参数解释	$1：为Loopback接口分配的IP地址 $2：设备的MAC地址 $3：接口名称 $4：IP地址分配的状态，取值包括： ○ 0：表示成功 ○ -1：表示 netconf 下发失败 ○ -2：表示 netconf 处理异常 ○ -3：表示 netconf 初始化失败
日志等级	5 (Notification)
举例	VCF/5/VCF_LOOPBACK_ALLOC: Phase 3.0.2, assigned IP 10.100.1.1 to Loopback0 on Device 0000-0000-0000: result=0.
对系统的影响	无
日志产生原因	VCF主节点为指定设备的接口分配IP地址
处理建议	管理员根据结果查找失败原因

172.21 VCF_LOOPBACK_NO_FREE_IP

日志内容	Phase [STRING], no IP addresses available for Device [STRING].
日志含义	主节点无法为指定设备的接口分配IP地址
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	4 (Warning)
举例	VCF/4/VCF_LOOPBACK_NO_FREE_IP: Phase 3.0.4, no IP addresses available for Device 0000-0000-0000.
对系统的影响	接口无法获取IP地址
日志产生原因	VCF主节点上没有可用的IP地址，无法为指定设备的接口分配IP地址
处理建议	请用户确认IP预留范围是否准确

172.22 VCF_LOOPBACK_RECLAIM

日志内容	Phase [STRING], reclaimed IP [STRING] from [STRING] on Device [STRING]: reason=[INT32].
日志含义	VCF收回已经分配出去的接口的IP地址
参数解释	$1：阶段 $2：收回的Loopback接口IP地址 $3：接口名称 $4：收回IP地址的设备的MAC地址 $5：收回原因，取值 o 1：表示设备 DOWN
日志等级	5 (Notification)
举例	VCF/5/VCF_LOOPBACK_RECLAIM: Phase 3.0.3, reclaimed IP 10.10.10.1 from Loopback0 on Device 0000-0000-0000: reason=1.
对系统的影响	无
日志产生原因	VCF收回已经分配出去的接口的IP地址
处理建议	无需处理

172.23 VCF_REBOOT

日志内容	Phase [STRING], Device [STRING] will reboot. Reason: [STRING].
日志含义	设备自动重启
参数解释	$1：阶段 $2：设备的MAC地址 $3：重启原因，取值为： o Hardware resource mode change：硬件资源模式修改 o Version upgrade success：版本升级成功 o IRF member ID change：自动化上线时修改成员 ID o IRF fabric setup success：IRF 成功建立 o Change of the maximum number of ECMP routes：最大等价路由条数修改 o Standalone-to-IRF mode switchover：设备由独立运行模式切换为 IRF 模式
日志等级	5 (Notification)
举例	VCF/5/VCF_REBOOT: Phase 1.2.3, Device 00e0-fc20-6304 will reboot. Reason: IRF member ID change.
对系统的影响	无
日志产生原因	完成新版本升级、IRF成员编号变更等操作后，设备自动重启
处理建议	无需处理

172.24 VCF_SKIP_INSTALL

日志内容	Phase [STRING], Device [STRING] skipped automatic version update.
日志含义	自动化部署跳过自动更新版本阶段
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	5 (Notification)
举例	VCF/5/VCF_SKIP_INSTALL: Phase 1.3.2, Device 0000-0000-0000 skipped automatic version update.
对系统的影响	无
日志产生原因	设备当前运版本与通过模板文件获取的版本一致时，跳过自动更新版本
处理建议	无需处理

172.25 VCF_STATIC_CMD_ERROR

日志内容	Phase [STRING], Device [STRING] failed to automatically execute static command '[STRING]' in context '[STRING]'.
日志含义	自动部署过程中执行失败的静态命令
参数解释	$1：阶段 $2：设备的MAC地址 $3：自动配置执行失败的命令 $4：执行失败的命令所在的完整片段
日志等级	4 (Warning)
举例	VCF/4/VCF_STATIC_CMD_ERROR: Phase 1.2.5, Device 0000-0000-0000 failed to automatically execute static command 'port link bridge' in context 'interface ten-gigabitethernet1/0/1; port link bridge'.
对系统的影响	导致自动化部署失败
日志产生原因	自动部署过程中执行失败的静态命令
处理建议	管理员查找错误原因，修改错误后需要重新部署

172.26 VCF_UP_LINK

日志内容	Phase [STRING], Device [STRING] discovered uplink interface [STRING].
日志含义	自动部署处于发现上行接口并下发配置阶段
参数解释	$1：阶段 $2：设备MAC地址 $3：上行接口名
日志等级	6 (Informational)
举例	VCF/6/VCF_UP_LINK: Phase 2.0.9, Device 0000-0000-0000 discovered uplink interface Ten-GigabitEthernet1/0/1.
对系统的影响	无
日志产生原因	VCF发现上行接口（Leaf设备上连接Spine的接口），并下发配置
处理建议	无需处理

172.27 VCF_UPDATE_COPY_FAILED

日志内容	Phase [STRING], Device [STRING] failed to copy image. Reason: [STRING].
日志含义	自动化部署进程中，拷贝版本失败
参数解释	$1：阶段 $2：设备的MAC地址 $3：拷贝版本失败的原因，取值为： o Insufficient spare space：剩余空间不足 o Copy failed：拷贝版本失败
日志等级	5 (Notification)
举例	VCF/5/VCF_UPDATE_COPY_FAILED: Phase 1.3.5, Device 00e0-fc20-6304 failed to copy image. Reason: Insufficient spare space.
对系统的影响	设备无法使用期望的软件版本
日志产生原因	VCF自动化升级拷贝版本失败，连续尝试拷贝版本失败三次，则设备退出VCF进程，每次拷贝版本失败均打印该日志
处理建议	• 若拷贝版本失败的原因为 Insufficient spare space：请清理设备的内存空间，保证设备上可使用的内存空间大于软件版本的文件大小 • 若拷贝版本失败的原因为 Copy failed：请检查设备与文件服务器之间的网络，保证设备与文件服务器之间网络互通

172.28 VCF_UPDATE_FAILED

日志内容	Phase [STRING], Device [STRING] update has failed and end automated deployment.
日志含义	自动化部署进程中，升级版本失败
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	4 (Warning)
举例	VCF/4/VCF_UPDATE_FAILED: Phase 1.3.6, Device 00e0-fc20-6304 update has failed and end automated deployment.
对系统的影响	设备无法使用期望的软件版本
日志产生原因	VCF自动化升级版本失败，设备退出VCF进程
处理建议	请结合VCF_UPDATE_COPY_FAILED日志，排查故障： • 若拷贝版本失败的原因为 Insufficient spare space：请清理设备的内存空间，保证设备上可使用的内存空间大于软件版本的文件大小 • 若拷贝版本失败的原因为 Copy failed：请检查设备与文件服务器之间的网络，保证设备与文件服务器之间网络互通

172.29 VCF_WHITE_LIST_CHECK

日志内容	Phase [STRING], Device [STRING] failed whitelist check and automated undelay network deployment stopped.
日志含义	自动化部署进程中，白名单检查失败
参数解释	$1：阶段 $2：本设备的MAC地址，格式为xxxx-xxxx-xxxx
日志等级	5 (Notification)
举例	VCF/5/VCF_WHITE_LIST_CHECK: Phase 1.0.1, Device 00e0-fc20-6304 failed whitelist check and automated undelay network deployment stopped.
对系统的影响	设备无法自动化上线
日志产生原因	VCF模块提示白名单检查失败，Underlay自动化配置下发停止。
处理建议	请将该设备添加到VCF的白名单中

173 VLAN

本节介绍接口 VLAN 模块输出的日志信息。

173.1 VLAN_CREATEFAIL

日志内容	Failed to create VLAN [STRING]. The maximum number of VLANs has been reached.
日志含义	由于可创建的VLAN已经达到上限，新的VLAN创建失败
参数解释	$1：VLAN ID
日志等级	4 (Warning)
举例	VLAN/4/ VLAN_CREATEFAIL: Failed to create VLAN 1025-4094. The maximum number of VLANs has been reached.
对系统的影响	无法创建指定VLAN
日志产生原因	VLAN硬件资源不足
处理建议	1. 执行 **display vlan brief**命令，查看已经创建的VLAN 2. 执行 **undo vlan**命令，删除不需要的VLAN

173.2 VLAN_FAILED

日志内容	Failed to add interface [STRING] to the default VLAN.
日志含义	端口无法加入到缺省VLAN中
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	VLAN/4/VLAN_FAILED: Failed to add interface GigabitEthernet1/0/1 to the default VLAN.
对系统的影响	本日志指定的端口无法接收携带缺省VLAN的报文
日志产生原因	在硬件资源不足时创建端口
处理建议	请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

173.3 VLAN_QINQETHTYPE_FAILED

日志内容	Failed to set the TPID value in CVLAN tags to [UINT32] (hexadecimal). The operation is not supported.
日志含义	配置报文内层VLAN Tag的TPID值失败
参数解释	$1：内层VLAN Tag的TPID值
日志等级	4 (Warning)
举例	VLAN/4/VLAN_QINQETHTYPE_FAILED: Failed to set the TPID value in CVLAN tags to 8200 (hexadecimal). The operation is not supported.
对系统的影响	无法修改报文内层VLAN Tag的TPID值
日志产生原因	在IRF3.1组网环境中，CB支持配置内层VLAN Tag的TPID值但PEX不支持的情况下，在CB上执行**qinq ethernet-type customer-tag命令后打印**本日志
处理建议	确认组网中的PEX设备是否支持配置内层VLAN Tag的TPID值。如果不支持，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

173.4 VLAN_VLANMAPPING_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
日志含义	端口上的VLAN映射配置丢失
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	VLAN/4/VLAN_VLANMAPPING_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
对系统的影响	该端口上的VLAN映射功能无法正常运行
日志产生原因	硬件资源不足或该端口加入/离开二层聚合组
处理建议	**1.** 在端口上重新配置 VLAN 映射功能。如果问题仍未解决，请执行步骤 2 **2.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

173.5 VLAN_VLANTRANSPARENT_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
日志含义	端口的VLAN透传功能丢失
参数解释	$1：接口名称
日志等级	4 (Warning)
举例	VLAN/4/VLAN_VLANTRANSPARENT_FAILED: The configuration failed because of resource insufficiency or conflicts on GigabitEthernet1/0/1.
对系统的影响	该端口上的VLAN透传功能无法正常运行
日志产生原因	硬件资源不足或该端口加入/离开二层聚合组
处理建议	**1.** 在端口上重新配置 VLAN 透传功能。如果问题仍未解决，请执行步骤 2 **2.** 请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

174 VRRP4

本节介绍 VRRP4（IPv4 VRRP）模块输出的日志信息。

174.1 VRRP_STATUS_CHANGE

日志内容	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
日志含义	设备在VRRP备份组中的角色发生变化
参数解释	$1：网络协议类型，取值包括IPv4 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：先前状态 $5：当前状态 $6：状态变化原因： • Interface event received：收到接口事件 • IP address deleted：VRRP 备份组的虚拟 IP 地址被删除 • The status of the tracked object changed：Track 对象状态变化 • VRRP packet received：收到 VRRP 报文 • Current device has changed to IP address owner：当前设备成为地址拥有者 • Master-down-timer expired：Master down 定时器超时 • Zero priority packet received：收到 0 优先级的报文 • Preempt：发生了抢占
日志等级	6 (Informational)
举例	VRRP4/6/VRRP_STATUS_CHANGE: The status of IPv4 virtual router 10 (configured on Ethernet0/0) changed from Backup to Master: Master-down-timer expired.
对系统的影响	对系统无影响
日志产生原因	日志产生原因可能为： • 原因一：收到接口事件 • 原因二：部署 VRRP 备份组的接口 IP 地址被删除 • 原因三：Track 对象状态变化 • 原因四：收到 VRRP 报文 • 原因五：当前设备成为地址拥有者 • 原因六：Master down 定时器超时 • 原因七：收到 0 优先级的报文 • 原因八：发生了抢占 • 原因九：管理备份组驱动
处理建议	请根据日志中携带的VRRP状态发生变化的原因，进行相应处理： • 针对原因一（收到接口事件），请关注备份组所在接口是否发生故障 请在本机和对端分别执行 **display interface**命令查看备份组连接接口的状态。如果接口状态显示为Down，请根据显示信息定位并处理接口故障 • 针对原因二（VRRP备份组的虚拟IP地址被删除），在接口视图下，执行 **vrrp [ipv6] vrid**命令为VRRP备份组配置虚拟IP地址 • 针对原因三（Track对象状态变化），先执行 **display vrrp**命令找到关联的Track项的编号，再使用 **display track**命令定位Track项故障，并解决Track项故障

- 针对原因四（收到 VRRP 报文），无需处理
- 针对原因五（当前设备成为地址拥有者），处理建议如下：

  确认是否需要将本机配置为VRRP备份组的IP地址拥有者：在本机执行不带参数的**display vrrp**命令，查看VRRP组的虚拟IP地址；在本机执行**display interface brief**命令，查看设备接口的IP地址，找到与VRRP备份组IP地址相同的接口。接口IP地址与虚拟IP地址相同的设备被称为IP地址拥有者。当备份组内存在IP地址拥有者时，只要其工作正常，则为Master

  - 如果确认需要将设备配置为 IP 地址拥有者，则无需处理
  - 如果确认无需将设备配置为IP地址拥有者，请在接口视图下，使用**vrrp vrid**命令修改VRRP备份组的虚拟IP地址
- 针对原因六（Master down 定时器超时）处理建议如下：
  - 确认是否为对端设备故障。在对端设备上执行**display vrrp**命令，如果State字段取值为Initialize，则说明设备故障。请检查故障原因，恢复对端设备
  - 确认是否为备份组连接接口故障。在本端和对端分别执行**display interface**命令查看备份组连接接口的状态。如果接口状态显示为Down，请根据显示信息定位并处理接口故障
  - 确认是否为VRRP配置错误，在本机和对端分别执行**display current-configuration | inculde vrrp**命令，过滤VRRP配置。本机和对端的VRRP配置有如下要求：
  - 本机和对端的VRRP备份组编号以及虚拟IP地址必须相同，如果不同，请使用**vrrp ipv6 vrid**命令重新配置
  - 对于VRRPv4，要求版本号一致，如果不一致，请在接口视图下使用**vrrp version**命令修改。VRRPv6 仅支持VRRPv3 版本，不支持修改
  - 对于VRRPv4，要求认证方式一致，如果配置了认证字，还要求认证字一致。如果不一致，请在接口视图下使用**vrrp vrid authentication-mode**命令修改。VRRPv6 不支持认证
- 针对原因七（收到 0 优先级的报文），处理建议如下：
  - 在本机和对端分别执行**display vrrp verbose**命令，查看配置的VRRP优先级（Config pri字段）：
  - 如果确认配置正确，则无需处理
  - 如果确认配置错误，请在接口视图下，使用**vrrp vrid priority**命令修改
  - 在本机和对端分别执行**display vrrp verbose**命令，查看配置的VRRP优先级（Config pri字段）和实际生效的VRRP优先级（Running pri字段）。如果两个取值不同，则进一步查看关联的Track项的编号，使用**display track**命令定位Track项故障，并解决Track项故障
- 针对原因八（发生了抢占），如果是管理员手工触发的抢占，则无需处理；如果是自动抢占，则说明监控对象故障，需要进一步确认自动抢占的原因
- 针对原因九（管理备份组驱动）在本机执行**display vrrp verbose**命令，根据Follow Name字段的取值找到关联的管理备份组名称，再根据管理备份组Trap中提示的原因字段取值进一步处理
- 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

174.2 VRRP_VF_STATUS_CHANGE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) virtual forwarder [UINT32] detected status change (from [STRING] to [STRING]): [STRING].
日志含义	虚拟转发器状态发生改变
参数解释	$1：网络协议类型，取值包括IPv4 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：VF ID $5：VF先前状态，取值包括： • Active：表示虚拟转发器处于转发状态 • Listening：表示虚拟转发器处于侦听状态（即备份状态） • Initialize：表示虚拟转发器处于初始状态 $6：VF当前状态，取值包括： • Active：表示虚拟转发器处于转发状态 • Listening：表示虚拟转发器处于侦听状态（即备份状态） • Initialize：表示虚拟转发器处于初始状态 $7：状态变化原因，取值包括： • Weight changed：权重变化 • Adding virtual MAC address failed：添加虚拟 MAC 地址失败 • Conceded：收到虚拟转发器优先级为 0 的报文，主动放弃转发权限 • Learnt from Advertisement：从 Advertisement 报文中学习 • Reply received：收到 reply 报文 • Release received：收到 release 报文 • Active timer expired：Active 定时器 超时 • Time-out timer expired：Time-Out 定时器超时 • Self-allocated：Master 为自己分配虚拟 MAC 地址 • VRRP down：VRRP 备份组 Down • Take over：接管 AVF 的工作 • The status of the tracked object changed：Track 项变化
日志等级	6 (Informational)
举例	VRRP4/6/VRRP_VF_STATUS_CHANGE: The IPv4 virtual router 10 (configured on GigabitEthernet5/1) virtual forwarder 2 detected status change (from Active to Initialize): Weight changed.
对系统的影响	正常主备倒换对系统无影响；如果倒换后，虚拟转发器状态异常，会导致业务中断
日志产生原因	日志产生原因可能为： • 原因一：权重变化 • 原因二：添加虚拟 MAC 地址失败 • 原因三：收到虚拟转发器优先级为 0 的报文，主动放弃转发权限 • 原因四：从 Advertisement 报文中学习 • 原因五：收到 reply 报文

	• 原因六：收到 release 报文 • 原因七：Active 定时器 超时 • 原因八：Time-Out 定时器超时 • 原因九：Master 为自己分配虚拟 MAC 地址 • 原因十：VRRP 备份组 Down • 原因十一：接管 AVF 的工作 • 原因十二：Track 项变化

处理建议	请根据日志中携带的VRRP状态发生变化的原因，进行相应处理：
	• 针对原因一（权重变化），处理建议如下：
	  ○ 查看配置的VRRP优先级（Config pri字段）和实际生效的VRRP优先级（Running pri字段）。如果两个取值不同，则进一步查看关联的Track项的编号，使用 **display track**命令定位Track项故障，并解决Track项故障
	• 针对原因二（添加虚拟 MAC 地址失败），确定 MAC 操作失败的根因并解决
	• 针对原因三（收到虚拟转发器优先级为 0 的报文，主动放弃转发权限），处理建议如下：请确认是否组网中有备份组的优先级高于本地优先级：
	  ○ 若配置正确，无需处理
	  ○ 若配置错误，请在接口视图下，使用 **vrrp vrid priority**命令修改
	• 针对原因四（从 Advertisement 报文中学习）：无需处理
	• 针对原因五（收到 reply 报文）：无需处理
	• 针对原因六（收到 release 报文）：无需处理
	• 针对原因七（Active 定时器 超时）：无需处理
	• 针对原因八（Time-Out 定时器超时）：无需处理
	• 针对原因九（Master 为自己分配虚拟 MAC 地址）：无需处理
	• 针对原因十（VRRP备份组Down），检查备份组所在接口是否发生故障：**display interface**命令查看备份组连接接口的状态。如果接口状态显示为Down，请根据显示信息定位并处理接口故障
	• 针对原因十一 （接管 AVF 的工作），处理建议如下：原来最高优先级的虚拟转发器 AVF 权重失效，请检查引起原 AVF 优先级变化的原因
	• 针对原因十二（Track 项变化），处理建议如下：
	  检查Track项的状态，可使用 **display track**命令定位Track项故障，并解决Track项故障

174.3 VRRP_VMAC_INEFFECTIVE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
日志含义	给VRRP备份组分配虚拟MAC地址失败
参数解释	$1：网络协议类型，取值包括IPv4 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：出现错误的原因，取值为Insufficient hardware resources，表示硬件资源不足
日志等级	3 (Error)
举例	VRRP4/3/VRRP_VMAC_INEFFECTIVE: The IPv4 virtual router 10 (configured on Ethernet0/0) failed to add virtual MAC: Insufficient hardware resources.
对系统的影响	本设备的VRRP备份组无法正常工作
日志产生原因	系统将VRRP备份组的虚拟MAC地址下发给驱动，驱动添加虚拟MAC地址失败，VRRP备份组将无法使用该虚拟MAC地址通信
处理建议	1. 在Probe视图下执行**display system internal vrrp kernel virtual-route**命令查看VRRP内核的虚拟路由器信息，收集显示信息 2. 收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

175 VRRP6

本节介绍 VRRP6（IPv6 VRRP）模块输出的日志信息。

175.1 VRRP_STATUS_CHANGE

日志内容	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
日志含义	设备在VRRP备份组中的角色发生变化
参数解释	$1：网络协议类型，取值包括IPv6 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：先前状态 $5：当前状态 $6：状态变化原因： • Interface event received：收到接口事件 • IP address deleted：VRRP 备份组的虚拟 IP 地址被删除 • The status of the tracked object changed：Track 对象状态变化 • VRRP packet received：收到 VRRP 报文 • Current device has changed to IP address owner：当前设备成为地址拥有者 • Master-down-timer expired：Master down 定时器超时 • Zero priority packet received：收到 0 优先级的报文 • Preempt：发生了抢占
日志等级	6 (Informational)
举例	VRRP6/6/VRRP_STATUS_CHANGE: The status of IPv6 virtual router 10 (configured on Ethernet0/0) changed from Backup to Master: Master-down-timer expired.
对系统的影响	对系统无影响
日志产生原因	日志产生原因可能为： • 原因一：收到接口事件 • 原因二：部署 VRRP 备份组的接口 IP 地址被删除 • 原因三：Track 对象状态变化 • 原因四：收到 VRRP 报文 • 原因五：当前设备成为地址拥有者 • 原因六：Master down 定时器超时 • 原因七：收到 0 优先级的报文 • 原因八：发生了抢占 • 原因九：管理备份组驱动
处理建议	请根据日志中携带的VRRP状态发生变化的原因，进行相应处理： • 针对原因一（收到接口事件），请关注备份组所在接口是否发生故障 请在本机和对端分别执行 **display interface**命令查看备份组连接接口的状态。如果接口状态显示为Down，请根据显示信息定位并处理接口故障 • 针对原因二（VRRP备份组的虚拟IP地址被删除），在接口视图下，执行 **vrrp ipv6 vrid**命令为VRRP备份组配置虚拟IP地址 • 针对原因三（Track对象状态变化），先执行 **display vrrp ipv6**命令找到关联的Track项的编号，再使用 **display track**命令定位Track项故障，并解决Track项故

	障 • 针对原因四（收到 VRRP 报文），无需处理 • 针对原因五（当前设备成为地址拥有者），处理建议如下： 确认是否需要将本机配置为VRRP备份组的IP地址拥有者：在本机执行不带参数的 **display vrrp ipv6**命令，查看VRRP组的虚拟IP地址；在本机执行 **display interface brief**命令，查看设备接口的IP地址，找到与VRRP备份组IP地址相同的接口。接口IP地址与虚拟IP地址相同的设备被称为IP地址拥有者。当备份组内存在IP地址拥有者时，只要其工作正常，则为Master o 如果确认需要将设备配置为 IP 地址拥有者，则无需处理 o 如果确认无需将设备配置为IP地址拥有者，请在接口视图下，使用 **vrrp ipv6 vrid**命令修改VRRP备份组的虚拟IP地址 • 针对原因六（Master down 定时器超时）处理建议如下： o 确认是否为对端设备故障。在对端设备上执行 **display vrrp ipv6**命令，如果State字段取值为Initialize，则说明设备故障。请检查故障原因，恢复对端设备 o 确认是否为备份组连接接口故障。在本端和对端分别执行 **display interface** 命令查看备份组连接接口的状态。如果接口状态显示为Down，请根据显示信息定位并处理接口故障 o 确认是否为VRRP配置错误，在本机和对端分别执行 **display current-configuration | inculde vrrp**命令，过滤VRRP配置。本机和对端的VRRP备份组编号以及虚拟IP地址必须相同，如果不同，请使用 **vrrp ipv6 vrid**命令重新配置 • 针对原因七（收到 0 优先级的报文），处理建议如下： o 在本机和对端分别执行 **display vrrp verbose**命令，查看配置的VRRP优先级（Config pri字段）： o 如果确认配置正确，则无需处理 o 如果确认配置错误，请在接口视图下，使用 **vrrp ipv6 vrid priority**命令修改 o 在本机和对端分别执行 **display vrrp ipv6 verbose**命令，查看配置的VRRP优先级（Config pri字段）和实际生效的VRRP优先级（Running pri字段）。如果两个取值不同，则进一步查看关联的Track项的编号，使用 **display track**命令定位Track项故障，并解决Track项故障 • 针对原因八（发生了抢占），如果是管理员手工触发的抢占，则无需处理；如果是自动抢占，则说明监控对象故障，需要进一步确认自动抢占的原因 • 针对原因九（管理备份组驱动）在本机执行 **display vrrp ipv6 verbose**命令，根据Follow Name字段的取值找到关联的管理备份组名称，再根据管理备份组Trap中提示的原因字段取值进一步处理 • 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

175.2 VRRP_VF_STATUS_CHANGE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) virtual forwarder [UINT32] detected status change (from [STRING] to [STRING]): [STRING].
日志含义	虚拟转发器状态发生改变
参数解释	$1：网络协议类型，取值包括IPv6 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：VF ID $5：VF先前状态，取值包括： • Active：表示虚拟转发器处于转发状态 • Listening：表示虚拟转发器处于侦听状态（即备份状态） • Initialize：表示虚拟转发器处于初始状态 $6：VF当前状态，取值包括： • Active：表示虚拟转发器处于转发状态 • Listening：表示虚拟转发器处于侦听状态（即备份状态） • Initialize：表示虚拟转发器处于初始状态 $7：状态变化原因，取值包括： • Weight changed：权重变化 • Adding virtual MAC address failed：添加虚拟 MAC 地址失败 • Conceded：收到虚拟转发器优先级为 0 的报文，主动放弃转发权限 • Learnt from Advertisement：从 Advertisement 报文中学习 • Reply received：收到 reply 报文 • Release received：收到 release 报文 • Active timer expired：Active 定时器 超时 • Time-out timer expired：Time-Out 定时器超时 • Self-allocated：Master 为自己分配虚拟 MAC 地址 • VRRP down：VRRP 备份组 Down • Take over：接管 AVF 的工作 • The status of the tracked object changed：Track 项变化
日志等级	6 (Informational)
举例	VRRP6/6/VRRP_VF_STATUS_CHANGE: The IPv6 virtual router 10 (configured on GigabitEthernet5/1) virtual forwarder 2 detected status change (from Active to Initialize): Weight changed.
对系统的影响	正常主备倒换对系统无影响；如果倒换后，虚拟转发器状态异常，会导致业务中断
日志产生原因	日志产生原因可能为： • 原因一：权重变化 • 原因二：添加虚拟 MAC 地址失败 • 原因三：收到虚拟转发器优先级为 0 的报文，主动放弃转发权限 • 原因四：从 Advertisement 报文中学习 • 原因五：收到 reply 报文

	• 原因六：收到 release 报文 • 原因七：Active 定时器 超时 • 原因八：Time-Out 定时器超时 • 原因九：Master 为自己分配虚拟 MAC 地址 • 原因十：VRRP 备份组 Down • 原因十一：接管 AVF 的工作 • 原因十二：Track 项变化

处理建议	请根据日志中携带的VRRP状态发生变化的原因，进行相应处理：
	• 针对原因一（权重变化），处理建议如下：
	  ○ 查看配置的VRRP优先级（Config pri字段）和实际生效的VRRP优先级（Running pri字段）。如果两个取值不同，则进一步查看关联的Track项的编号，使用 **display track**命令定位Track项故障，并解决Track项故障
	• 针对原因二（添加虚拟 MAC 地址失败），确定 MAC 操作失败的根因并解决
	• 针对原因三（收到虚拟转发器优先级为 0 的报文，主动放弃转发权限），处理建议如下：请确认是否组网中有备份组的优先级高于本地优先级：
	  ○ 若配置正确，无需处理
	  ○ 若配置错误，请在接口视图下，使用 **vrrp ipv6 vrid priority**命令修改
	• 针对原因四（从 Advertisement 报文中学习）：无需处理
	• 针对原因五（收到 reply 报文）：无需处理
	• 针对原因六（收到 release 报文）：无需处理
	• 针对原因七（Active 定时器 超时）：无需处理
	• 针对原因八（Time-Out 定时器超时）：无需处理
	• 针对原因九（Master 为自己分配虚拟 MAC 地址）：无需处理
	• 针对原因十（VRRP备份组Down），检查备份组所在接口是否发生故障：**display interface**命令查看备份组连接接口的状态。如果接口状态显示为Down，请根据显示信息定位并处理接口故障
	• 针对原因十一（接管 AVF 的工作），处理建议如下：原来最高优先级的虚拟转发器 AVF 权重失效，请检查引起原 AVF 优先级变化的原因
	• 针对原因十二（Track 项变化），处理建议如下：
	  检查Track项的状态，可使用 **display track**命令定位Track项故障，并解决Track项故障

175.3 VRRP_VMAC_INEFFECTIVE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
日志含义	给VRRP备份组分配虚拟MAC地址失败
参数解释	$1：网络协议类型，取值包括IPv6 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：出现错误的原因，取值为Insufficient hardware resources，表示硬件资源不足
日志等级	3 (Error)
举例	VRRP6/3/VRRP_VMAC_INEFFECTIVE: The IPv6 virtual router 10 (configured on Ethernet0/0) failed to add virtual MAC: Insufficient hardware resources.
对系统的影响	本设备的VRRP备份组无法正常工作
日志产生原因	系统将VRRP备份组的虚拟MAC地址下发给驱动，驱动添加虚拟MAC地址失败，VRRP备份组将无法使用该虚拟MAC地址通信
处理建议	1. 在Probe视图下执行 **display system internal vrrp ipv6 kernel virtual-route**命令查看VRRP内核的虚拟路由器信息，收集显示信息 2. 收集设备的配置文件、日志信息、告警信息，并联系技术支持人员

176 VSRP

本节介绍 VSRP 模块输出的日志信息。

176.1 VSRP_BIND_FAILED

日志内容	Failed to bind the IP addresses and the port on VSRP peer [STRING].
日志含义	VSRP创建到对端的TCP连接失败
参数解释	$1：VSRP peer name.
日志等级	6 (Informational)
举例	VSRP/6/VSRP_BIND_FAILED: Failed to bind the IP addresses and the port on VSRP peer aaa.
对系统的影响	VSRP多机备份实例的控制通道建立失败，当VSRP关联的业务模块无法决策出主备设备的时候，会影响VSRP决策主备，最终影响VSRP功能的正常运行
日志产生原因	TCP端口正在被使用，创建到VSRP对端的TCP连接时接口绑定IP地址失败系统内存资源不足
处理建议	1. 释放内存。例如：执行 **logfile save**命令手动将日志文件缓冲区中的内容全部保存到日志文件，释放日志文件缓冲区占用的内存资源 2. 执行 **display memory**命令查看进程对内存的使用情况： ○ 如果内存占用率恢复到告警阈值以下，内存告警解除，则无需继续处理 ○ 如果内存占用率未恢复到阈值以下，则请执行 **display process**命令查看用户态进程对内存的使用情况。如果某进程占用内存较多，可以开启或者关闭进程对应的软件功能，来释放内存 3. 如果问题仍未解决，请收集告警信息和配置信息，并联系技术支持工程师

177 VXLAN

本节介绍 VXLAN 模块输出的日志信息。

177.1 VXLAN_LICENSE_UNAVAILABLE

日志内容	The VXLAN feature is disabled, because no licenses are valid.
日志含义	VXLAN的License已失效
参数解释	无
日志等级	3 (Error)
举例	VXLAN/3/VXLAN_LICENSE_UNAVAILABLE: The VXLAN feature is disabled, because no licenses are valid.
对系统的影响	VXLAN相关功能无法使用
日志产生原因	因为没有有效的License，VXLAN特性被禁用
处理建议	检查VXLAN的License，若要使用VXLAN特性，请安装有效的License

178 WEB

本节介绍 WEB 模块输出的普通日志信息。

178.1 LOGIN

日志内容	[STRING] logged in from [STRING].
日志含义	Web用户登录成功
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5 (Notification)
举例	WEB/5/LOGIN: admin logged in from 127.0.0.1.
对系统的影响	占用一个HTTP或HTTPS会话资源
日志产生原因	用户登录成功
处理建议	系统正常运行时产生的信息，无需处理

178.2 LOGIN_FAILED

日志内容	[STRING] failed to log in from [STRING].
日志含义	Web用户登录失败
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5 (Notification)
举例	WEB/5/LOGIN_FAILED: admin failed to log in from 127.0.0.1.
对系统的影响	Web用户无法正常访问系统
日志产生原因	用户登录失败，可能的原因包括： • 设备上的 HTTP 或者 HTTPS 服务未开启 • 用户没有 HTTP 或者 HTTPS 服务的权限 • 用户不存在 • 密码校验失败 • 验证码错误 • 在线用户达到上限
处理建议	• 确保设备上的 HTTP 或者 HTTPS 服务处于开启状态 • 确保该用户具有 HTTP 或者 HTTPS 类型的接入权限 • 重新输入正确的用户名、密码、验证码 • 确保为该账户设置的最大在线用户数能够满足实际接入需求 • 如果问题无法解决，请收集设备的配置文件、日志信息、告警信息，并联系 H3C 技术支持工程师

178.3 LOGOUT

日志内容	[STRING] logged out from [STRING].
日志含义	Web用户退出登录
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5 (Notification)
举例	WEB/5/LOGOUT: admin logged out from 127.0.0.1.
对系统的影响	释放一个HTTP或HTTPS会话资源
日志产生原因	用户退出登录
处理建议	系统正常运行时产生的信息，无需处理

179 WEBAUTH

本节介绍 Web 认证模块输出的日志信息。

179.1 WEBAUTH_USER_LOGON_SUCCESS

日志内容	-Username=[STRING]-IfName=[STRING]-MACAddr=[STRING]-AccessVLANID=[STRING]-AuthorizationVLANID=[STRING]; User passed Web authentication and came online successfully.
日志含义	Web认证用户上线成功
参数解释	$1：用户名 $2：接口名 $3：MAC地址 $4：接入VLAN ID $5：授权VLAN ID
日志等级	6 (Informational)
举例	WEBAUTH/6/WEBAUTH_USER_LOGON_SUCCESS: -Username=admin-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-Access VLAN ID=444-AuthorizationVLANID=444; User passed Web authentication and came online successfully.
对系统的影响	对系统无影响
日志产生原因	Web认证用户上线成功
处理建议	无需处理

179.2 WEBAUTH_USER_LOGON_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; User failed Web authentication. Reason: [STRING].
日志含义	Web认证用户上线失败
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：失败原因： • MAC address authorization failed：授权 MAC 地址失败 • VLAN authorization failed：授权 VLAN 失败 • VSI authorization failed：授权 VSI 失败 • ACL authorization failed：授权 ACL 失败 • User profile authorization failed：授权 User Profile 失败 • URL authorization failed：授权 URL 失败 • Microsegment authorization failed：授权微分段失败 • Authentication process failed：认证失败 • VSI authorization failed because of insufficient resources：资源不足，授权 VSI 失败 • ACL authorization failed because of insufficient resources：资源不足，授权 ACL 失败 • MAC address authorization failed after a MAC move：MAC 迁移后授权 MAC 失败 • VLAN authorization failed because of failure in authorization VLAN selection：选择授权 VLAN 失败 • VLAN authorization failed because a free VLAN was assigned as the authorization VLAN：授权 VLAN 为 free VLAN，授权失败 • VLAN authorization failed because of failure in authorization VLAN creation：创建授权 VLAN 失败 • VSI authorization failed because the user belongs to a free VLAN：用户加入了 free vlan，授权 VSI 失败 • VSI authorization failed because the user's access interface does not permit the user VLAN ：接口不允许用户 VLAN 通过，授权 VSI 失败 • VSI authorization failed because of failure in AC creation：创建 AC 失败，授权 VSI 失败 • ACL authorization failed because the specified ACL does not exist ：ACL 不存在，授权 ACL 失败 • ACL authorization failed because of unsupported ACL type：ACL 类型不支持，授权 ACL 失败 • ACL authorization failed because the specified ACL conflicts with other ACLs on the user's access interface：ACL 与所在接口其他 ACL 冲突，授权 ACL 失败 • ACL authorization failed because no rule was obtained for the specified ACL：无法获取任何 ACL 规则，授权 ACL 失败 • ACL authorization failed because of ACL parameter error：ACL 的相关参数出错，授权 ACL 失败

	• User profile authorization failed because an invalid user profile was assigned to the user (the authorization-fail offline feature is enabled)：配置了授权失败下线功能，User Profile 非法 • User profile authorization failed because of failure in issuing the specified user profile to driver：下驱动失败 • URL authorization failed because of insufficient resources：资源不足，授权 URL 失败 • URL authorization failed because of invalid parameter in the specified URL：URL 参数错误，授权 URL 失败 • URL authorization failed because the specified URL was not supported：不支持 URL，授权 URL 失败 • URL authorization failed because of deny rule issuing failure：下发 deny 规则失败，授权 URL 失败 • URL authorization failed because of failure in issuing the specified URL to driver：下驱动失败，授权 URL 失败 • URL authorization failed because no servers were reachable and the url-user-logoff parameter was specified：配置 Critical microsegment、Critical VSI 时指定了 url-user-logoff 参数，服务器不可达时，授权 URL 失败 • URL authorization failed because the escape critical VSI feature of port security was configured：配置了端口安全逃生到 Critical VSI 功能，授权 URL 失败
日志等级	6 (Informational)
举例	WEBAUTH/6/WEBAUTH_USER_LOGON_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0000-0001-VLANID=1-Username=0000-0000-0001; User failed Web authentication. Reason: VLAN authorization failed.
对系统的影响	Web认证失败，Web认证用户无法正常上线
日志产生原因	用户Web认证失败，具体原因见【参数解释】
处理建议	根据日志中具体提示的失败原因，进行相应处理

180 WIPS

本节介绍 WIPS 模块输出的日志信息。

180.1 APFLOOD

日志内容	-VSD=[STRING]; AP flood detected.
日志含义	检测到AP泛洪攻击
参数解释	$1：VSD名字
日志等级	5 (Notification)
举例	WIPS/5/APFLOOD: -VSD=home; AP flood detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到AP设备数量过多时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.2 AP_CHANNEL_CHANGE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Channel change detected.
日志含义	检测到AP信道改变
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5 (Notification)
举例	WIPS/5/AP_CHANNEL_CHANGE: -VSD=home-SrcMAC=1122-3344-5566; Channel change detected.
对系统的影响	AP信道发生改变，可能会影响其他工作的AP信道
日志产生原因	指定VSD内检测到指定AP信道改变时触发日志
处理建议	检查AP信道改变是否正常

180.3 ASSOCIATEOVERFLOW

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Association/Reassociation DoS attack detected.
日志含义	检测到关联/重关联DoS攻击
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5 (Notification)
举例	WIPS/5/ASSOCIATEOVERFLOW: -VSD=home-SrcMAC=1122-3344-5566; Association/Reassociation DoS attack detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到指定AP回应status code为17的关联回应帧时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.4 HONEYPOT

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Honeypot AP detected.
日志含义	检测到蜜罐AP
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5 (Notification)
举例	WIPS/5/HONEYPOT: -VSD=home-SrcMAC=1122-3344-5566; Honeypot AP detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到指定AP为蜜罐时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.5 HTGREENMODE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; HT-Greenfield AP detected.
日志含义	检测到AP使用绿野模式
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5 (Notification)
举例	WIPS/5/HTGREENMODE: -VSD=home-SrcMAC=1122-3344-5566; HT-Greenfield AP detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到指定AP携带绿野模式时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.6 MAN_IN_MIDDLE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Man-in-the-middle attack detected.
日志含义	检测到中间人攻击
参数解释	$1：VSD名字 $2：client的地址
日志等级	5 (Notification)
举例	WIPS/5/MAN_IN_MIDDLE: -VSD=home-SrcMAC=1122-3344-5566; Man-in-the-middle attack detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到指定client受到中间人攻击时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.7 WIPS_DOS

日志内容	-VSD=[STRING]; [STRING] rate attack detected.
日志含义	检测到WIPS学习表项的攻击
参数解释	$1：VSD名字 $2：设备类型 • AP：AP • Client：客户端
日志等级	5 (Notification)
举例	WIPS/5/WIPS_DOS: -VSD=home; AP rate attack detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	设备指定VSD内的表项建立速率超过阈值时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.8 WIPS_FLOOD

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] flood detected.
日志含义	检测到泛洪攻击
参数解释	$1：VSD名字 $2：Flood攻击的MAC地址 $3：Flood帧类型 • Association request：Association 帧 • Authentication：Authentication 帧 • Disassociation：Disassociation 帧 • Reassociation request：Reassociation request 帧 • Deauthentication：Deauthentication 帧 • Null data：Null data 帧 • Beacon：Beacon 帧 • Probe request：Probe request 帧 • BlockAck：BlockAck 帧 • CTS：CTS 帧 • RTS：RTS 帧 • EAPOL start：EAPOL start 帧
日志等级	5 (Notification)
举例	WIPS/5/WIPS_FLOOD: -VSD=home-SrcMAC=1122-3344-5566; Association request flood detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	一定时间内在指定VSD内检测到同一类型的报文超过阈值时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.9 WIPS_MALF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Error detected: [STRING].
日志含义	检测到畸形报文
参数解释	$1：VSD名字 $2：发送者的MAC地址 $3：畸形报文类型 • invalid ie length：非法 IE 长度 • duplicated ie：重复 IE • redundant ie：冗余 IE • invalid pkt length：报文长度无效 • illegal ibss ess：不合法 IBSS ESS • invalid source addr：无效源 MAC • overflow eapol key：EAPOL-Key 帧畸形 • malf auth：畸形认证 • malf assoc req：畸形关联请求 • malf ht ie：HT IE 畸形 • large duration：large duration 畸形 • null probe resp：null probe resp 畸形 • invalid deauth code：Deauthentication 畸形 • invalid disassoc code：解除关联码畸形 • over flow ssid：Overflow-ssid 畸形 • fata jack：fata jack 畸形
日志等级	5 (Notification)
举例	WIPS/5/WIPS_MALF: -VSD=home-SrcMAC=1122-3344-5566; Error detected: fata jack.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到指定类型的畸形报文时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.10 WIPS_SPOOF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] detected.
日志含义	检测到Spoofing攻击
参数解释	$1：VSD名字 $2：仿冒的MAC地址 $3：仿冒类型 • AP spoofing AP：AP 仿冒为 AP • AP spoofing client：AP 仿冒为 client • AP spoofing ad-hoc：AP 仿冒为 ad-hoc • Ad-hoc spoofing AP：Ad-hoc 仿冒为 AP • Client spoofing AP：Client 仿冒为 AP
日志等级	5 (Notification)
举例	WIPS/5/WIPS_SPOOF: -VSD=home-SrcMAC=1122-3344-5566; AP spoofing AP detected.
对系统的影响	当前空口环境中存在攻击时，可能会影响空口性能
日志产生原因	指定VSD内检测到设备仿冒时触发日志
处理建议	1. 配置对发起攻击的设备进行反制，并检查问题是否得到解决。 2. 如果问题仍未解决，请收集设备的配置文件、日志信息、告警信息，并联系技术支持人员。

180.11 WIPS_WEAKIV

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Weak IV detected.
日志含义	检测到采用Weak IV加密的报文
参数解释	$1：VSD名字 $2：发送者的MAC地址
日志等级	5 (Notification)
举例	WIPS/5/WIPS_WEAKIV: -VSD=home-SrcMAC=1122-3344-5566; Weak IV detected.
对系统的影响	采用Weak IV加密会增加密钥被破解的可能性，影响空口安全
日志产生原因	指定VSD内检测到采用Weak IV加密的报文
处理建议	使用安全级别更高的加密方法加密报文

180.12 WIRELESSBRIDGE

日志内容	-VSD=[STRING]-AP1=[MAC]-AP2=[MAC]]; Wireless bridge detected.
日志含义	检测到无线网桥
参数解释	$1：VSD名字 $2：AP的地址 $3：AP的地址
日志等级	5 (Notification)
举例	WIPS/5/WIRELESSBRIDGE: -VSD=home-AP1=1122-3344-5566-AP2=7788-9966-5544; Wireless bridge detected.
对系统的影响	检测到无线网桥时，当前无线网络环境存在安全隐患
日志产生原因	指定VSD内检测到AP1和AP2建立无线网桥时触发日志
处理建议	检查无线网桥是否合法