H3C 盒式交换机 日志信息参考

资料版本：6W103-20240708

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。

除了园区盒式交换机特有的日志信息外，本文还包含园区盒式交换机 Release 63xx 系列版本基于的 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

字段	描述
	• -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，不携带 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

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

参数标识	参数类型
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 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 flash:/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
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CFD	Connectivity Fault Detection
CFGMAN	Configuration Management
CONNLMT	Connect Limit
DEV	Device Management
DHCP	Dynamic Host Configuration Protocol

模块名	模块全称
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
DRNI	Distributed Resilient Network Interconnect
EDEV	Extender Device Management
ERPS	Ethernet Ring Protection Switching
ETH	Ethernet
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
FIB	Forwarding Information Base
FILTER	Filter
FIPSNG	FIP Snooping
FS	File System
FTP	File Transfer Protocol
HA	High Availability
HQOS	Hierarchical QoS
HTTPD	Hypertext Transfer Protocol Daemon
IFNET	Interface Net Management
IKE	Internet Key Exchange
IP6ADDR	IPv6 address
IPADDR	IP address
IPFW	IP Forwarding
IPSEC	IP Security
IPSG	IP Source Guard
IRDP	ICMP Router Discovery Protocol

模块名	模块全称
IRF	Intelligent Resilient Framework
ISIS	Intermediate System-to-Intermediate System
ISSU	In-Service Software Upgrade
L2PT	Layer 2 Protocol Tunneling
L2TPV2	Layer 2 Tunneling Protocol Version 2
L2VPN	Layer 2 VPN
LAGG	Link Aggregation
LDP	Label Distribution Protocol
LLDP	Link Layer Discovery Protocol
LOAD	Load Management
LOGIN	Login
LPDT	Loopback Detection
LS	Local Server
LSPV	LSP Verification
MAC	Media Access Control
MACA	MAC Authentication
MACSEC	MAC Security
MBFD	MPLS BFD
MBUF	Memory buffer
MDC	Multitenant Device Context
MFIB	Multicast Forwarding Information Base
MGROUP	Mirroring group
MPLS	Multiprotocol Label Switching
MTLK	Monitor Link
NAT	Network Address Translate
NETCONF	Network Configuration Protocol
ND	Neighbor Discovery
NQA	Network Quality Analyzer
NTP	Network Time Protocol
OAP	Open Application Platform
OPENSRC(FreeRADIUS)	Open Source
OBJP	Object Policy
OFP	OpenFlow Protocol
OPTMOD	Optical Module

模块名	模块全称
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PKTCPT	Packet Capture
PFILTER	Packet Filter
PBB	Provider Backbone Bridge
PBR	Policy Based Route
PCE	Path Computation Element
PEX	Port Extender
PIM	Protocol Independent Multicast
PING	Packet Internet Groper
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PoE	Power over Ethernet
PORTAL	Portal
PORTSEC	Port Security
PPP	Point to Point Protocol
PTP	Precision Time Protocol
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
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
SCMD	Service Control Manager
SCRLSP	Static CRLSP
SESSION	Session
SFLOW	Sampler Flow
SHELL	Shell
SLSP	Static LSP
SMLK	Smart Link

模块名	模块全称
SNMP	Simple Network Management Protocol
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
TACACS	Terminal Access Controller Access Control System
TELNETD	Telnet Daemon
TRILL	Transparent Interconnect of Lots of Links
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
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).
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).
日志说明	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.
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
举例	AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA failed.
日志说明	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

2.2 AAA_LAUNCH

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA launched.
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
举例	AAA/6/AAA_LAUNCH: -AAAType=AUTHEN-AAADomain=domain1-Service=login-UserName=cwf@system; AAA launched.
日志说明	用户发送AAA请求
处理建议	无

2.3 AAA_SUCCESS

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA succeeded.
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
举例	AAA/6/AAA_SUCCESS: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA succeeded.
日志说明	接受用户的AAA请求
处理建议	无

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.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NO_RES: Failed to accelerate IPv6 ACL 2001. The resources are insufficient.
日志说明	因硬件资源不足，系统加速ACL失败
处理建议	删除一些规则或者关闭其他ACL的加速功能，释放硬件资源

3.2 ACL_ACCELERATE_NONCONTIGUOUSMASK

日志内容	Failed to accelerate ACL [UINT32]. ACL acceleration supports only contiguous wildcard masks.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NONCONTIGUOUSMASK: Failed to accelerate ACL 2001. ACL acceleration supports only contiguous wildcard masks.
日志说明	因IPv4 ACL中的规则指定了非连续的掩码，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.3 ACL_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The operation is not supported.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 ACL 2001. The operation is not supported.
日志说明	因系统不支持ACL加速而导致ACL加速失败
处理建议	无

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.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
日志说明	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	检查ACL规则并删除不支持的配置

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.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support specifying multiple TCP flags in one rule.
日志说明	因IPv6 ACL中的规则指定了多个Tcp Flag参数，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.6 ACL_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] ACL [UINT32].
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 ACL 2001.
日志说明	因系统故障导致ACL加速失败
处理建议	无

3.7 ACL_IPV6_STATIS_INFO

日志内容	IPv6 ACL [UINT32] [STRING] [UINT64] packet(s).
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
举例	ACL/6/ACL_IPV6_STATIS_INFO: IPv6 ACL 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
日志说明	匹配上IPv6 ACL规则的报文数量发生变化
处理建议	无

3.8 ACL_NO_MEM

日志内容	Failed to configure [STRING] ACL [UINT] due to lack of memory
参数解释	$1：ACL类型 $2：ACL编号
日志等级	3
举例	ACL/3/ACL_NO_MEM: Failed to configure ACL 2001 due to lack of memory.
日志说明	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

3.9 ACL_STATIS_INFO

日志内容	ACL [UINT32] [STRING] [UINT64] packet(s).
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
举例	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	匹配上IPv4 ACL规则的报文数量发生变化
处理建议	无

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.
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
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.
日志说明	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	无需处理

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.
参数解释	无
日志等级	4
举例	APMGR/4/APMGR_AC_MEM_ALERT: The memory utilization has reached the threshold.
日志说明	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].
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
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.
日志说明	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_ADDBAC_INFO

日志内容	Add BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	APMGR/6/APMGR_ADDBAC_INFO: Add BAS AC 3ce5-a616-28cd.
日志说明	Master AC与BAS AC建立连接
处理建议	无

5.4 APMGR_AP_OFFLINE

日志内容	AP [STRING] went offline. State changed to Idle.
参数解释	$1：AP的名称
日志等级	6
举例	APMGR/6/APMGR_AP_OFFLINE: AP ap1 went offline. State changed to Idle.
日志说明	AP下线，状态变为Idle状态
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

5.5 APMGR_AP_ONLINE

日志内容	AP [STRING] went online. State changed to Run.
参数解释	$1：AP的名称
日志等级	6
举例	APMGR/6/APMGR_AP_ONLINE: AP ap1 went online. State changed to Run.
日志说明	AP上线，状态变为运行状态
处理建议	无

5.6 APMGR_CWC_IMG_DOWNLOAD_COMPLETE

日志内容	System software image file [STRING] downloading through the CAPWAP tunnel to AC [STRING] completed.
参数解释	$1：镜像文件名 $2：AC的IP地址
日志等级	6
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.
日志说明	AP从AC下载系统镜像成功
处理建议	无

5.7 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].
参数解释	$1：下载的镜像文件名 $2：AC的IP地址
日志等级	6
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.
日志说明	AP开始进行版本文件下载
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

5.8 APMGR_CWC_IMG_NO_ENOUGH_SPACE

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

5.9 APMGR_CWC_LOCAL_AC_DOWN

日志内容	CAPWAP tunnel to Central AC [STRING] went down. Reason: [STRING].
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
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.
日志说明	Central AC与Local AC之间隧道断开及断开原因
处理建议	• 检查 Central AC 与 Local AC 的连接是否正常 • 检查 Central AC 上的配置 • 检查 Local AC 上的配置

5.10 APMGR_CWC_LOCAL_AC_UP

日志内容	CAPWAP tunnel to Central AC [STRING] went up.
参数解释	$1：Central AC的IP地址
日志等级	6
举例	APMGR/6/APMGR_CWC_LOCAL_AC_UP: CAPWAP tunnel to Central AC 2.2.2.1 went up.
日志说明	Central AC与Local AC建立CAPWAP隧道
处理建议	无

5.11 APMGR_CWC_REBOOT

日志内容	AP in state [STRING] is rebooting. Reason: [STRING]
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
举例	APMGR/6/APMGR_CWC_REBOOT: AP in State Run is rebooting. Reason: AP was reset.
日志说明	AP重启及重启原因
处理建议	无

5.12 APMGR_CWC_RUN_DOWNLOAD_COMPLETE

日志内容	File [STRING] successfully downloaded through the CAPWAP tunnel to AC [STRING].
参数解释	$1：下载文件的文件名 $2：AC的IP地址
日志等级	6
举例	APMGR/6/APMGR_CWC_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel to AC 192.168.10.1.
日志说明	AP从AC下载文件成功
处理建议	无

5.13 APMGR_CWC_RUN_DOWNLOAD_START

日志内容	Started to download the file [STRING] through the CAPWAP tunnel to AC [STRING].
参数解释	$1：下载文件的文件名 $2：AC的IP地址
日志等级	6
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.
日志说明	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

5.14 APMGR_CWC_RUN_NO_ENOUGH_SPACE

日志内容	Insufficient flash memory space for downloading file [STRING].
参数解释	$1：下载文件的文件名
日志等级	6
举例	APMGR/6/APMGR_CWC_RUN_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading file ac.cfg.
日志说明	由于AP上的Flash剩余空间不足导致AP进行文件下载不成功
处理建议	建议删除AP上无用的文件以进行文件下载

5.15 APMGR_CWC_TUNNEL_DOWN

日志内容	CAPWAP tunnel to AC [STRING] went down. Reason: [STRING].
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
举例	APMGR/6/APMGR_CWC_TUNNEL_DOWN: CAPWAP tunnel to AC 192.168.10.1 went down. Reason: AP was reset.
日志说明	AP与AC之间CAPWAP隧道断开以及断开原因
处理建议	请检查AP与AC之间的网络连接是否正常

5.16 APMGR_CWC_TUNNEL_UP

日志内容	[STRING] CAPWAP tunnel to AC [STRING] went up.
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
举例	APMGR/6/APMGR_CWC_TUNNEL_UP: Master CAPWAP tunnel to AC 192.168.10.1 went up.
日志说明	AP成功连接到AC，即AP已进入Run状态
处理建议	无

5.17 APMGR_CWS_IMG_DOWNLOAD_COMPLETE

日志内容	System software image file [STRING] downloading through the CAPWAP tunnel for AP [STRING] completed.
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
举例	APMGR/6/APMGR_ CWS_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel for AP ap2 completed.
日志说明	AP已经成功完成版本文件下载
处理建议	无

5.18 APMGR_CWS_IMG_DOWNLOAD_START

日志内容	AP [STRING] started to download the system software image file [STRING].
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
举例	APMGR/6/APMGR_CWS_IMG_DOWNLOAD_START: AP ap1 started to download the system software image file 5800.ipe.
日志说明	AP开始进行版本文件下载
处理建议	无

5.19 APMGR_CWS_LOCAL_AC_DOWN

日志内容	CAPWAP tunnel to local AC [STRING] went down. Reason: [STRING].
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
举例	APMGR/4/APMGR_CWS_LOCAL_AC_DOWN: CAPWAP tunnel to local AC 1.1.1.1 went down. Reason: Serial number changed.
日志说明	Central AC与Local AC之间隧道断开及断开原因
处理建议	• 检查 Central AC 与 Local AC 的连接是否正常 • 检查 Central AC 上的配置 • 检查 Local AC 上的配置

5.20 APMGR_CWS_LOCAL_AC_UP

日志内容	CAPWAP tunnel to local AC [STRING] went up.
参数解释	$1：Local AC的IP地址
日志等级	6
举例	APMGR/6/APMGR_CWS_LOCAL_AC_UP: CAPWAP tunnel to local AC 1.1.1.1 went up.
日志说明	Central AC与 Local AC建立CAPWAP隧道
处理建议	无

5.21 APMGR_CWS_RUN_DOWNLOAD_COMPLETE

日志内容	File [STRING] successfully downloaded through the CAPWAP tunnel for AP [STRING].
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
举例	APMGR/6/APMGR_CWS_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel for AP ap2.
日志说明	AP已经成功完成文件下载
处理建议	无

5.22 APMGR_CWS_RUN_DOWNLOAD_START

日志内容	AP [STRING] started to download the file [STRING].
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
举例	APMGR/6/APMGR_CWS_RUN_DOWNLOAD_START: AP ap1 started to download the file ac.cfg.
日志说明	AP开始进行配置文件下载
处理建议	无

5.23 APMGR_CWS_TUNNEL_DOWN

日志内容	CAPWAP tunnel to AP [STRING] went down. Reason: [STRING].
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
举例	APMGR/6/APMGR_CWS_TUNNEL_DOWN: CAPWAP tunnel to AP ap1 went down. Reason: AP was reset.
日志说明	AP下线及下线原因
处理建议	• 检查设备 AP 与设备 AC 的连接是否正常 • 检查 AP 上的配置 • 检查 AC 上的配置

5.24 APMGR_CWS_TUNNEL_UP

日志内容	[STRING] CAPWAP tunnel to AP [STRING] went up.
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
举例	APMGR/6/APMGR_CWS_TUNNEL_UP: Backup CAPWAP tunnel to AP ap1 went up.
日志说明	AC端配置的AP成功上线，即此AP进入Run状态
处理建议	无

5.25 APMGR_DELBAC_INFO

日志内容	Delete BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	APMGR/6/APMGR_DELBAC_INFO: Delete BAS AC 3ce5-a616-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

5.26 APMGR_LOCAL_AC_OFFLINE

日志内容	Local AC [STRING] went offline. State changed to Idle.
参数解释	$1：Local AC的名称
日志等级	6
举例	APMGR/6/APMGR_LOCAL_AC_OFFLINE: Local AC ac1 went offline. State changed to Idle.
日志说明	Local AC下线，状态变为Idle状态
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，需要根据调试信息定位并解决问题

5.27 APMGR_LOCAL_AC_ONLINE

日志内容	Local AC [STRING] went online. State changed to Run.
参数解释	$1：Local AC的名称
日志等级	6
举例	APMGR/6/APMGR_LOCAL_AC_ONLINE: Local AC ac1 went online. State changed to Run.
日志说明	Local AC上线，状态变为运行状态
处理建议	无

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].
参数解释	$1：IP 地址 $2：接口名称
日志等级	6
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.
日志说明	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.** 请联系系统支持

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.
参数解释	$1：接口名称 $2：IP地址
日志等级	6
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.
日志说明	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	设备丢弃该ARP应答

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].
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
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.
日志说明	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	**3.** 使用 **`display qos-acl resource`** 查看硬件 ACL 资源是否充足 如果充足，则请执行步骤 2 如果不充足，则请取消部分 ACL 配置或接受当前结果 **4.** 使用 **`display memory`** 查看内存资源是否充足 如果充足，则请执行步骤 3 如果不充足，则请取消部分配置或接受当前结果 **5.** **硬件发生错误，请取消最后一次相关配置，并重新尝试**

6.4 ARP_DETECTION_LOG

日志内容	Detected an ARP attack on interface [STRING]: IP [STRING], MAC [STRING], VLAN [STRING]. [UINT32] packet(s) dropped.
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
举例	ARP/5/ARP_INSPECTION: -MDC=1; Detected an ARP attack on interface GigabitEthernet1/0/1: IP 1.1.1.1, MAC 1-1-1, VLAN 100. 2 packet(s) dropped.
日志说明	ARP Detection发现接口下连接的用户发起的攻击，并丢弃了该用户发送的报文
处理建议	检查攻击来源

6.5 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].
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
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.
日志说明	ARP检测到重复地址 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	修改IP地址

6.6 ARP_DYNAMIC

日志内容	The maximum number of dynamic ARP entries for the device reached.
参数解释	无
日志等级	6
举例	ARP/6/ARP_DYNAMIC: The maximum number of dynamic ARP entries for the device reached.
日志说明	设备学到的ARP表项总数到达最大值
处理建议	不需处理

6.7 ARP_DYNAMIC_IF

日志内容	The maximum number of dynamic ARP entries for interface [STRING] reached.
参数解释	$1：接口名
日志等级	6
举例	ARP/6/ARP_DYNAMIC_IF: The maximum number of dynamic ARP entries for interface GigabitEthernet1/0/1 reached.
日志说明	接口学到的ARP表项总数到达最大值
处理建议	无需处理

6.8 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.
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
举例	ARP/6/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for slot 2 reached.
日志说明	形式一： 指定slot学到的动态ARP表项数达到最大值 形式二： 指定chassis内slot上学到的动态ARP表项数达到最大值
处理建议	无需处理

6.9 ARP_ENTRY_CONFLICT

日志内容	The software entry for [STRING] on [STRING] and the hardware entry did not have the same [STRING].
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
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.
日志说明	ARP软件表项与硬件表项不一致，比如ARP表项的出接口
处理建议	不需要处理，ARP会主动重刷硬件表项

6.10 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].
参数解释	$1：IP地址 $2：接口名 $3：接口名
日志等级	4
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.
日志说明	接口收到主机ARP报文中的源IP与其他接口连接的主机的IP地址冲突
处理建议	检查发送ARP报文的主机的合法性。如果非法，需要断开该主机网络

6.11 ARP_LOCALPROXY_ENABLE_FAILED

日志内容	Failed to enable local proxy ARP on interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	ARP/4/ARP_LOCALPROXY_ENABLE_FAILED: -MDC=1-Slot=2; Failed to enable local proxy ARP on interface VSI-interface 1.
日志说明	VSI虚接口下开启ARP本地代理失败。主控板设置成功、非主控板设置失败的情况下在相应非主控板打印
处理建议	**6.** 检查设备相应单板是否支持本功能； **7.** 确认设备的硬件资源是否充足

6.12 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.
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
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.
日志说明	接口接收ARP报文速率超过了接口的限速值
处理建议	检查ARP报文发送主机的合法性

6.13 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].
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
举例	ARP/6/ARP_RATELIMIT_NOTSUPPORT: ARP packet rate limit is not support on slot 2.
日志说明	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

6.14 ARP_SENDER_IP_INVALID

日志内容	Sender IP [STRING] was not on the same network as the receiving interface [STRING].
参数解释	$1：IP地址 $2：接口名称
日志等级	6
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.
日志说明	接口收到ARP报文中发送端IP与本接口不在同一网段
处理建议	检查发送端IP对应主机的合法性

6.15 ARP_SENDER_MAC_INVALID

日志内容	Sender MAC [STRING] was not identical to Ethernet source MAC [STRING] on interface [STRING].
参数解释	$1：MAC 地址 $2：MAC 地址 $3：接口名称
日志等级	6
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.
日志说明	接口收到ARP报文的以太网数据帧首部中的源MAC地址和ARP报文中的发送端MAC地址不同
处理建议	检查发送端MAC地址对应主机的合法性

6.16 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].
参数解释	$1：接口名 $2：发送端IP地址 $3：目标IP地址
日志等级	6
举例	ARP/6/ ARP_SENDER_SMACCONFLICT: Packet discarded for the sender MAC address is the same as the receiving interface. Interface: GigabitEthernet1/0/1 sender IP: 1.1.2.2 target IP: 1.1.2.1,
日志说明	设备从接口GigabitEthernet1/0/1接收到的ARP报文中的源MAC和设备的MAC地址冲突
处理建议	无需处理

6.17 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].
参数解释	$1：接口名 $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
举例	ARP/6/ ARP_SENDER_SMACCONFLICT_VSI: Packet discarded for the sender MAC address is the same as the receiving interface. Interface: VSI3 sender IP: 1.1.2.2 target IP: 1.1.2.1, VSI Index: 2, Link ID: 0
日志说明	设备从VSI接口3接收到的ARP报文中的源MAC和设备的MAC地址冲突
处理建议	无需处理

6.18 ARP_SRC_MAC_FOUND_ATTACK

日志内容	An attack from MAC [STRING] was detected on interface [STRING].
参数解释	$1：MAC 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_SRC_MAC_FOUND_ATTACK: An attack from MAC 0000-5E14-0E00 was detected on interface GigabitEthernet1/0/1.
日志说明	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	检查该源MAC地址对应主机的合法性

6.19 ARP_SUP_ENABLE_FAILED

日志内容	Failed to enable ARP flood suppression on VSI [STRING].
参数解释	$1：VSI名称
日志等级	4
举例	ARP/4/ARP_SUP_ENABLE_FAILED: -MDC=1; Failed to enable ARP flood suppression on VSI vpna.
日志说明	在VSI内开启ARP泛洪抑制功能失败。本日志打印间隔时间为不低于2s，若配置下发过快，部分日志信息将不能输出
处理建议	**8.** 检查设备是否支持本功能； **9.** 确认设备的硬件资源是否足够

6.20 ARP_TARGET_IP_INVALID

日志内容	Target IP [STRING] was not the IP of the receiving interface [STRING].
参数解释	$1：IP 地址 $2：接口名称
日志等级	6
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.
日志说明	接口收到ARP报文中的目标IP与本接口IP不一致
处理建议	检查发送ARP报文的主机的合法性

6.21 ARP_THRESHOLD_REACHED

日志内容	The alarm threshold for dynamic ARP entry learning was reached on interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	ARP/4/ARP_THRESHOLD_REACHED: The alarm threshold for dynamic ARP entry learning was reached on interface GigabitEthernet1/0/1
日志说明	接口GigabitEthernet1/0/1学习的动态ARP表项个数到达了告警门限值
处理建议	检查该接口学习这么多ARP表项是否合理，网络内是否存在攻击源

6.22 ARP_USER_DUPLICATE_IPADDR_DETECT

日志内容	Detected a user IP address conflict. New user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) connecting on interface [STRING] and old user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) connecting on interface [STRING] were using the same IP address [IPADDR].
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
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) connecting on interface GigabitEthernet1/0/1 and old user (MAC 0120-1e00-0102, SVLAN 100, CVLAN 10) connecting on interface GigabitEthernet1/0/1 were using the same IP address 192.168.1.1.
日志说明	ARP检测到终端用户间IP地址冲突，某个新用户的IP地址和某个旧用户的IP地址冲突
处理建议	排查所有终端用户的IP地址，解决IP地址冲突问题

6.23 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].
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
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.
日志说明	ARP检测到终端用户发生接口迁移动作
处理建议	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

6.24 DUPIFIP

日志内容	Duplicate address [STRING] on interface [STRING], sourced from [STRING].
参数解释	$1：IP 地址 $2：接口名称 $3：MAC 地址
日志等级	6
举例	ARP/6/DUPIFIP: Duplicate address 1.1.1.1 on interface GigabitEthernet1/0/1, sourced from 0015-E944-A947.
日志说明	ARP检测到重复地址 接口收到ARP报文的发送端IP地址与该接口的IP地址重复
处理建议	修改IP地址配置

6.25 DUPIP

日志内容	IP address [STRING] conflicted with global or imported IP address, sourced from [STRING].
参数解释	$1：IP 地址 $2：MAC 地址
日志等级	6
举例	ARP/6/DUPIP: IP address 30.1.1.1 conflicted with global or imported IP address, sourced from 0000-0000-0001.
日志说明	收到ARP报文中的发送端IP地址与全局或导入的IP地址冲突
处理建议	修改IP地址配置

6.26 DUPVRRPIP

日志内容	IP address [STRING] conflicted with VRRP virtual IP address on interface [STRING], sourced from [STRING].
参数解释	$1：IP 地址 $2：接口名称 $3：MAC 地址
日志等级	6
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.
日志说明	收到ARP报文中的发送端IP与VRRP虚拟IP地址冲突
处理建议	修改IP地址配置

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	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ: IcmpType(1058)=17; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.2 ATK_ICMP_ADDRMASK_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW: IcmpType(1058)=17; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW_SZ: IcmpType(1058)=17; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.4 ATK_ICMP_ADDRMASK_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_SZ: IcmpType(1058)=17; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.5 ATK_ICMP_ADDRMASK_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL: IcmpType(1058)=18; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.6 ATK_ICMP_ADDRMASK_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW: IcmpType(1058)=18; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW_SZ: IcmpType(1058)=18; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.8 ATK_ICMP_ADDRMASK_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_SZ: IcmpType(1058)=18; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.9 ATK_ICMP_ECHO_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ECHO_REQ: IcmpType(1058)=8; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.10 ATK_ICMP_ECHO_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1004)=[UINT16]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：目的端口 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW: IcmpType(1058)=8; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DstPort(1004)=22; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.11 ATK_ICMP_ECHO_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1004)=[UINT16]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：目的端口 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW_SZ: IcmpType(1058)=8; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DstPort(1004)=22; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.12 ATK_ICMP_ECHO_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ECHO_REQ_SZ: IcmpType(1058)=8; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.13 ATK_ICMP_ECHO_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ECHO_RPL: IcmpType(1058)=0; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.14 ATK_ICMP_ECHO_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW: IcmpType(1058)=0; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.15 ATK_ICMP_ECHO_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW_SZ: IcmpType(1058)=0; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.16 ATK_ICMP_ECHO_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_ECHO_RPL_SZ: IcmpType(1058)=0; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.17 ATK_ICMP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_ICMP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.18 ATK_ICMP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_ICMP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.19 ATK_ICMP_INFO_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_INFO_REQ: IcmpType(1058)=15; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.20 ATK_ICMP_INFO_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW: IcmpType(1058)=15; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.21 ATK_ICMP_INFO_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW_SZ: IcmpType(1058)=15; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.22 ATK_ICMP_INFO_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_INFO_REQ_SZ: IcmpType(1058)=15; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.23 ATK_ICMP_INFO_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_INFO_RPL: IcmpType(1058)=16; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.24 ATK_ICMP_INFO_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW: IcmpType(1058)=16; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.25 ATK_ICMP_INFO_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW_SZ: IcmpType(1058)=16; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.26 ATK_ICMP_INFO_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_INFO_RPL_SZ: IcmpType(1058)=16; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.27 ATK_ICMP_LARGE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_LARGE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.28 ATK_ICMP_LARGE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.29 ATK_ICMP_LARGE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_LARGE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.30 ATK_ICMP_LARGE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_LARGE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.31 ATK_ICMP_PARAPROBLEM

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_PARAPROBLEM: IcmpType(1058)=12; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.32 ATK_ICMP_PARAPROBLEM_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW: IcmpType(1058)=12; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.33 ATK_ICMP_PARAPROBLEM_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW_SZ: IcmpType(1058)=12; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.34 ATK_ICMP_PARAPROBLEM_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_PARAPROBLEM_SZ: IcmpType(1058)=12; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.35 ATK_ICMP_PINGOFDEATH

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文数超过1，聚合后触发日志
处理建议	无

7.36 ATK_ICMP_PINGOFDEATH_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 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(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文触发一个日志
处理建议	无

7.37 ATK_ICMP_PINGOFDEATH_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 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(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文触发一个日志
处理建议	无

7.38 ATK_ICMP_PINGOFDEATH_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文数超过1，聚合后触发日志
处理建议	无

7.39 ATK_ICMP_REDIRECT

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_REDIRECT: IcmpType(1058)=5; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.40 ATK_ICMP_REDIRECT_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW: IcmpType(1058)=5; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.41 ATK_ICMP_REDIRECT_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW_SZ: IcmpType(1058)=5; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.42 ATK_ICMP_REDIRECT_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_REDIRECT_SZ: IcmpType(1058)=5; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.43 ATK_ICMP_SMURF

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_SMURF: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.44 ATK_ICMP_SMURF_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.45 ATK_ICMP_SMURF_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.46 ATK_ICMP_SMURF_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_SMURF_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.47 ATK_ICMP_SOURCEQUENCH

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_SOURCEQUENCH: IcmpType(1058)=4; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.48 ATK_ICMP_SOURCEQUENCH_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW: IcmpType(1058)=4; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW_SZ: IcmpType(1058)=4; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.50 ATK_ICMP_SOURCEQUENCH_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_SZ: IcmpType(1058)=4; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.51 ATK_ICMP_TIMEEXCEED

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TIMEEXCEED: IcmpType(1058)=11; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.52 ATK_ICMP_TIMEEXCEED_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW: IcmpType(1058)=11; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.53 ATK_ICMP_TIMEEXCEED_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW_SZ: IcmpType(1058)=11; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.54 ATK_ICMP_TIMEEXCEED_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TIMEEXCEED_SZ: IcmpType(1058)=11; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.55 ATK_ICMP_TRACEROUTE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_TRACEROUTE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.56 ATK_ICMP_TRACEROUTE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.57 ATK_ICMP_TRACEROUTE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.58 ATK_ICMP_TRACEROUTE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.59 ATK_ICMP_TSTAMP_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TSTAMP_REQ: IcmpType(1058)=13; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.60 ATK_ICMP_TSTAMP_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW: IcmpType(1058)=13; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW_SZ: IcmpType(1058)=13; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.62 ATK_ICMP_TSTAMP_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_SZ: IcmpType(1058)=13; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.63 ATK_ICMP_TSTAMP_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TSTAMP_RPL: IcmpType(1058)=14; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.64 ATK_ICMP_TSTAMP_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW: IcmpType(1058)=14; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW_SZ: IcmpType(1058)=14; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.66 ATK_ICMP_TSTAMP_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_SZ: IcmpType(1058)=14; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.67 ATK_ICMP_TYPE

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TYPE: IcmpType(1058)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.68 ATK_ICMP_TYPE_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW: IcmpType(1058)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.69 ATK_ICMP_TYPE_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW_SZ: IcmpType(1058)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.70 ATK_ICMP_TYPE_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_TYPE_SZ: IcmpType(1058)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.71 ATK_ICMP_UNREACHABLE

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_UNREACHABLE: IcmpType(1058)=3; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.72 ATK_ICMP_UNREACHABLE_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW: IcmpType(1058)=3; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.73 ATK_ICMP_UNREACHABLE_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW_SZ: IcmpType(1058)=3; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.74 ATK_ICMP_UNREACHABLE_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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
举例	ATK/5/ATK_ICMP_UNREACHABLE_SZ: IcmpType(1058)=3; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	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	无

7.75 ATK_ICMPV6_DEST_UNREACH

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH: Icmpv6Type(1059)=133; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.76 ATK_ICMPV6_DEST_UNREACH_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW: Icmpv6Type(1059)=133; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW_SZ: Icmpv6Type(1059)=133; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.78 ATK_ICMPV6_DEST_UNREACH_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_SZ: Icmpv6Type(1059)=133; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.79 ATK_ICMPV6_ECHO_REQ

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_REQ: Icmpv6Type(1059)=128; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.80 ATK_ICMPV6_ECHO_REQ_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW: Icmpv6Type(1059)=128; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW_SZ: Icmpv6Type(1059)=128; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.82 ATK_ICMPV6_ECHO_REQ_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_SZ: Icmpv6Type(1059)=128; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.83 ATK_ICMPV6_ECHO_RPL

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_RPL: Icmpv6Type(1059)=129; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.84 ATK_ICMPV6_ECHO_RPL_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW: Icmpv6Type(1059)=129; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW_SZ: Icmpv6Type(1059)=129; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.86 ATK_ICMPV6_ECHO_RPL_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_SZ: Icmpv6Type(1059)=129; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.87 ATK_ICMPV6_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_ICMPV6_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1007)=2002::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.88 ATK_ICMPV6_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_ICMPV6_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1007)=2002::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.89 ATK_ICMPV6_GROUPQUERY

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPQUERY: Icmpv6Type(1059)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.90 ATK_ICMPV6_GROUPQUERY_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW: Icmpv6Type(1059)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW_SZ: Icmpv6Type(1059)=130; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.92 ATK_ICMPV6_GROUPQUERY_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_SZ: Icmpv6Type(1059)=130; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.93 ATK_ICMPV6_GROUPREDUCTION

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION: Icmpv6Type(1059)=132; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.94 ATK_ICMPV6_GROUPREDUCTION_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW: Icmpv6Type(1059)=132; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW_SZ: Icmpv6Type(1059)=132; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.96 ATK_ICMPV6_GROUPREDUCTION_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_SZ: Icmpv6Type(1059)=132; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.97 ATK_ICMPV6_GROUPREPORT

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREPORT: Icmpv6Type(1059)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.98 ATK_ICMPV6_GROUPREPORT_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW: Icmpv6Type(1059)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW_SZ: Icmpv6Type(1059)=131; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.100 ATK_ICMPV6_GROUPREPORT_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_SZ: Icmpv6Type(1059)=131; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.101 ATK_ICMPV6_LARGE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.102 ATK_ICMPV6_LARGE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.103 ATK_ICMPV6_LARGE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.104 ATK_ICMPV6_LARGE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.105 ATK_ICMPV6_PACKETTOOBIG

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG: Icmpv6Type(1059)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.106 ATK_ICMPV6_PACKETTOOBIG_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW: Icmpv6Type(1059)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW_SZ: Icmpv6Type(1059)=136; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.108 ATK_ICMPV6_PACKETTOOBIG_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_SZ: Icmpv6Type(1059)=136; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.109 ATK_ICMPV6_PARAPROBLEM

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM: Icmpv6Type(1059)=135; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.110 ATK_ICMPV6_PARAPROBLEM_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW: Icmpv6Type(1059)=135; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW_SZ: Icmpv6Type(1059)=135; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.112 ATK_ICMPV6_PARAPROBLEM_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_SZ: Icmpv6Type(1059)=135; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.113 ATK_ICMPV6_TIMEEXCEED

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED: Icmpv6Type(1059)=134; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.114 ATK_ICMPV6_TIMEEXCEED_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW: Icmpv6Type(1059)=134; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW_SZ: Icmpv6Type(1059)=134; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.116 ATK_ICMPV6_TIMEEXCEED_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_SZ: Icmpv6Type(1059)=134; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.117 ATK_ICMPV6_TRACEROUTE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.118 ATK_ICMPV6_TRACEROUTE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435.
日志说明	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	无

7.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435.
日志说明	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	无

7.120 ATK_ICMPV6_TRACEROUTE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.121 ATK_ICMPV6_TYPE

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TYPE: Icmpv6Type(1059)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.122 ATK_ICMPV6_TYPE _RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TYPE_RAW: Icmpv6Type(1059)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.123 ATK_ICMPV6_TYPE _RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TYPE_RAW_SZ: Icmpv6Type(1059)=38; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.124 ATK_ICMPV6_TYPE_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $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
举例	ATK/5/ATK_ICMPV6_TYPE_SZ: Icmpv6Type(1059)=38; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	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	无

7.125 ATK_IP_OPTION

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IP_OPTION: IPOptValue(1057)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.126 ATK_IP_OPTION_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IP_OPTION_RAW: IPOptValue(1057)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.127 ATK_IP_OPTION_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IP_OPTION_RAW_SZ: IPOptValue(1057)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.128 ATK_IP_OPTION_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IP_OPTION_SZ: IPOptValue(1057)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.129 ATK_IP4_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_ACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.130 ATK_IP4_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.131 ATK_IP4_DIS_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; TcpFlag(1074)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：TCP类型（仅在TCP报文中显示该字段） $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
举例	ATK/3/ATK_IP4_DIS_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=TCP; TcpFlag(1074)=[SYN]; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式port scan时触发日志
处理建议	无

7.132 ATK_IP4_DIS_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：目的IP地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DIS_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式port scan时触发日志
处理建议	无

7.133 ATK_IP4_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_DNS_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNS Query的报文数超过阈值，触发日志发送
处理建议	无

7.134 ATK_IP4_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_DNS_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNS Query的报文数超过阈值，触发日志发送
处理建议	无

7.135 ATK_IP4_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_FIN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.136 ATK_IP4_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_FIN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.137 ATK_IP4_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_FRAGMENT: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.138 ATK_IP4_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.139 ATK_IP4_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.140 ATK_IP4_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.141 ATK_IP4_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_HTTP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.142 ATK_IP4_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_HTTP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.143 ATK_IP4_IMPOSSIBLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_IMPOSSIBLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.144 ATK_IP4_IMPOSSIBLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.145 ATK_IP4_IMPOSSIBLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.146 ATK_IP4_IMPOSSIBLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_IMPOSSIBLE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.147 ATK_IP4_IPSWEEP

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009060657.
日志说明	报文满足ip sweep时触发日志
处理建议	无

7.148 ATK_IP4_IPSWEEP_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009060657.
日志说明	报文满足ip sweep时触发日志
处理建议	无

7.149 ATK_IP4_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; DstIPAddr(1007)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：目的IP地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; DstIPAddr(1007)=6.1.1.5; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足port scan时触发日志
处理建议	无

7.150 ATK_IP4_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; DstIPAddr(1007)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：目的IP地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; DstIPAddr(1007)=6.1.1.5; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足port scan时触发日志
处理建议	无

7.151 ATK_IP4_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_RST_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.152 ATK_IP4_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_RST_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.153 ATK_IP4_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_SYN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.154 ATK_IP4_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP4_SYN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.155 ATK_IP4_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_SYNACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.156 ATK_IP4_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_SYNACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.157 ATK_IP4_TCP_ALLFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.158 ATK_IP4_TCP_ALLFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.159 ATK_IP4_TCP_ALLFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.160 ATK_IP4_TCP_ALLFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.161 ATK_IP4_TCP_FINONLY

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_FINONLY: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.162 ATK_IP4_TCP_FINONLY_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.163 ATK_IP4_TCP_FINONLY_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.164 ATK_IP4_TCP_FINONLY_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.165 ATK_IP4_TCP_INVALIDFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.166 ATK_IP4_TCP_INVALIDFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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 TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4 TCP报文触发一个日志
处理建议	无

7.167 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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 TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4 TCP报文触发一个日志
处理建议	无

7.168 ATK_IP4_TCP_INVALIDFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.169 ATK_IP4_TCP_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_LAND: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.170 ATK_IP4_TCP_LAND_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.171 ATK_IP4_TCP_LAND_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.172 ATK_IP4_TCP_LAND_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_LAND_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.173 ATK_IP4_TCP_NULLFLAG

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=4.
日志说明	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	无

7.174 ATK_IP4_TCP_NULLFLAG_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.175 ATK_IP4_TCP_NULLFLAG_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.176 ATK_IP4_TCP_NULLFLAG_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=4.
日志说明	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	无

7.177 ATK_IP4_TCP_SYNFIN

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.178 ATK_IP4_TCP_SYNFIN_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.179 ATK_IP4_TCP_SYNFIN_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.180 ATK_IP4_TCP_SYNFIN_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.181 ATK_IP4_TCP_WINNUKE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=5.
日志说明	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	无

7.182 ATK_IP4_TCP_WINNUKE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.183 ATK_IP4_TCP_WINNUKE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.184 ATK_IP4_TCP_WINNUKE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=5.
日志说明	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	无

7.185 ATK_IP4_TEARDROP

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_TEARDROP: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.186 ATK_IP4_TEARDROP_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.187 ATK_IP4_TEARDROP_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.188 ATK_IP4_TEARDROP_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_TEARDROP_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	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	无

7.189 ATK_IP4_TINY_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_TINY_FRAGMENT: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=6.
日志说明	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	无

7.190 ATK_IP4_TINY_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.191 ATK_IP4_TINY_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	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	无

7.192 ATK_IP4_TINY_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=6.
日志说明	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	无

7.193 ATK_IP4_UDP_BOMB

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_UDP_BOMB: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.194 ATK_IP4_UDP_BOMB_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.195 ATK_IP4_UDP_BOMB_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.196 ATK_IP4_UDP_BOMB_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_UDP_BOMB_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.197 ATK_IP4_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP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
举例	ATK/3/ATK_IP4_UDP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.198 ATK_IP4_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP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
举例	ATK/3/ATK_IP4_UDP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	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	无

7.199 ATK_IP4_UDP_FRAGGLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=11.
日志说明	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	无

7.200 ATK_IP4_UDP_FRAGGLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.201 ATK_IP4_UDP_FRAGGLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.202 ATK_IP4_UDP_FRAGGLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=11.
日志说明	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	无

7.203 ATK_IP4_UDP_SNORK

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_UDP_SNORK: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.204 ATK_IP4_UDP_SNORK_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.205 ATK_IP4_UDP_SNORK_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.206 ATK_IP4_UDP_SNORK_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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	3
举例	ATK/3/ATK_IP4_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	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	无

7.207 ATK_IP6_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_ACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	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	无

7.208 ATK_IP6_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	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	无

7.209 ATK_IP6_DIS_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DIS_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=UDP; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式port scan时触发日志
处理建议	无

7.210 ATK_IP6_DIS_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DIS_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式port scan时触发日志
处理建议	无

7.211 ATK_IP6_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_DNS_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNS Query的IPV6报文数超过阈值，触发日志发送
处理建议	无

7.212 ATK_IP6_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_DNS_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNS Query的IPV6报文数超过阈值，触发日志发送
处理建议	无

7.213 ATK_IP6_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_FIN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	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	无

7.214 ATK_IP6_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_FIN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	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	无

7.215 ATK_IP6_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $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
举例	ATK/3/ATK_IP6_FRAGMENT: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	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	无

7.216 ATK_IP6_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	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	无

7.217 ATK_IP6_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	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	无

7.218 ATK_IP6_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $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
举例	ATK/3/ATK_IP6_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	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	无

7.219 ATK_IP6_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_HTTP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的HTTP的IPV6 Get报文数超过阈值，触发日志发送
处理建议	无

7.220 ATK_IP6_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_HTTP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的HTTP的IPV6 Get报文数超过阈值，触发日志发送
处理建议	无

7.221 ATK_IP6_IMPOSSIBLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $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
举例	ATK/3/ATK_IP6_IMPOSSIBLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	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	无

7.222 ATK_IP6_IMPOSSIBLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	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	无

7.223 ATK_IP6_IMPOSSIBLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	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	无

7.224 ATK_IP6_IMPOSSIBLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $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
举例	ATK/3/ATK_IP6_IMPOSSIBLE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	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	无

7.225 ATK_IP6_IPSWEEP

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_IPSWEEP: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=UDP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ip sweep时触发日志
处理建议	无

7.226 ATK_IP6_IPSWEEP_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_IPSWEEP_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ip sweep时触发日志
处理建议	无

7.227 ATK_IP6_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：目的IPv6地址 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=UDP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; DstIPv6Addr(1037)=2::2; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足port scan时触发日志
处理建议	无

7.228 ATK_IP6_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：目的IPv6地址 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; DstIPv6Addr(1037)=2::2; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足port scan时触发日志
处理建议	无

7.229 ATK_IP6_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_RST_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	无

7.230 ATK_IP6_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_RST_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	无

7.231 ATK_IP6_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_SYN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	满足周期内指定目的地址的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	无

7.232 ATK_IP6_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_SYN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	满足周期内指定目的地址的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	无

7.233 ATK_IP6_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_SYNACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	无

7.234 ATK_IP6_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_SYNACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	无

7.235 ATK_IP6_TCP_ALLFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.236 ATK_IP6_TCP_ALLFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.237 ATK_IP6_TCP_ALLFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.238 ATK_IP6_TCP_ALLFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.239 ATK_IP6_TCP_FINONLY

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.240 ATK_IP6_TCP_FINONLY_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.241 ATK_IP6_TCP_FINONLY_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.242 ATK_IP6_TCP_FINONLY_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.243 ATK_IP6_TCP_INVALIDFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.244 ATK_IP6_TCP_INVALIDFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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 TCP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IPV6 TCP报文触发一个日志
处理建议	无

7.245 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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 TCP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IPV6 TCP报文触发一个日志
处理建议	无

7.246 ATK_IP6_TCP_INVALIDFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.247 ATK_IP6_TCP_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6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	无

7.248 ATK_IP6_TCP_LAND_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6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IPV6源目的地址相同的TCP报文触发一个日志
处理建议	无

7.249 ATK_IP6_TCP_LAND_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6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IPV6源目的地址相同的TCP报文触发一个日志
处理建议	无

7.250 ATK_IP6_TCP_LAND_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6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	无

7.251 ATK_IP6_TCP_NULLFLAG

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.252 ATK_IP6_TCP_NULLFLAG_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.253 ATK_IP6_TCP_NULLFLAG_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.254 ATK_IP6_TCP_NULLFLAG_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.255 ATK_IP6_TCP_SYNFIN

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.256 ATK_IP6_TCP_SYNFIN_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.257 ATK_IP6_TCP_SYNFIN_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.258 ATK_IP6_TCP_SYNFIN_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.259 ATK_IP6_TCP_WINNUKE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.260 ATK_IP6_TCP_WINNUKE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.261 ATK_IP6_TCP_WINNUKE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.262 ATK_IP6_TCP_WINNUKE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.263 ATK_IP6_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_UDP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定IPV6目的地址的UDP报文数超过阈值，触发日志
处理建议	无

7.264 ATK_IP6_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
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
举例	ATK/3/ATK_IP6_UDP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定IPV6目的地址的UDP报文数超过阈值，触发日志
处理建议	无

7.265 ATK_IP6_UDP_FRAGGLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.266 ATK_IP6_UDP_FRAGGLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.267 ATK_IP6_UDP_FRAGGLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.268 ATK_IP6_UDP_FRAGGLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.269 ATK_IP6_UDP_SNORK

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.270 ATK_IP6_UDP_SNORK_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.271 ATK_IP6_UDP_SNORK_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.272 ATK_IP6_UDP_SNORK_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.273 ATK_IPOPT_ABNORMAL

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IPOPT_ABNORMAL: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011072002; EndTime_c(1012)=20131011072502; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，两个以上IP选项置位的报文数超过1，聚合后触发日志
处理建议	无

7.274 ATK_IPOPT_ABNORMAL_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，两个以上IP选项置位的报文首包触发日志；日志聚合开关关闭，每个两个以上IP选项置位的报文触发一个日志
处理建议	无

7.275 ATK_IPOPT_ABNORMAL_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，两个以上IP选项置位的报文首包触发日志；日志聚合开关关闭，每个两个以上IP选项置位的报文触发一个日志
处理建议	无

7.276 ATK_IPOPT_ABNORMAL_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP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
举例	ATK/3/ATK_IPOPT_ABNORMAL_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011072002; EndTime_c(1012)=20131011072502; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，两个以上IP选项置位的报文数超过1，聚合后触发日志
处理建议	无

7.277 ATK_IPOPT_LOOSESRCROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE: IPOptValue(1057)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.278 ATK_IPOPT_LOOSESRCROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW: IPOptValue(1057)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.279 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW_SZ: IPOptValue(1057)=131; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.280 ATK_IPOPT_LOOSESRCROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)= [UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_SZ: IPOptValue(1057)=131; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.281 ATK_IPOPT_RECORDROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE: IPOptValue(1057)=7; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.282 ATK_IPOPT_RECORDROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW: IPOptValue(1057)=7; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.283 ATK_IPOPT_RECORDROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW_SZ: IPOptValue(1057)=7; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.284 ATK_IPOPT_RECORDROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_SZ: IPOptValue(1057)=7; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.285 ATK_IPOPT_ROUTEALERT

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT: IPOptValue(1057)=148; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.286 ATK_IPOPT_ROUTEALERT_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW: IPOptValue(1057)=148; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.287 ATK_IPOPT_ROUTEALERT_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW_SZ: IPOptValue(1057)=148; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.288 ATK_IPOPT_ROUTEALERT_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_SZ: IPOptValue(1057)=148; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.289 ATK_IPOPT_SECURITY

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_SECURITY: IPOptValue(1057)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131009091022; EndTime_c(1012)=20131009091522; AtkTimes(1050)=2.
日志说明	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	无

7.290 ATK_IPOPT_SECURITY_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW: IPOptValue(1057)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.291 ATK_IPOPT_SECURITY_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW_SZ: IPOptValue(1057)=130; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.292 ATK_IPOPT_SECURITY_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_SECURITY_SZ: IPOptValue(1057)=130; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131009091022; EndTime_c(1012)=20131009091522; AtkTimes(1050)=2.
日志说明	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	无

7.293 ATK_IPOPT_STREAMID

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STREAMID: IPOptValue(1057)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.294 ATK_IPOPT_STREAMID_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW: IPOptValue(1057)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.295 ATK_IPOPT_STREAMID_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW_SZ: IPOptValue(1057)=136; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.296 ATK_IPOPT_STREAMID_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STREAMID_SZ: IPOptValue(1057)=136; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.297 ATK_IPOPT_STRICTSRCROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE: IPOptValue(1057)=137; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.298 ATK_IPOPT_STRICTSRCROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW: IPOptValue(1057)=137; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.299 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW_SZ: IPOptValue(1057)=137; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.300 ATK_IPOPT_STRICTSRCROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_SZ: IPOptValue(1057)=137; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.301 ATK_IPOPT_TIMESTAMP

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP: IPOptValue(1057)=68; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.302 ATK_IPOPT_TIMESTAMP_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW: IPOptValue(1057)=68; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.303 ATK_IPOPT_TIMESTAMP_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW_SZ: IPOptValue(1057)=68; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	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	无

7.304 ATK_IPOPT_TIMESTAMP_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel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	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_SZ: IPOptValue(1057)=68; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	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	无

7.305 ATK_IPV6_EXT_HEADER

日志内容	IPv6ExtHeader(1060)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IPv6 扩展头 $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	5
举例	ATK/5/ATK_IPV6_EXT_HEADER: IPv6ExtHeader(1060)=43; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

7.306 ATK_IPV6_EXT_HEADER_RAW

日志内容	IPv6ExtHeader(1060)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IPv6 扩展头 $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
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW: IPv6ExtHeader(1060)=43; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.307 ATK_IPV6_EXT_HEADER_RAW_SZ

日志内容	IPv6ExtHeader(1060)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IPv6 扩展头 $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
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW_SZ: IPv6ExtHeader(1060)=43; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	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	无

7.308 ATK_IPV6_EXT_HEADER_SZ

日志内容	IPv6ExtHeader(1060)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IPv6 扩展头 $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	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_SZ: IPv6ExtHeader(1060)=43; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	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	无

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.
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
举例	ATM/5/ATM_PVCDOWN: Interface ATM2/0/2 PVC 0/100 status is down.
日志说明	PVC的状态转变为down。触发该日志的原因可能有：PVC所属ATM接口状态转变为down、PVC的OAM状态转变为down或该PVC被shutdown
处理建议	**10.** 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： **11.** 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 **12.** 如果 OAM State 字段显示为 DOWN • 当两台路由器直连时： o 检查对端接口上创建的 PVC 的 VPI/VCI 是否与本端相同 o 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**） o 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 o 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 **13.** 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

8.2 ATM_PVCUP

日志内容	Interface [STRING] PVC [UINT16]/[UINT16] status is 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
举例	ATM/5/ATM_PVCUP: Interface ATM2/0/2 PVC 0/100 status is up.
日志说明	PVC的状态转变为up
处理建议	**14.** 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, Sta: [STRING]->[STRING], Diag: [STRING]
参数解释	$1：BFD会话的源地址、目的地址、接口和消息类型 $2：变化前状态机的名称 $3：变化后状态机的名称 $4：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
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).
日志说明	BFD会话的状态机发生变化。当BFD会话up或down时出现此信息。如果出现会话异常丢失的情况，可能由高错误率或高丢包率导致
处理建议	需要检查是否BFD配置的问题或网络出现拥塞

9.2 BFD_REACHED_UPPER_LIMIT

日志内容	The total number of BFD sessions [ULONG] reached the upper limit. Can’t create a new session.
参数解释	$1：BFD会话总数
日志等级	5
举例	BFD/5/BFD_REACHED_UPPER_LIMIT: The total number of BFD session 100 reached upper limit.
日志说明	BFD会话总数达到上限
处理建议	请检查BFD会话配置

10 BGP

本节介绍 BGP 模块输出的日志信息。

10.1 BGP_EXCEED_ROUTE_LIMIT

日志内容	BGP.[STRING]: The number of routes from peer [STRING] ([STRING]) exceeds the limit [UINT32].
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
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.
日志说明	从对等体学到的路由数量超过了允许的最大路由数量
处理建议	检查是否是攻击导致，如果是，需要管理员找到问题原因，对攻击进行防御 否则，查看是否需要增大允许的最大路由数量

10.2 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]%).
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
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%).
日志说明	接收的路由数量占允许的最大路由数量的百分比达到了阈值
处理建议	检查是否是攻击导致，如果是，需要管理员找到问题原因，对攻击进行防御 否则，查看是否需要增大以下数值： • 允许的最大路由数量 • 接收的路由数量占允许的最大路由数量百分比的阈值

10.3 BGP_LOG_ROUTE_FLAP

日志内容	BGP.[STRING]: The route [STRING] [STRING]/[UINT32] learned from peer [STRING] ([STRING]) flapped.
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
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.
日志说明	从对等体学到的路由发生抖动
处理建议	检查路由抖动是否不正常，如果是，需要管理员找到路由抖动的源头，并制定解决方案

10.4 BGP_MEM_ALERT

日志内容	BGP process received system memory alert [STRING] event.
参数解释	$1：内存告警的类型，包括stop、start
日志等级	5
举例	BGP/5/BGP_MEM_ALERT: BGP process received system memory alert start event.
日志说明	BGP模块收到内存告警信息
处理建议	如果内存告警类型为start，请检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

10.5 BGP_PEER_LICENSE_REACHED

日志内容	Number of peers in Established state reached the license limit.
参数解释	无
日志等级	5
举例	BGP/5/BGP_PEER_LICENSE_REACHED: Number of peers in Established state reached the license limit.
日志说明	处于established状态的邻居数量已达到license规格限制
处理建议	检查license安装情况，判断是否需要安装新的license

10.6 BGP_ROUTE_LICENSE_REACHED

日志内容	Number of [STRING] routes reached the license limit.
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
举例	BGP/5/BGP_ROUTE_LICENSE_REACHED: Number of IPv4-UNC public routes reached the license limit.
日志说明	指定类型的路由数量已达到license规格限制
处理建议	检查license安装情况，判断是否需要安装新的license 当指定类型的路由数量降低到License的规格限制以下或者License规格限制扩大时，之前被丢弃的路由不能自动恢复，需要用户手工配置，以便重新学习路由

10.7 BGP_STATE_CHANGED

日志内容	BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING].
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：变化前的状态名称 $4：变化后的状态名称
日志等级	5
举例	BGP/5/BGP_STATE_CHANGED: BGP.vpn1: 192.99.0.2 state has changed from ESTABLISHED to IDLE.
日志说明	BGP对等体的状态发生变化 此日志信息当BGP对等体从其他状态进入Established状态或者从Established状态进入其他状态时产生
处理建议	如果BGP对等体意外Down，请检查网络是否发生故障或丢包

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].
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
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.
日志说明	日志开关打开；手动配置一个黑名单；scan检测添加一个黑名单；触发日志发送
处理建议	无

11.2 BLS_ENTRY_DEL

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
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
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.
日志说明	日志开关打开；手动删除一个黑名单；老化删除一个黑名单；触发日志发送
处理建议	无

11.3 BLS_IPV6_ENTRY_ADD

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
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
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.
日志说明	日志开关打开；手动配置一个黑名单；scan检测添加一个黑名单；触发日志发送
处理建议	无

11.4 BLS_IPV6_ENTRY_DEL

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
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
举例	BLS/5/BLS_IPV6_ENTRY_DEL: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; Reason(1052)=Configuration.
日志说明	日志开关打开；手动删除一个黑名单；老化删除一个黑名单；触发日志发送
处理建议	无

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. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
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
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.
日志说明	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
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. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
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
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.
日志说明	MEP收到错误的CCM报文，该报文包含错误的MEP ID或生存时间
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].
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
举例	CFD/6/CFD_LOST_CCM: MEP 1 in SI 7 failed to receive CCMs from RMEP 2.
日志说明	MEP在3.5个CCM报文发送周期内没有收到CCM报文，可能的原因是链路故障或远端MEP在此期间没有发送CCM报文
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]
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
举例	CFD/6/CFD_RECEIVE_CCM: MEP 1 in SI 7 received CCMs from RMEP 2.
日志说明	MEP收到远端MEP发送的CCM报文
处理建议	无

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]
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
举例	CFGMAN/5/CFGMAN_ARCHIVE_SCP_FAIL: Archive configuration to SCP server failed: IP = 192.168.21.21, Directory = /test/, Username = admin
日志说明	设备向SCP服务器保存配置文件失败时，打印此日志信息
处理建议	无

13.2 CFGMAN_CFGCHANGED

日志内容	-EventIndex=[INT32]-CommandSource=[INT32]-ConfigSource=[INT32]-ConfigDestination=[INT32]; Configuration changed.
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
举例	CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=[6]-CommandSource=[snmp]-ConfigSource=[startup]-ConfigDestination=[running]; Configuration changed.
日志说明	如果配置在过去的十分钟内发生了变化，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
处理建议	无

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.
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
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.
日志说明	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
处理建议	无

13.4 CFGMAN_OPTCOMPLETION

日志内容	-OperateType=[INT32]-OperateTime=[INT32]-OperateState=[INT32]-OperateEndTime=[INT32]; Operation completed.
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
举例	CFGMAN/5/CFGMAN_OPTCOMPLETION: -OperateType=[running2startup]-OperateTime=[248]-OperateState=[success]-OperateEndTime=[959983]; Operation completed.
日志说明	操作完成后记录操作的类型、状态以及时间
处理建议	请根据OperateState的值定位、处理问题

14 CONNLMT

本节介绍连接数限制模块输出的日志信息。

14.1 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];
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
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;
日志说明	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

14.2 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];
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
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;
日志说明	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

14.3 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];
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
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;
日志说明	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

14.4 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];
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
举例	CONNLMT/6/CONNLMT_IPV6_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=2001::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;
日志说明	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

15 DEV

本节介绍 DEV（设备管理）模块输出的日志信息。

15.1 BOARD_INSERTED

日志内容	Board was inserted on [STRING], type is unknown.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/5/BOARD_INSERTED: Board was inserted on slot 1, type is unknown.
日志说明	有单板插入设备，但是单板类型未知
处理建议	单板插入设备后，需要一段时间才能完成启动，该段时间内，提示该日志，属于正常情况，无需处理

15.2 BOARD_REBOOT

日志内容	Board is rebooting on [STRING].
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/5/BOARD_REBOOT: Board is rebooting on slot 1.
日志说明	用户在重启指定slot，或者指定slot因为异常而重启
处理建议	**15.** 检查是否有用户在重启指定 slot **16.** 如果没有用户重启，等待指定 slot 重新启动后，通过 **`display version`** 命令、对应指定 slot 信息中的 Last reboot reason 字段，查看重启原因 **17.** 如果重启原因为异常重启，请联系技术支持

15.3 BOARD_REMOVED

日志内容	Board was removed from [STRING], type is [STRING].
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
举例	DEV/3/BOARD_REMOVED: Board was removed from slot 1, type is LSQ1FV48SA.
日志说明	一块LPU或者备用MPU被拔出。设备退出IRF
处理建议	**18.** 检查对应单板是否插紧 **19.** 检查对应单板是否损坏 **20.** 重新插入单板或更换单板 **21.** 重新将设备加入 IRF

15.4 BOARD_STATE_FAULT

日志内容	Board state changed to Fault on [STRING], type is [STRING].
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
举例	DEV/2/BOARD_STATE_FAULT: Board state changed to Fault on slot 1, type is LSQ1FV48SA.
日志说明	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：请联系技术支持

15.5 BOARD_STATE_NORMAL

日志内容	Board state changed to Normal on [STRING], type is [STRING].
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
举例	DEV/5/BOARD_STATE_NORMAL: Board state changed to Normal on slot 1, type is LSQ1FV48SA.
日志说明	一块新插入的LPU或者备用MPU完成了初始化
处理建议	无

15.6 BOARD_STATE_STARTING

日志内容	Board state changed to Starting on [STRING], type is unknown.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/5/BOARD_STATE_STARTING: Board state changed to Starting on slot 1, type is unknown.
日志说明	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
处理建议	**22.** 查看单板型号和设备型号是否适配 **23.** 查看启动文件和设备软件版本以及硬件是否适配 **24.** 请联系技术支持

15.7 CFCARD_INSERTED

日志内容	CF card was inserted in [STRING] CF card slot [INT32].
参数解释	$1：chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号
日志等级	4
举例	DEV/4/CFCARD_INSERTED: CF card was inserted in slot 1 CF card slot 1.
日志说明	一块CF卡安装到了指定槽位
处理建议	无

15.8 CFCARD_REMOVED

日志内容	CF card was removed from [STRING] CF card slot [INT32].
参数解释	$1：chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号
日志等级	3
举例	DEV/3/CFCARD_REMOVED: CF card was removed from slot 1 CF card slot 1.
日志说明	一块CF卡被拔出
处理建议	**25.** 检查 CF 卡是否插紧 **26.** 检查 CF 卡是否损坏 **27.** 重新安装 CF 卡或更换 CF 卡

15.9 CHASSIS_REBOOT

日志内容	Chassis [INT32] is rebooting now.
参数解释	$1：chassis编号
日志等级	5
举例	DEV/5/CHASSIS_REBOOT: Chassis 1 is rebooting now.
日志说明	用户在重启成员设备，或者成员设备因为异常而重启
处理建议	**28.** 检查是否有用户在重启成员设备 **29.** 如果没有用户重启，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 **30.** 如果重启原因为异常重启，请联系技术支持

15.10 DEV_CLOCK_CHANGE

日志内容	-User=[STRING]-IPAddr=[IPADDR]; System clock changed from [STRING] to [STRING].
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
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.
日志说明	系统时间发生了变更
处理建议	无

15.11 DEV_FAULT_TOOLONG

日志内容	Card in [STRING] is still in Fault state for [INT32] minutes.
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
举例	DEV/4/DEV_FAULT_TOOLONG: Card in slot 1 is still in Fault state for 60 minutes.
日志说明	单板长期处于Fault状态
处理建议	**31.** 重启单板尝试恢复 **32.** 联系工程师分析解决

15.12 DEV_MNT_LogToIC

日志内容	The device don't support Power-to-Port Fan [UINT32].
参数解释	$1：风扇槽位号
日志等级	5
举例	DEV/5/DEV_MNT_LogToIC: The device don't support Power-to-Port Fan 1.
日志说明	设备不支持抽风风扇
处理建议	• 检查是否使用了抽风风扇 • 拔下换成吹风风扇

15.13 DYINGGASP

日志内容	Power failure or manual power-off occurred.
参数解释	无
日志等级	0
举例	DYINGGASP/0/DYINGGASP: Power failure or manual power-off occurred.
日志说明	设备掉电，发送断电告警
处理建议	**33.** 检查设备电源连接是否正确 **34.** 如果为电源模块故障，请更换电源模块 **35.** 联系工程师定位解决

15.14 FAN_ABSENT

日志内容	形式一： Fan [INT32] is absent. 形式二： Chassis [INT32] fan [INT32] is absent.
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
举例	DEV/3/FAN_ABSENT: Fan 2 is absent.
日志说明	指定位置没有风扇，或风扇被拔出
处理建议	**36.** 如果指定位置没有风扇，则可能因散热不好，引起设备温度升高，建议安装风扇 **37.** 如果有风扇，检查风扇框是否插紧 **38.** 检查风扇框是否损坏 **39.** 重新安装风扇框或更换风扇框

15.15 FAN_DIRECTION_NOT_PREFERRED

日志内容	Fan [INT32] airflow direction is not preferred on [STRING], please check it.
参数解释	$1：风扇ID $2：chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/FAN_DIRECTION_NOT_PREFERRED: Fan 1 airflow direction is not preferred on slot 1, please check it.
日志说明	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	**40.** 根据机房通风系统的风向，选择风向一致的型号的风扇 **41.** 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

15.16 FAN_FAILED

日志内容	形式一： Fan [INT32] failed. 形式二： Chassis [INT32] fan [INT32] failed.
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
举例	DEV/2/FAN_FAILED: Fan 2 failed.
日志说明	风扇出现了故障，停止工作
处理建议	更换风扇

15.17 FAN_RECOVERED

日志内容	形式一： Fan [INT32] recovered. 形式二： Chassis [INT32] fan [INT32] recovered.
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	5
举例	DEV/5/FAN_RECOVERED: Fan 2 recovered.
日志说明	插入风扇，稍后，风扇转入正常工作状态
处理建议	无

15.18 MAD_DETECT

日志内容	Multi-active devices detected, please fix it.
参数解释	无
日志等级	1
举例	DEV/1/MAD_DETECT: Multi-active devices detected, please fix it.
日志说明	当收到冲突消息的时候，检测到冲突，需要解决冲突问题
处理建议	**42.** 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 **43.** 使用 **display irf link** 查看 IRF 链路信息，确认故障的 IRF 链路 **44.** 手工修复状态为 DOWN 的 IRF 链路

15.19 POWER_ABSENT

日志内容	形式一： Power [INT32] is absent. 形式二： Chassis [INT32] power [INT32] is absent.
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
举例	DEV/3/POWER_ABSENT: Power 1 is absent.
日志说明	电源模块被拔出
处理建议	**45.** 检查电源是否插紧 **46.** 检查电源是否损坏 **47.** 重新安装电源或更换电源

15.20 POWER_FAILED

日志内容	形式一： Power [INT32] failed. 形式二： Chassis [INT32] power [INT32] failed.
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
举例	DEV/2/POWER_FAILED: Power 1 failed.
日志说明	电源模块出现故障
处理建议	更换电源

15.21 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.
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
举例	DEV/3/POWER_MONITOR_ABSENT: Power monitor unit 1 is absent.
日志说明	电源监控模块被拔出
处理建议	**48.** 检查电源监控模块是否插紧 **49.** 检查电源监控模块是否损坏 **50.** 重新安装电源监控模块或更换电源监控模块

15.22 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.
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
举例	DEV/2/POWER_MONITOR_FAILED: Power monitor unit 1 failed.
日志说明	电源监控模块出现故障
处理建议	更换电源监控模块

15.23 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.
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	5
举例	DEV/5/POWER_MONITOR_RECOVERED: Power monitor unit 1 recovered.
日志说明	电源监控模块插入后，状态从Failed或者Absent状态转换为Normal
处理建议	无

15.24 POWER_RECOVERED

日志内容	形式一： Power [INT32] recovered. 形式二： Chassis [INT32] power [INT32] recovered.
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	5
举例	DEV/5/POWER_RECOVERED: Power 1 recovered.
日志说明	电源模块插入后，状态从Failed或者Absent状态转换为Normal
处理建议	无

15.25 RPS_ABSENT

日志内容	形式一： RPS [INT32] is absent. 形式二： Chassis [INT32] RPS [INT32] is absent.
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
举例	DEV/3/RPS_ABSENT: RPS 1 is absent.
日志说明	冗余电源模块被拔出
处理建议	**51.** 检查冗余电源模块是否插紧 **52.** 检查冗余电源模块是否损坏 **53.** 重新安装冗余电源模块或更换冗余电源模块

15.26 RPS_FAILED

日志内容	形式一： RPS [INT32] failed. 形式二： Chassis [INT32] RPS [INT32] failed.
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
举例	DEV/2/RPS_FAILED: RPS 2 failed.
日志说明	冗余电源模块没供电或者故障
处理建议	**54.** 检查冗余电源线是否插紧 **55.** 检查冗余电源模块是否故障 **56.** 对于可插拔的冗余电源模块，请重新安装冗余电源模块或更换冗余电源模块

15.27 RPS_NORMAL

日志内容	形式一： RPS [INT32] is normal. 形式二： Chassis [INT32] RPS [INT32] is normal.
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
举例	DEV/5/RPS_NORMAL: RPS 1 is normal.
日志说明	冗余电源模块插入后，状态正常
处理建议	无

15.28 SUBCARD_FAULT

日志内容	Subcard state changed to Fault on [STRING] subslot [INT32], type is [STRING].
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
举例	DEV/2/SUBCARD_FAULT: Subcard state changed to Fault on slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	子卡重启，稍后，子卡状态转换为Fault，或者子卡故障
处理建议	**57.** 如果后续子卡状态可以变为 Normal，则无需处理 **58.** 如果子卡一直处于 Falut 状态，则子卡故障，更换子卡

15.29 SUBCARD_INSERTED

日志内容	Subcard was inserted in [STRING] subslot [INT32], type is [STRING].
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
举例	DEV/4/SUBCARD_INSERTED: Subcard was inserted in slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	一块子卡安装到了指定槽位
处理建议	无

日志内容	This firmware does not exist on Slot [UINT32] . Please download the firmware to nandflash first, then re-plug the SSAE-CS card.
参数解释	$1：设备slot号
日志等级	4
举例	DEV/4/SUBCARD_INSERTED: This firmware does not exist on Slot 1. Please download the firmware to nandflash first, then re-plug the SSAE-CS card.
日志说明	检查固件是否存在
处理建议	先将固件下载到nandflash，然后重新插入LSWM2FPGA NetStream或LSWM2FPGAB NetStream接口模块扩展卡

15.30 SUBCARD_REBOOT

日志内容	Subcard is rebooting on [STRING] subslot [INT32].
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
举例	DEV/5/SUBCARD_REBOOT: Subcard is rebooting on slot 1 subslot 1.
日志说明	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	如果子卡重启后能正常运行，则无需处理。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，请联系技术支持

15.31 SUBCARD_REMOVED

日志内容	Subcard was removed from [STRING] subslot [INT32], type is [STRING].
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
举例	DEV/3/SUBCARD_REMOVED: Subcard was removed from slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	一块子卡被拔出
处理建议	**59.** 检查子卡是否插紧 **60.** 检查子卡是否损坏 **61.** 重新安装子卡或更换子卡

15.32 SYSTEM_REBOOT

日志内容	System is rebooting now.
参数解释	无
日志等级	5
举例	DEV/5/SYSTEM_REBOOT: System is rebooting now.
日志说明	用户在重启系统，或者系统因为异常而重启
处理建议	**62.** 检查是否有用户在重启系统 **63.** 如果没有用户重启，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 **64.** 如果重启原因为异常重启，请联系技术支持

15.33 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].
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
举例	DEV/4/TEMPERATURE_ALARM: Temperature is greater than the high-temperature alarming threshold on slot 1 sensor inflow 1.
日志说明	传感器温度超过了严重级（Alarm）高温告警门限。环境温度太高或者风扇异常
处理建议	**65.** 检查环境温度是否过高，保持设备环境正常通风 **66.** **`display fan`** 命令检查风扇是否不在或故障，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

15.34 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].
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
举例	DEV/4/TEMPERATURE_LOW: Temperature is less than the low-temperature threshold on slot 1 sensor inflow 1.
日志说明	传感器温度低于低温告警门限
处理建议	环境温度过低，改善环境温度

15.35 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].
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	5
举例	DEV/5/TEMPERATURE_NORMAL: Temperature changed to normal on slot 1 sensor inflow 1.
日志说明	传感器温度指示正常（大于低温告警门限，小于一般级高温告警门限）
处理建议	无

15.36 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.
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
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.
日志说明	传感器温度高过了关断级高温告警门限，设备将自动关闭。环境温度太高或者风扇异常
处理建议	**67.** 检查环境温度是否过高，保持设备环境通风正常 **68.** **`display fan`** 命令检查风扇是否不在或故障，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

15.37 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].
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
举例	DEV/4/TEMPERATURE_WARNING: Temperature is greater than the high-temperature warning threshold on slot 1 sensor inflow 1.
日志说明	传感器温度高过了一般级高温告警门限。环境温度太高或者风扇异常
处理建议	**69.** 检查环境温度是否过高，保持设备环境通风正常 **70.** **`display fan`** 命令检查风扇是否不在或故障，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

15.38 VCHK_VERSION_INCOMPATIBLE

日志内容	Software version of [STRING] is incompatible with that of the MPU.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/ VCHK_VERSION_INCOMPATIBLE: Software version of slot 1 is incompatible with that of the MPU.
日志说明	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	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

16 DHCP

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

16.1 DHCP_NORESOURCES

日志内容	Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
参数解释	无
日志等级	3
举例	DHCP/3/DHCP_NORESOURCES: Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
日志说明	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	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功能

16.2 DHCP_NOTSUPPORTED

日志内容	Failed to apply filtering rules for DHCP packets because some rules are not supported.
参数解释	无
日志等级	3
举例	DHCP/3/DHCP_NOTSUPPORTED: Failed to apply filtering rules for DHCP packets because some rules are not supported.
日志说明	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	无

17 DHCPR

本节介绍 DHCPR（IPv4 DHCP Relay）模块输出的日志信息。

17.1 DHCPR_SERVERCHANGE

日志内容	Switched to the server at [IPADDR] (VPN name: [STRING]) because the current server did not respond. Switched to the DHCP server at [IPADDR] (Public network) because the current DHCP server did not respond.
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
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.
日志说明	因为DHCP中继无法从当前的DHCP服务器得到应答，所以DHCP中继切换到下一台指定VPN内或公网内的DHCP服务器申请IP地址
处理建议	无需处理

17.2 DHCPR_SWITCHMASTER

日志内容	Switched to the master DHCP server at [IPADDR].
参数解释	$1：主用DHCP服务器的IP地址
日志等级	3
举例	DHCPR/3/DHCPR_SWITCHMASTER: -MDC=1; Switched to the master DHCP server at 2.2.2.2.
日志说明	DHCP中继可以配置延迟回切时间，如果当时生效的为备用服务器，在经过延迟时间，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

18 DHCPS

本节介绍 DHCPS（ipv4 DHCP server）模块输出的日志信息。

18.1 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.
参数解释	$1：ipv4 DHCP服务器所在接口的接口名 $2：分配给ipv4 DHCP客户端的ipv4地址 $3：分配给ipv4 DHCP客户端的ipv4地址租约时长 $4：ipv4 DHCP客户端的MAC地址 $5：ipv4 DHCP服务器地址池名
日志等级	5
举例	DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server received a DHCP client's request packet on interface Ethernet0/2, and allocated an IP address 1.0.0.91(lease 86400 seconds) for the DHCP client(MAC 0000-0000-905a) from p1 pool.
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端分配一个ipv4地址租约
处理建议	无

18.2 DHCPS_CONFLICT_IP

日志内容	A conflict IP [IPADDR] from [STRING] pool was detected by DHCP server on interface [STRING].
参数解释	$1：冲突的IPv4地址 $2：IPv4 DHCP服务器地址池名 $3：IPv4 DHCP服务器所在接口的接口名
日志等级	5
举例	DHCPS/5/DHCPS_CONFLICT_IP: A conflict IP 100.1.1.1 from p1 pool was detected by DHCP server on interface Ethernet0/2.
日志说明	IPv4 DHCP服务器从地址池中删除一个冲突地址
处理建议	无

18.3 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]).
参数解释	$1：IPv4 DHCP服务器所在接口的接口名 $2：IPv4 DHCP服务器地址池名 $3：分配给IPv4 DHCP客户端的IPv4地址 $4：IPv4 DHCP客户端的MAC地址
日志等级	5
举例	DHCPS/5/DHCPS_EXTEND_IP: DHCP server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IP 1.0.0.91, MAC 0000-0000-905a).
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端续约
处理建议	无

18.4 DHCPS_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPS/4/DHCPS_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCP server保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

18.5 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]).
参数解释	$1：IPv4 DHCP服务器地址池名 $2：分配给IPv4 DHCP客户端的IPv4地址 $3：分配给IPv4 DHCP客户端的IPv4地址租约时长 $4：IPv4 DHCP客户端的MAC地址
日志等级	5
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).
日志说明	IPv4 DHCP服务器回收一个分配给IPv4 DHCP客户端的地址租约
处理建议	无

18.6 DHCPS_VERIFY_CLASS

日志内容	Illegal DHCP client-PacketType=[STRING]-ClientAddress=[MAC];
参数解释	$1：报文类型 $2：IPv4 DHCP客户端的硬件地址
日志等级	5
举例	DHCPS/5/DHCPS_VERIFY_CLASS: Illegal DHCP client-PacketType= DHCPDISCOVER-ClientAddress=0000-5e01-0104;
日志说明	IPv4 DHCP服务器对客户端报文白名单验证不通过
处理建议	确认该DHCP客户端是否合法

19 DHCPS6

本节介绍 DHCPS6（IPv6 DHCP server）模块输出的 日志信息。

19.1 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 DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的ipv6地址 $3：分配给IPv6 DHCP客户端的ipv6地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID $6：IPv6 DHCP服务器地址池名
日志等级	5
举例	DHCPS6/5/DHCPS6_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 DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端分配一个IPv6地址租约
处理建议	无

19.2 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 DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的IPv6前缀地址 $3：分配给IPv6 DHCP客户端的IPv6前缀地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID $6：IPv6 DHCP服务器地址池名
日志等级	5
举例	DHCPS6/5/DHCPS6_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 DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端分配一个IPv6前缀地址租约
处理建议	无

19.3 DHCPS6_CONFLICT_ADDRESS

日志内容	A conflict IPv6 address [IPADDR] from [STRING] pool was detected by DHCPv6 server on interface [STRING].
参数解释	$1：冲突的IPv6地址 $2：IPv6 DHCP服务器地址池名 $3：IPv6 DHCP服务器所在接口的接口名
日志等级	5
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.
日志说明	IPv6 DHCP服务器从地址池删除一个冲突地址
处理建议	无

19.4 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]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：IPv6 DHCP服务器地址池名 $3：分配给IPv6 DHCP客户端的IPv6地址 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_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).
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端地址续约
处理建议	无

19.5 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]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：IPv6 DHCP服务器地址池名 $3：分配给IPv6 DHCP客户端的IPv6前缀地址 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_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).
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端前缀地址续约
处理建议	无

19.6 DHCPS6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPS6/4/DHCPS6_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv6 server保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

19.7 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]).
参数解释	$1：IPv6 DHCP服务器地址池名 $2：分配给IPv6 DHCP客户端的IPv6地址 $3：分配给IPv6 DHCP客户端的IPv6地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_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).
日志说明	IPv6 DHCP服务器回收一个分配给IPv6客户端的地址租约
处理建议	无

19.8 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]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的IPv6前缀地址 $3：分配给IPv6 DHCP客户端的IPv6前缀地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_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).
日志说明	IPv6 DHCP服务器回收一个分配给IPv6客户端的前缀地址租约
处理建议	无

20 DHCPSP4

本节介绍 DHCPSP4 模块输出的日志信息。

20.1 DHCPSP4_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPSP4/4/DHCPSP4_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv4 snooping保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

21 DHCPSP6

本节介绍 DHCPSP6 模块输出的 日志信息。

21.1 DHCPSP6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPSP6/4/DHCPSP6_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv6 snooping保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

22 DIAG

本节介绍 diagnostic 模块输出的日志信息。

22.1 CPU_MINOR_RECOVERY

日志内容	CPU usage recovered to normal state.
参数解释	无
日志等级	5
举例	DIAG/5/CPU_MINOR_THRESHOLD: CPU usage recovered to normal state.
日志说明	当设备处于CPU低级别告警状态，并且采样值小于或等于恢复门限时，解除CPU低级别告警状态，CPU使用率恢复到正常
处理建议	根据提示信息操作设备，合理使用CPU资源

22.2 CPU_MINOR_THRESHOLD

日志内容	CPU usage is in minor alarm state.
参数解释	无
日志等级	4
举例	DIAG/4/CPU_MINOR_THRESHOLD: CPU usage is in minor alarm state.
日志说明	当CPU使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低级别告警状态，并定期输出该日志，直到CPU低级别告警状态解除
处理建议	根据提示信息操作设备，合理使用CPU资源

22.3 CPU_SEVERE_RECOVERY

日志内容	CPU usage severe alarm removed.
参数解释	无
日志等级	5
举例	DIAG/5/CPU_RECOVERY: CPU usage severe alarm removed.
日志说明	当设备处于CPU高级别告警状态，并且采样值小于或等于低级别告警门限时，解除CPU高级别告警状态，输出该日志
处理建议	无

22.4 CPU_SEVERE_THRESHOLD

日志内容	CPU usage is in severe alarm state.
参数解释	无
日志等级	3
举例	DIAG/3/CPU_THRESHOLD: CPU usage is in severe alarm state.
日志说明	当CPU使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，并定期输出该日志，直到CPU高级别告警状态解除
处理建议	请使用**display current-configuration | include "monitor cpu-usage"**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

22.5 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]

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
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
日志说明	内存告警。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，系统会输出该信息，告知用户内存的具体使用情况
处理建议	**71.** 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**

	72. 检查 ARP、路由表信息，排除设备受到非法攻击可能 **73.** 检查和优化组网，减少路由条目或者更换更高规格的设备

22.6 MEM_BELOW_THRESHOLD

日志内容	Memory usage has dropped below [STRING] threshold.
参数解释	$1：内存告警门限级别，包括： ○ minor：一级 ○ severe：二级 ○ critical：三级
日志等级	1
举例	DIAG/1/MEM_BELOW_THRESHOLD: Memory usage has dropped below critical threshold.
日志说明	内存告警解除。当系统剩余空闲内存大于内存恢复门限时，系统会输出该信息
处理建议	无

22.7 MEM_EXCEED_THRESHOLD

日志内容	Memory [STRING] threshold has been exceeded.
参数解释	$1：内存告警门限级别，包括： ○ minor：一级 ○ severe：二级 ○ critical：三级
日志等级	1
举例	DIAG/1/MEM_EXCEED_THRESHOLD: Memory minor threshold has been exceeded.
日志说明	内存告警。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，系统会输出该信息，并通知各业务模块进行自动修复：比如，不再申请新的内存或者释放部分内存
处理建议	**74.** 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** **75.** 检查 ARP、路由表信息，排除设备受到非法攻击可能 **76.** 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 DLDP

本节介绍 DLDP 模块输出的日志信息。

23.1 DLDP_AUTHENTICATION_FAILED

日志内容	The DLDP packet failed the authentication because of unmatched [STRING] field.
参数解释	$1：验证字段 o AUTHENTICATION PASSWORD：表示验证字不匹配 o AUTHENTICATION TYPE：表示验证类型不匹配 o INTERVAL：表示通告间隔不匹配
日志等级	5
举例	DLDP/5/DLDP_AUTHENTICATION_FAILED: The DLDP packet failed the authentication because of unmatched INTERVAL field.
日志说明	报文验证失败。可能的原因包括：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

23.2 DLDP_LINK_BIDIRECTIONAL

日志内容	DLDP detected a bidirectional link on interface [STRING].
参数解释	$1：接口名
日志等级	6
举例	DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface Ethernet1/1.
日志说明	DLDP在接口上检测到双向链路
处理建议	无

23.3 DLDP_LINK_SHUTMODECHG

日志内容	DLDP automatically [STRING] interface [STRING] because the port shutdown mode was changed [STRING].
参数解释	$1：接口关闭模式指定的动作 o blocked：表示 DLDP 关闭了端口 o 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 o from manual to auto：表示由手动模式切换到自动模式 o from manual to hybrid：表示由手动模式切换到混合模式 o from hybrid to auto：表示由混合模式切换到自动模式 o from hybrid to manual：表示由混合模式切换到手动模式
日志等级	5
举例	DLDP/5/DLDP_LINK_SHUTMODECHG: DLDP automatically blocked interface Ethernet1/1 because the port shutdown mode was changed from manual to auto.
日志说明	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	无

23.4 DLDP_LINK_UNIDIRECTIONAL

日志内容	DLDP detected a unidirectional link on interface [STRING]. [STRING].
参数解释	$1：接口名 $2：接口关闭模式所指定的动作 o DLDP automatically blocked the interface：表示 DLDP 自动关闭了端口 o Please manually shut down the interface：表示需要用户手动关闭端口 o DLDP automatically shut down the interface. Please manually bring up the interface：表示 DLDP 自动关闭了端口，需要用户手动打开端口
日志等级	3
举例	DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface Ethernet1/1. DLDP automatically blocked the interface.
日志说明	DLDP在接口上检测到单向链路
处理建议	检查线缆是否错接、脱落或者出现其他故障

23.5 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].
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	5
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.
日志说明	接口删除了一个已老化的邻居
处理建议	无

23.6 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].
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	6
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.
日志说明	接口检测到一个处于确定状态的邻居
处理建议	无

23.7 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].
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
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.
日志说明	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
处理建议	无

24 DOT1X

本节介绍 802.1X（DOT1X）模块输出的日志信息。

24.1 DOT1X_CONFIG_NOTSUPPORT

日志内容	802.1X is not supported on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_CONFIG_NOTSUPPORT: 802.1X is not supported on interface GigabitEthernet1/0/1.
日志说明	接口不支持802.1X特性
处理建议	无

24.2 DOT1X_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING] -ErrCode=[STRING]; User failed 802.1X authentication. Reason: [STRING].
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
日志等级	6
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.
日志说明	用户802.1X认证失败
处理建议	查看失败原因并修改相关配置

24.3 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.
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
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.
日志说明	802.1X用户认证成功
处理建议	无

24.4 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.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名
日志等级	6
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.
日志说明	802.1X认证失败但通过开放认证模式认证成功
处理建议	无

24.5 DOT1X_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; 802.1X user was logged off.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X user was logged off.
日志说明	802.1X用户正常下线
处理建议	无

24.6 DOT1X_LOGOFF (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; 802.1X open user was logged off.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X open user was logged off.
日志说明	802.1X open用户正常下线
处理建议	无

24.7 DOT1X_LOGOFF_ABNORMAL

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X user was logged off abnormally.
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
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.
日志说明	802.1X用户异常下线
处理建议	查看异常下线原因或进行后续操作

24.8 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.
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
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.
日志说明	802.1X open用户异常下线
处理建议	查看异常下线原因或进行后续操作

24.9 DOT1X_MACBINDING_EXIST

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; MAC address was already bound to interface [STRING].
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
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.
日志说明	用户MAC地址已绑定在其它端口，用户无法上线
处理建议	在其它端口取消MAC地址绑定

24.10 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.
参数解释	$1：IP地址 $2：接口名
日志等级	3
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.
日志说明	当在接口上使能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	暂不使能802.1X，之后尝试重新使能802.1X

24.11 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.
参数解释	$1：接口名
日志等级	3
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.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备不能下发允许该接口上DHCP协议和DNS协议报文通过的规则
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

24.12 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].
参数解释	$1：HTTP报文源MAC地址 $2：接口名
日志等级	3
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.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备不能重定向在指定接口上收到的源MAC地址为特定地址的HTTP报文
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

24.13 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.
参数解释	$1：接口名
日志等级	3
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.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备不能指定规则允许该接口重定向HTTP报文
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

24.14 DOT1X_NOTENOUGH_ENABLEDOT1X_RES

日志内容	Failed to enable 802.1X on interface [STRING] due to lack of ACL resources.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_ENABLEDOT1X_RES: Failed to enable 802.1X on interface Ethernet3/1/2 due to lack of ACL resources.
日志说明	因为ACL资源不足，不能配置接口的802.1X特性
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

24.15 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.
参数解释	$1：接口名
日志等级	3
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.
日志说明	因为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

24.16 DOT1X_SMARTON_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; User failed SmartOn authentication because [STRING].
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
举例	DOT1X/6/DOT1X_SMARTON_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; User failed SmartOn authentication because the password is mismatched.
日志说明	SmartOn认证失败，及其原因
处理建议	根据失败原因修改相关配置

24.17 DOT1X_UNICAST_NOT_EFFECTIVE

日志内容	The unicast trigger feature is enabled but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_UNICAST_NOT_EFFECTIVE: The unicast trigger feature is enabled but is not effective on interface Ethernet3/1/2.
日志说明	单播触发特性在接口上不生效，因为该接口不支持单播触发特性
处理建议	更换到支持单播触发功能的接口上对用户进行802.1X认证

25 DRNI

本节介绍 DRNI 模块输出的日志信息。

25.1 DRNI_AUTO-RECOVERY_TIMEOUT

日志内容	The reload delay timer timed out. Please check configuration of the DR system.
参数解释	无
日志等级	4
举例	DRNI/4/DRNI_AUTO-RECOVERY_TIMEOUT: The reload delay timer timed out. Please check configuration of the DR system.
日志说明	DR系统自动恢复定时器超时，DR系统仅一台设备启动或DR系统出现双主情况
处理建议	• 检查对端 DR 设备是否正常启动 • 检查 IPL 和 Keepalive 链路是否正常 • 检查自动恢复定时器配置值是否过小

25.2 DRNI_GLBCONSISTENCYCHECK_SUCCESS

日志内容	Global type [UINT16] configuration consistency check succeeded.
参数解释	$1：配置一致性检查类型，1或2
日志等级	6
举例	DRNI/6/DRNI_GLBCONSISTENCYCHECK_SUCCESS: Global type 1 configuration consistency check succeeded.
日志说明	分布式聚合全局配置一致性检查结果一致
处理建议	无

25.3 DRNI_GLBCONSISTENCYCHECK_FAILURE

日志内容	Global type [UINT16] configuration consistency check failed.
参数解释	$1：配置一致性检查类型，1或2
日志等级	6
举例	DRNI/6/DRNI_GLBCONSISTENCYCHECK_FAILURE: Global type 1 configuration consistency check failed.
日志说明	分布式聚合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 drni 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

25.4 DRNI_IFCONSISTENCYCHECK_SUCCESS

日志内容	DR interface [STRING] type [UINT16] configuration consistency check succeeded.
参数解释	$1：接口名称 $2：配置一致性检查类型，1或2
日志等级	6
举例	DRNI/6/DRNI_IFCONSISTENCYCHECK_SUCCESS: DR interface Bridge-Aggregation 2 type 1 configuration consistency check succeeded.
日志说明	分布式聚合接口配置一致性接口检查结果一致
处理建议	无

25.5 DRNI_IFCONSISTENCYCHECK_FAILURE

日志内容	DR interface [STRING] type [UINT16] configuration consistency check failed.
参数解释	$1：接口名称 $2：配置一致性检查类型，1或2
日志等级	6
举例	DRNI/6/DRNI_IFCONSISTENCYCHECK_FAILURE: DR interface Bridge-Aggregation 2 type 1 configuration consistency check failed.
日志说明	分布式聚合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 drni 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

25.6 DRNI_IFEVENT_DR_BIND

日志内容	Interface [STRING] was assigned to DR group [UINT32].
参数解释	$1：二层聚合接口 $2：分布式聚合组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_BIND: Interface Bridge-Aggregation1 was assigned to DR group 1.
日志说明	聚合接口加入分布式聚合组，触发该日志的原因为用户设置
处理建议	无

25.7 DRNI_IFEVENT_DR_GLOBALDOWN

日志内容	The state of DR interface [STRING] changed to globally down.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_GLOBALDOWN: The state of DR interface Bridge-Aggregation1 changed to globally down.
日志说明	分布式聚合接口变为全局DOWN状态，触发该日志的原因为两台DR设备相同DR口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DR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

25.8 DRNI_IFEVENT_DR_GLOBALUP

日志内容	The state of DR interface [STRING] changed to globally up.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_GLOBALUP: The state of DR interface Bridge-Aggregation1 changed to globally up.
日志说明	分布式聚合接口变为全局UP状态，触发该日志的原因为两台DR设备相同DR口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

25.9 DRNI_IFEVENT_DR_NOSELECTED

日志内容	Local DR group [UINT32] does not have Selected member ports.
参数解释	$1：DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_NOSELECTED: Local DR group 10 does not have Selected member ports.
日志说明	DR组对应的聚合组内无选中端口
处理建议	检查聚合组成员端口配置或者线缆连接情况

25.10 DRNI_IFEVENT_DR_PEER_NOSELECTED

日志内容	Peer DR group [UINT32] does not have Selected member ports.
参数解释	$1：DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_PEER_NOSELECTED: Peer DR group 10 does not have Selected member ports.
日志说明	对端DR组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

25.11 DRNI_IFEVENT_DR_PEER_SELECTED

日志内容	Peer DR group [UINT32] has Selected member ports.
参数解释	$1：DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_PEER_SELECTED: Peer DR group 10 has Selected member ports.
日志说明	对端DR组对应的聚合组内存在选中端口
处理建议	无

25.12 DRNI_IFEVENT_DR_SELECTED

日志内容	Local DR interface [STRING] has Selected member ports.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_SELECTED: Local DR interface Bridge-Aggregation1 has Selected member ports.
日志说明	DR接口对应的聚合组内存在选中端口
处理建议	无

25.13 DRNI_IFEVENT_DR_UNBIND

日志内容	Interface [STRING] was removed from DR group [UINT32].
参数解释	$1：二层聚合接口 $2：分布式聚合组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_UNBIND: Interface Bridge-Aggregation1 was removed from DR group 1.
日志说明	聚合接口退出分布式聚合组，触发该日志的原因为用户设置
处理建议	无

25.14 DRNI_IFEVENT_IPP_BIND

日志内容	Interface [STRING] was configured as IPP [UINT16].
参数解释	$1：二层聚合接口 $2：IPP口编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_BIND: Interface Bridge-Aggregation1 was configured as IPP 1.
日志说明	聚合接口配置为IPP口，触发该日志的原因为用户设置
处理建议	无

25.15 DRNI_IFEVENT_IPP_DOWN

日志内容	IPP [STRING] went down.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_DOWN: IPP Bridge-Aggregation1 went down.
日志说明	IPP口变为DOWN状态，触发该日志的原因为DR系统两端不能正常收发DRCP协议报文
处理建议	• 检查 DR 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 • 检查配置为 IPP 口的二层聚合接口状态

25.16 DRNI_IFEVENT_IPP_UNBIND

日志内容	Configuration for IPP [UINT16] was removed from interface [STRING].
参数解释	$1：IPP口编号 $2：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_UNBIND: Configuration for IPP 1 was removed from interface Bridge-Aggregation1.
日志说明	删除IPP口，触发该日志的原因为用户设置
处理建议	无

25.17 DRNI_IFEVENT_IPP_UP

日志内容	IPP [STRING] came up.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_UP: IPP Bridge-Aggregation1 came up.
日志说明	IPP口变为UP状态，触发该日志的原因为DR系统两端能正常收发DRCP协议报文
处理建议	无

25.18 DRNI_IPP_BLOCK

日志内容	The status of IPP [STRING] changed to blocked.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IPP_BLOCK: The status of IPP Bridge-Aggregation20 changed to blocked.
日志说明	IPP口变为阻塞状态，该状态下IPP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IPP口down时，IPP口变为阻塞状态
处理建议	• 检查 IPL 连接线缆是否正常 • 检查 IPL 两端配置是否一致

25.19 DRNI_IPP_UNBLOCK

日志内容	The status of IPP [STRING] changed to unblocked.
参数解释	$1：二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IPP_UNBLOCK: The status of IPP Bridge-Aggregation20 changed to unblocked.
日志说明	IPP口变为非阻塞状态，该状态下IPP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IPP口up时，IPP口变为非阻塞状态
处理建议	无

25.20 DRNI_KEEPALIVEINTERVAL_MISMATCH

日志内容	Keepalive interval on the local DR device is different from that on the neighbor.
参数解释	无
日志等级	6
举例	DRNI/6/DRNI_KEEPALIVEINTERVAL_MISMATCH: Keepalive interval on the local DR device is different from that on the neighbor.
日志说明	DR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DR系统两端配置的Keepalive报文发包间隔不一致
处理建议	将DR系统两端的Keepalive报文发包间隔配置一致

25.21 DRNI_KEEPALIVELINK_DOWN

日志内容	Keepalive link went down.
参数解释	无
日志等级	6
举例	DRNI/6/DRNI_KEEPALIVELINK_DOWN: Keepalive link went down.
日志说明	KEEPALIVE链路变为DOWN状态，触发该日志的原因为DR系统两端不能正常收发Keepalive协议报文
处理建议	• 检查所选取的三层链路状态 • 检查 DR 设备的 Keepalive 配置，两端源 IP、目的 IP 是否匹配

25.22 DRNI_KEEPALIVELINK_UP

日志内容	Keepalive link came up.
参数解释	无
日志等级	6
举例	DRNI/6/DRNI_KEEPALIVELINK_UP: Keepalive link came up.
日志说明	KEEPALIVE链路变为UP状态，触发该日志的原因为DR系统两端能正常收发Keepalive协议报文
处理建议	无

25.23 DRNI_SECONDARY_MADDOWN

日志内容	All service interfaces on the secondary device changed to the MAD ShutDown state because the IPL went down. Please check the settings on the DR devices on both ends of the IPL.
参数解释	无
日志等级	4
举例	DRNI/6/DRNI_SECONDARY_MADDOWNN: All service interfaces on the secondary device changed to the MAD ShutDown state because the IPL went down. Please check the settings on the DR devices on both ends of the IPL.
日志说明	IPL down时，Secondary设备会关闭所有业务接口
处理建议	检查IPL两端配置

25.24 DRNI_SYSEVENT_DEVICEROLE_CHANGE

日志内容	Device role changed from [STRING] to [STRING].
参数解释	$1：旧的设备角色，Primary或Secondary $2：新的设备角色，Primary或Secondary
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_DEVICEROLR_CHANGE: Device role changed from Secondary to Primary.
日志说明	分布式聚合系统设备角色变化，触发该日志的原因为用户设置
处理建议	无

25.25 DRNI_SYSEVENT_MAC_CHANGE

日志内容	System MAC address changed from [STRING] to [STRING].
参数解释	$1：旧的系统MAC $2：新的系统MAC
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_MAC_CHANGE: System MAC address changed from 1-1-1 to 2-2-2.
日志说明	分布式聚合系统MAC变化，触发该日志的原因为用户设置
处理建议	无

25.26 DRNI_SYSEVENT_NUMBER_CHANGE

日志内容	System number changed from [STRING] to [STRING].
参数解释	$1：旧的系统编号 $2：新的系统编号
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_NUMBER_CHANGE: System number changed from 1 to 2.
日志说明	分布式聚合系统编号变化，触发该日志的原因为用户设置
处理建议	无

25.27 DRNI_SYSEVENT_PRIORITY_CHANGE

日志内容	System priority changed from [UINT16] to [UINT16].
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
举例	DRNI/6/DRNI_SYSEVENT_PRIORITY_CHANGE: System priority changed from 123 to 564.
日志说明	分布式聚合系统优先级改变，触发该日志的原因为用户设置
处理建议	无

26 DRV

本节介绍产品驱动输出的日志信息。

26.1 DRV_CLK

日志内容	Phase lock changed, current phase lock mode is [STRING].
参数解释	$1：锁相状态，具体状态如下 • Freerun：自由运行 • Holdover：保持 • Unknown：未知 • Locked ：锁定 • Pre-locked：预锁 1 • Pre-locked2：预锁 2 • Lost Phase：丢失
日志等级	5
举例	DRV/5/DRV_CLK: Phase lock changed, current phase lock mode is Freerun.
日志说明	相位锁定状态变更时，打印当前相位锁定状态
处理建议	无

日志内容	SSM out level changed, current SSM out level is [STRING].
参数解释	$1：SSM等级，具体如下 • Unknown：同步状态未知 • PRC：基准参考时钟 • SSUA：转接局时钟 • SSUB：本地局时钟) • SEC：设备时钟 • DNU：不应用作同步
日志等级	5
举例	DRV/5/DRV_CLK: SSM out level changed, current SSM out level is Unknown.
日志说明	SSM等级变更时，打印当前的输出SSM等级
处理建议	无

日志内容	Selected Source changed, current source is [STRING].
参数解释	$1：时钟源，具体如下 • PTP：PTP 时钟源 • 端口名称：接口时钟 • N/A：PTP 和接口时钟源都不是
日志等级	5
举例	DRV/5/DRV_CLK: Selected Source changed, current source is PTP.
日志说明	时钟源变更时打印当前时钟源，仅当时钟锁相状态为锁定时打印
处理建议	无

日志内容	Get PHY Status error! ifIndex = [UINT32]
参数解释	$1：时钟源端口索引
日志等级	3
举例	DRV/3/DRV_CLK: Get PHY Status error! ifIndex = 1
日志说明	在根据时钟源配置显示字符串时，获取物理链接状态失败时打印
处理建议	无

日志内容	p1 = [UINT32]
参数解释	$1：时钟源SSM等级的异常值
日志等级	3
举例	DRV/3/DRV_CLK: p1 = 10
日志说明	打印SSM等级的异常值
处理建议	无

26.2 DRV_DEVM

日志内容	The Mac chip's temperature is more than [INT32], reboot now!
参数解释	$1：设备MAC芯片重启温度
日志等级	2
举例	DRV/2/DRV_DEVM: The Mac chip's temperature is more than 105, reboot now!
日志说明	MAC芯片温度超过重启温度，设备即将重启
处理建议	无

26.3 DRV_PTP

日志内容	PTP TOD is biased，The bias is [UINT64] ns in PHY [UNIT32]
参数解释	$1：时钟偏差数值 $2：PHY芯片号
日志等级	5
举例	DRV/5/DRV_PTP: PTP TOD is biased，The bias is 24 ns in PHY 2
日志说明	TOD单元调整时钟偏差，打印存在偏差的PHY芯片号和时钟偏差数值
处理建议	无

日志内容	Not SyncE Slave Port!
参数解释	无
日志等级	3
举例	DRV/3/DRV_PTP: Not SyncE Slave Port!
日志说明	配置同步以太网后，提示存在千兆电口不是从时钟端口
处理建议	将端口设置为同步以太网的从时钟端口

日志内容	SyncE is not configured, Clock Recovery will work when SyncE is set!
参数解释	无
日志等级	6
举例	DRV/6/DRV_PTP: SyncE is not configured, Clock Recovery will work when SyncE is set!
日志说明	配置同步以太网功能后时钟同步恢复，并打印该日志信息
处理建议	配置同步以太网功能

27 DRVPLAT

本节介绍驱动平台模块输出的日志信息。

27.1 DRVPLAT_COPP_FAIL

日志内容	Due to hardware resource limitations, the protocol match criterion cannot take effect.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DRVPLAT_COPP_FAIL: Due to hardware resource limitations, the protocol match criterion cannot take effect.
日志说明	由于硬件资源的限制，协议匹配条件不能生效
处理建议	建议合理利用协议，将不需要的协议去使能

27.2 DRVPLAT_ECMP_NO_RESOURCE

日志内容	current ECMP count [UINT32], max ECMP count [UINT32]
参数解释	$1：已经配置的ECMP组的数量 $2：硬件支持的最大ECMP组的数量
日志等级	4
举例	DRVPLAT/4/DRVPLAT_ECMP_NO_RESOURCE: current ECMP count 20, max ECMP count 20
日志说明	当前ECMP组的最大数超过硬件支持的ECMP组的最大数量，无法继续配置ECMP组
处理建议	减少ECMP组的数量，或修改最大等价路由条数（最大等价路由条数的值越小，支持的ECMP组的数量越大）

27.3 DRVPLAT_MAC_Confilict

日志内容	ERROR:The 40MSB OF INTFMAC SHOULD BE THE SAME WITH THE FIRST CONFIGURED MAC_ADDRESS!
参数解释	无
日志等级	4
举例	DRVPLAT/4/DRVPLAT_MAC_Confilict: ERROR:The 40MSB OF INTFMAC SHOULD BE THE SAME WITH THE FIRST CONFIGURED MAC_ADDRESS!
日志说明	当前VLAN接口下配置的MAC地址和首个VLAN接口下配置的MAC地址的高40位不同
处理建议	非第一次在VLAN接口下配置的MAC地址，需要与首次在VLAN接口下配置的MAC地址的高40位保持一致

27.4 DRVPLAT_NO_ENOUGH_RESOURCE

日志内容	WARNING: The resource of the evlanid is not enough !! [STRING]
参数解释	$1：端口名称
日志等级	4
举例	DRVPLAT/4/DRVPLAT_NO_ENOUGH_RESOURCE: WARNING: The resource of the evlanid is not enough!! GigabitEthernet1/0/1
日志说明	二层以太网接口切换为三层以太网接口时，需要的扩展VLAN ID硬件资源不足
处理建议	扩展VLAN ID硬件源不足的情况下，二层以太网接口不能作为组播转发的上行口或下行口

27.5 DRVPLAT_POE_AI_DISCONNET_AC

日志内容	POE,POE_AI_DISCONNET_AC, Changing from MPS detection to AC detection on PoE port [STRING]. Reason: The port has stopped power supply because of MPS current insufficiency.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_DISCONNET_AC: POE,POE_AI_DISCONNET_AC, Changing from MPS detection to AC detection on PoE port GigabitEthernet1/0/1. Reason: The port has stopped power supply because of MPS current insufficiency.
日志说明	以DC-MPS方式检测到端口电流不足，当前端口从DC-MPS检测更改为AC检测，并输出该日志信息
处理建议	无

日志内容	POE,POE_AI_DISCONNET_AC, The detection on PoE port [STRING] has already been AC, keeping the mode in effect.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_DISCONNET_AC: POE,POE_AI_DISCONNET_AC, The detection on PoE port GigabitEthernet1/0/1 has already been AC, keeping the mode in effect.
日志说明	当端口断电的处理模式为AC检测方式时，且DC-MPS未做相关配置，将输出该日志信息
处理建议	无

27.6 DRVPLAT_POE_AI_DISCONNET_DELAY

日志内容	POE,POE_AI_DISCONNET_DELAY, Delaying the MPS detection on PoE port [STRING]. Reason: The port has stopped power supply because of MPS current insufficiency.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_DISCONNET_DELAY: POE,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.
日志说明	以DC-MPS方式检测到端口电流不足，端口延时500ms再进行一次DC-MPS检测，并输出该日志信息
处理建议	无

27.7 DRVPLAT_POE_AI_HIGH_INRUSH

日志内容	POE,POE_AI_HIGH_INRUSH, Increasing the inrush current threshold for PoE port [STRING]. Reason: The port has stopped power supply because of a high inrush current.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_HIGH_INRUSH: POE,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.
日志说明	端口在没有开启high_inrush功能的情况下，配置了AI_POE功能。AI检测到供电后，会开启high_inrush功能，并打印告警信息提醒用户
处理建议	检测端口接入的负载设备所需功率是否不在阈值范围内

处理建议	检查PSE可分配功率数值，与Allocated power（已分配功率数值），并作相应调整
日志内容	POE,POE_AI_HIGH_INRUSH, The inrush current threshold for PoE port [STRING] has already been HIGH_INRUSH, Keeping it that way.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_HIGH_INRUSH: POE,POE_AI_HIGH_INRUSH, The inrush current threshold for PoE port GigabitEthernet1/0/1 has already been HIGH_INRUSH, Keeping it that way.
日志说明	当设备因冲击电流过大导致断电，触发high_inrush计数时，将输出该日志信息
处理建议	检测端口配置与负载设备是否符合供电标准

27.8 DRVPLAT_POE_AI_PORT_MAXPOWER

日志内容	POE,POE_AI_PORT_MAXPOWER, IcutAlarming of PoE port [STRING]. Reason: An instant power surge has caused overload self-protection of the port.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_PORT_MAXPOWER: POE,POE_AI_PORT_MAXPOWER, IcutAlarming of PoE port GigabitEthernet1/0/1. Reason: An instant power surge has caused overload self-protection of the port.
日志说明	当设备因瞬时功率过大断电，触发过流过载告警，将输出该日志
处理建议	重新调整端口最大可输出功率，以匹配对应的负载设备

日志内容	POE,POE_AI_PORT_MAXPOWER, Increasing the maximum power of PoE port [STRING] to [UINT]. Reason: An instant power surge has caused overload self-protection of the port.
参数解释	$1：端口名称 $2：端口最大功率
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_PORT_MAXPOWER: POE,POE_AI_PORT_MAXPOWER, Increasing the maximum power of PoE port GigabitEthernet1/0/1 to 30000. Reason: An instant power surge has caused overload self-protection of the port.
日志说明	当设备因瞬时功率超过端口阈值，端口触发过载计数，并输出该日志信息
处理建议	重新调整端口最大可输出功率，以匹配对应的负载设备

日志内容	POE,POE_AI_PORT_MAXPOWER, The maximum power of PoE port [STRING] has already been [UINT]
参数解释	$1：端口名称 $2：端口最大功率
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_PORT_MAXPOWER: POE,POE_AI_PORT_MAXPOWER, The maximum power of PoE port GigabitEthernet1/0/1 has already been 30000.
日志说明	当设备因瞬时功率过大断电，端口触发过载计数时，并输出该日志信息
处理建议	无

27.9 DRVPLAT_POE_AI_PORT_RESTART

日志内容	POE,POE_AI_PORT_RESTART, Re-enabling PoE on port [STRING]. Reason: The power consumption of the port is 0.
参数解释	$1：端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_AI_PORT_RESTART: POE,POE_AI_PORT_RESTART, Re-enabling PoE on port GigabitEthernet1/0/1. Reason: The power consumption of the port is 0.
日志说明	开启AI POE 功能后，检测到端口输出功率为0，则置端口状态为初始值，并输出该打印信息
处理建议	检查端口与负载硬件连接

27.10 DRVPLAT_PORT

本节介绍的日志信息仅 S5130S-52S-HI-EDF 电子网络集线器支持。

日志内容	DRVMSG, PORT, Cannot operate trunk group because there are ports had already switched to trunk port.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Cannot operate trunk group because there are ports had already switched to trunk port.
日志说明	端口上配置了聚合口为备份口，删除聚合组时打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, Support only backup port.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Support only backup port.
日志说明	S5130S-52S-HI-EDF设备上仅编号为25～28的Backup接口可以加入聚合组。如果其余端口加入聚合组，则打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, Front and back interfaces restored to normal.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Front and back interfaces restored to normal.
日志说明	前后端口为正常状态后，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, Linkage down FAILED.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Linkage down FAILED.
日志说明	端口从Backup状态切换到Normal状态失败时，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, This port cannot be operated.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, This port cannot be operated.
日志说明	备份口一般连接备用交换机，当被设置为备份口的端口不是连接交换机的端口时，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, A new backup port cannot be set because an existing port has been switched to backup mode.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, A new backup port cannot be set because an existing port has been switched to backup mode.
日志说明	若当前接口已经为backup接口，再次配置时，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, This interface is not supported. Support backup interface.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, This interface is not supported. Support backup interface.
日志说明	S5130S-52S-HI-EDF设备上仅编号为25～28的接口或其组成的聚合组可以为backup口。若其它端口被设置为备份口，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, Backup port not initialized. Port status change to block.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Backup port not initialized. Port status change to block.
日志说明	流量切换到未初始化的备份口上时，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, Not support this interface. Support 1/0/1 to 1/0/24.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Not support this interface. Support 1/0/1 to 1/0/24.
日志说明	S5130S-52S-HI-EDF设备仅前面板上编号1～24的Bypass Front接口支持流量切换。如果想要切换状态的端口不是接交换机的24个端口，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, Port status is down. Need up.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, Port status is down. Need up.
日志说明	如果想要切换状态的端口状态为down，打印此日志信息
处理建议	无

日志内容	DRVMSG, PORT, The port is not in backup mode. No need to set to normal.
参数解释	无
日志等级	5
举例	DRVPLAT/5/PORT: DRVMSG, PORT, The port is not in backup mode. No need to set to normal.
日志说明	如果想要切换状态的端口不是backup状态，而是Normal状态，则打印此日志信息
处理建议	无

27.11 DRVPLAT_PORT_ATTACK_OCCUR

日志内容	Auto port-defend started.(SourceAttackInterface=[STRING], AttackProtocol=[STRING])
参数解释	$1：触发防攻击的端口 $2：防攻击的协议类型 • IPV6_ND_PASS：表示邻居请求报文 NS、路由请求报文 RS 或路由通告报文 RA • IPV6_ND_DEST：表示邻居通告报文 NA 或重定向报文 • ARP：表示 ARP 请求报文 • ARP_REPLY：表示 ARP 应答报文
日志等级	4
举例	DRVPLAT/4/DRVPLAT_PORT_ATTACK_OCCUR: Auto port-defend started. (SourceAttackInterface=GigabitEthernet3/0/19, AttackProtocol= IPV6_ND_PASS)
日志说明	ND或ARP报文收包速率大于设置的防攻击阈值，触发防攻击功能
处理建议	可通过减少ND或ARP报文上送速率，消除攻击

日志内容	Auto port-defend stopped.(SourceAttackInterface=[STRING], AttackProtocol=[STRING])
参数解释	$1：防攻击消除的端口 $2：防攻击消除的协议类型 • IPV6_ND_PASS：表示邻居请求报文 NS、路由请求报文 RS 或路由通告报文 RA • IPV6_ND_DEST：表示邻居通告报文 NA 或重定向报文 • ARP：表示 ARP 请求报文 • ARP_REPLY：表示 ARP 应答报文
日志等级	4
举例	DRVPLAT/4/DRVPLAT_PORT_ATTACK_OCCUR: Auto port-defend stopped.(SourceAttackInterface=GigabitEthernet3/0/19, AttackProtocol= IPV6_ND_PASS)
日志说明	ND或ARP报文收包速率小于报文设置的防攻击阈值，防攻击功能关闭
处理建议	无

27.12 DRVPLAT_PORT_FORCE_POWER_OFF

日志内容	POE, PORT_FORCE_POWER_OFF, Disabled forced PoE on port [string] automatically. Reason: The power consumed by [string] had exceeded the max allowed limit.
参数解释	$1:端口名称 $2:端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_PORT_FORCE_POWER_OFF: POE, PORT_FORCE_POWER_OFF, Disabled forced PoE on port [string] automatically. Reason: The power consumed by [string] had exceeded the max allowed limit.
日志说明	端口消耗功率超过可允许输出的上限，自动关闭force power模式，并打印本日志信息
处理建议	无

27.13 DRVPLAT_POE_FORCE_POWER_ON

日志内容	POE, POE_FORCE_POWER_ON, Re-enabled forced PoE on port [string]. Reason: The allocable power on the PSE had become sufficient.
参数解释	$1:端口名称
日志等级	6
举例	DRVPLAT/6/DRVPLAT_POE_FORCE_POWER_ON: POE, POE_FORCE_POWER_ON, Re-enabled forced PoE on port GigabitEthernet1/0/1. Reason: The allocable power on the PSE had become sufficient.
日志说明	PSE可分配功率满足force power的限制，重新配置端口force power模式，并打印本日志信息
处理建议	无

27.14 DRVPLAT_SOFTCAR_DROP

日志内容	PktType=[STRING], SrcMAC=[STRING], Dropped from interface=[STRING] at Stage=[STRING], StageCnt=[STRING], TotalCnt=[STRING], MaxRateInterface=[STRING]. PktType=[STRING], SrcMAC=[STRING], Dropped at Stage=[UINT],StageCnt=[UINT], TotalCnt=[UINT].
参数解释	$1：被丢弃报文的类型 $2：被丢弃报文的源MAC地址 $3：被丢弃报文的接收端口 $4：报文丢弃的阶段，取值为0或非0（仅打印周期10分钟时有效） o 0：表示统计周期为 10 分钟 o 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 $5：被丢弃报文的阶段计数 $6：被丢弃报文的总数 $7：丢弃报文时最大速率的端口
日志等级	4
举例	DRVPLAT/4/SOFTCAR_DROP: PktType=ARP, SrcMAC=0000-0000-0001, Dropped from interface=GigabitEthernet1/0/1 at Stage=0, StageCnt=1200, TotalCnt=1200, MaxRateInterface=GigabitEthernet1/0/1.
日志说明	上送CPU的报文超过设定的阈值后，报文将被随机丢弃，并输出限速丢弃日志。 若接口返回错误，则输出不带接口信息的日志。
处理建议	查看丢弃报文时的最大速率端口，确认超速原因并处理。

28 EDEV

本节介绍扩展设备管理模块输出的日志信息。

28.1 ALARM_IN_REMOVED

日志内容	Alarm removed on the alarm-in port [UNIT].
参数解释	$1：表示告警输入端口的编号
日志等级	5
举例	EDEV/5/ALARM_IN_REMOVED: Alarm removed on the alarm-in port 1.
日志说明	某个告警输入接口的告警信号已解除，恢复到正常状态
处理建议	无

28.2 ALARM_IN_REPORTED

日志内容	Alarm reported on the alarm-in port [UNIT].
参数解释	$1：表示告警输入端口的编号
日志等级	5
举例	EDEV/5/EDEV_ALARM_IN_REPORTED: Alarm reported on the alarm-in port 1.
日志说明	某个告警输入接口收到告警信号
处理建议	检查和告警输入接口相连的设备，确认该邻居设备是否发生异常

28.3 EDEV_BOOTROM_UPDATE_FAILED

日志内容	Failed to execute the bootrom update command.
参数解释	无
日志等级	5
举例	EDEV/5/EDEV_BOOTROM_UPDATE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the bootrom update command.
日志说明	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
处理建议	请根据提示信息采取相应措施

28.4 EDEV_BOOTROM_UPDATE_SUCCESS

日志内容	Executed the bootrom update command successfully.
参数解释	无
日志等级	5
举例	EDEV/5/EDEV_BOOTROM_UPDATE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the bootrom update command successfully.
日志说明	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
处理建议	无

28.5 EDEV_FAILOVER_GROUP_STATE_CHANGE

日志内容	Status of stateful failover group [STRING] with ID [UINT32] changed to [STRING].
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
举例	EDEV/5/EDEV_FAILOVER_GROUP_STATE_CHANGE: -MDC=1; Status of stateful failover group 123 with ID 0 changed to primary.
日志说明	备份组的状态发生了变化
处理建议	无

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].
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
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.
日志说明	监控到终端上线
处理建议	无

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].
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
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.
日志说明	监控到终端下线
处理建议	无

29.3 EPA_DEVICETYPE_CHANGE

日志内容	Cleared EPA monitor rule configurations. Reason: Device type changed from [STRING] to [STRING].
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
举例	EPA/6/EPA_DEVICETYPE_CHANGE: Cleared EPA monitor rule configurations. Reason: Device type changed from TC to Self-managed.
日志说明	因为设备类型切换，EPA监控规则被完全清除
处理建议	无

30 ERPS

本节介绍 ERPS 模块输出的日志信息。

30.1 ERPS_STATE_CHANGED

日志内容	Ethernet ring [UINT16] instance [UINT16] changed state to [STRING].
参数解释	$1：ERPS环号 $2：ERPS环实例编号 $3：ERPS实例状态
日志等级	6
举例	ERPS/4/ERPS_STATE_CHANGED: Ethernet ring 1 instance 1 changed state to Idle.
日志说明	ERPS环上实例状态发生改变
处理建议	无

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].
参数解释	$1：MAC地址 $2：接口名称
日志等级	5
举例	ETH/5/ETH_SET_MAC_FAILED: Failed to set the MAC address 0001-0001-0001 on GigabitEthernet1/0/1.
日志说明	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 ETHOAM

本节介绍 ETHOAM 模块输出的日志信息。

32.1 ETHOAM_CONNECTION_FAIL_DOWN

日志内容	The link is down on interface [string] because a remote failure occurred on peer interface.
参数解释	$1：接口名称
日志等级	5
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.
日志说明	对端接口发生故障，链路down
处理建议	检查链路状态或对端的OAM状态

32.2 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.
参数解释	$1：接口名称
日志等级	5
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.
日志说明	接口在超时时间内没有收到信息OAMPDU，所以删除OAM连接
处理建议	检查链路状态或对端的OAM状态

32.3 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.
参数解释	$1：接口名称
日志等级	3
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.
日志说明	对端与本端接口的OAM协议状态不匹配，建立OAM连接失败
处理建议	分析两端发出的OAM报文中的协议状态字段

32.4 ETHOAM_CONNECTION_SUCCEED

日志内容	An OAM connection is established on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_CONNECTION_SUCCEED: An OAM connection is established on interface Ethernet1/0/1.
日志说明	OAM连接建立成功
处理建议	无

32.5 ETHOAM_DISABLE

日志内容	Ethernet OAM is now disabled on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_DISABLE: Ethernet OAM is now disabled on interface Ethernet1/0/1.
日志说明	以太网OAM功能已关闭
处理建议	无

32.6 ETHOAM_DISCOVERY_EXIT

日志内容	OAM interface [string] quit the OAM connection..
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_DISCOVERY_EXIT: OAM interface Ethernet1/0/1 quit the OAM connection.
日志说明	本端接口退出OAM连接
处理建议	无

32.7 ETHOAM_ENABLE

日志内容	Ethernet OAM is now enabled on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_ENABLE: Ethernet OAM is now enabled on interface Ethernet1/0/1.
日志说明	以太网OAM功能已使能
处理建议	无

32.8 ETHOAM_ENTER_LOOPBACK_CTRLLED

日志内容	The local OAM entity enters remote loopback as controlled DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLED: The local OAM entity enters remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
日志说明	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
处理建议	无

32.9 ETHOAM_ENTER_LOOPBACK_CTRLLING

日志内容	The local OAM entity enters remote loopback as controlling DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLING: The local OAM entity enters remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
日志说明	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
处理建议	无

32.10 ETHOAM_LOCAL_DYING_GASP

日志内容	A local Dying Gasp event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_DYING_GASP: A local Dying Gasp event occurred on interface Ethernet1/0/1.
日志说明	重启设备或关闭接口导致本端产生致命故障（Dying Gasp）事件
处理建议	链路恢复之前不能使用

32.11 ETHOAM_LOCAL_ERROR_FRAME

日志内容	An errored frame event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME: An errored frame event occurred on local interface Ethernet1/0/1.
日志说明	本地接口产生错误帧事件
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

32.12 ETHOAM_LOCAL_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_PERIOD: An errored frame period event occurred on local interface Ethernet1/0/1.
日志说明	本地接口产生错误帧周期事件
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

32.13 ETHOAM_LOCAL_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_SECOND: An errored frame seconds event occurred on local port Ethernet1/0/1.
日志说明	本地接口产生错误帧秒事件
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

32.14 ETHOAM_LOCAL_ERROR_SYMBOL

日志内容	An errored symbol event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_ERROR_SYMBOL: An errored symbol event occurred on local interface Ethernet1/0/1.
日志说明	本端产生错误信号事件
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

32.15 ETHOAM_LOCAL_LINK_FAULT

日志内容	A local Link Fault event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_LINK_FAULT: A local Link Fault event occurred on interface Ethernet1/0/1.
日志说明	本地链路down，产生链路故障事件
处理建议	重新连接本地接口的光纤接收端

32.16 ETHOAM_LOOPBACK_EXIT

日志内容	OAM interface [string] quit remote loopback.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_EXIT: OAM interface Ethernet1/0/1 quit remote loopback.
日志说明	远端环回连接建立未完成时，接口关闭远端环回或OAM连接断开后，OAM接口退出远端环回
处理建议	无

32.17 ETHOAM_LOOPBACK_EXIT_ERROR_STATU

日志内容	OAM interface [string] quit remote loopback due to incorrect multiplexer or parser status.
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOOPBACK_EXIT_ERROR_STATU: OAM interface Ethernet1/0/1 quit remote loopback due to incorrect multiplexer or parser status.
日志说明	复用器或解析器状态错误，OAM接口Ethernet1/0/1退出远端环回
处理建议	在OAM实体上关闭并重新使能以太网OAM

32.18 ETHOAM_LOOPBACK_NO_RESOURCE

日志内容	OAM interface [string] can’t enter remote loopback due to insufficient resources.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_NO_RESOURCE: OAM interface Ethernet1/0/1 can’t enter remote loopback due to insufficient resources.
日志说明	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

32.19 ETHOAM_LOOPBACK_NOT_SUPPORT

日志内容	OAM interface [string] can’t enter remote loopback because the operation is not supported.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_NOT_SUPPORT: OAM interface Ethernet1/0/1 can’t enter remote loopback because the operation is not supported.
日志说明	由于设备不支持，OAM接口无法进入远端环回
处理建议	无

32.20 ETHOAM_NO_ENOUGH_RESOURCE

日志内容	The configuration failed on OAM interface [string] because of insufficient resources.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ ETHOAM_NO_ENOUGH_RESOURCE: The configuration failed on OAM interface Ethernet1/0/1 because of insufficient resources.
日志说明	系统内存资源不足导致OAM接口上的配置失败
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

32.21 ETHOAM_NOT_CONNECTION_TIMEOUT

日志内容	Interface [string] quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
参数解释	$1：接口名称
日志等级	5
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.
日志说明	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
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

32.22 ETHOAM_QUIT_LOOPBACK_CTRLLED

日志内容	The local OAM entity quit remote loopback as controlled DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_QUIT_LOOPBACK_CTRLLED: The local OAM entity quit remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
日志说明	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
处理建议	无

32.23 ETHOAM_QUIT_LOOPBACK_CTRLLING

日志内容	The local OAM entity quit remote loopback as controlling DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_QUIT_LOOPBACK_CONTROLLING: The local OAM entity quit remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
日志说明	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
处理建议	无

32.24 ETHOAM_REMOTE_CRITICAL

日志内容	A remote Critical event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_CRITICAL: A remote Critical event occurred on interface Ethernet1/0/1.
日志说明	发生远端紧急事件
处理建议	链路恢复之前不能使用

32.25 ETHOAM_REMOTE_DYING_GASP

日志内容	A remote Dying Gasp event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_DYING_GASP: A remote Dying Gasp event occurred on interface Ethernet1/0/1.
日志说明	重启远端设备或关闭接口导致远端产生致命故障（Dying Gasp）事件
处理建议	链路恢复之前不能使用

32.26 ETHOAM_REMOTE_ERROR_FRAME

日志内容	An errored frame event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME: An errored frame event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误帧事件
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

32.27 ETHOAM_REMOTE_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_PERIOD: An errored frame period event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误帧周期事件
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

32.28 ETHOAM_REMOTE_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_SECOND: An errored frame seconds event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误帧秒事件
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

32.29 ETHOAM_REMOTE_ERROR_SYMBOL

日志内容	An errored symbol event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_SYMBOL: An errored symbol event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误信号事件
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

32.30 ETHOAM_REMOTE_EXIT

日志内容	OAM interface [string] quit OAM connection because Ethernet OAM is disabled on the peer interface.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_REMOTE_EXIT: OAM interface Ethernet1/0/1 quit OAM connection because Ethernet OAM is disabled on the peer interface.
日志说明	对端接口关闭以太网OAM功能导致本端接口退出OAM连接
处理建议	无

32.31 ETHOAM_REMOTE_FAILURE_RECOVER

日志内容	Peer interface [string] recovered.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_REMOTE_FAILURE_RECOVER: Peer interface Ethernet1/0/1 recovered.
日志说明	对端接口链路故障清除，OAM连接恢复
处理建议	无

32.32 ETHOAM_REMOTE_LINK_FAULT

日志内容	A remote Link Fault event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_LINK_FAULT: A remote Link Fault event occurred on interface Ethernet1/0/1.
日志说明	远端链路down，产生远端链路故障事件
处理建议	重新连接远端接口的光纤接收端

33 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。

33.1 EVB_AGG_FAILED

日志内容	Remove port [STRING] from aggregation group [STRING]. Otherwise, the EVB feature does not take effect.
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	6
举例	EVB/6/EVB_AGG_FAILED: Remove port GigabitEthernet5/0/5 from aggregation group Bridge-Aggregation5. Otherwise, the EVB feature does not take effect.
日志说明	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

33.2 EVB_LICENSE_EXPIRE

日志内容	The EVB feature's license will expire in [UINT32] days.
参数解释	$1：天数
日志等级	6
举例	EVB/6/EVB_LICENSE_EXPIRE: The EVB feature's license will expire in 15 days.
日志说明	EVB的License将在指定天数后失效
处理建议	更新EVB的License

33.3 EVB_VSI_OFFLINE

日志内容	VSI [STRING] went offline.
参数解释	$1：VSI接口/VSI聚合接口名称
日志等级	6
举例	EVB/6/EVB_VSI_OFFLINE: VSI Schannel-Aggregation1:2.0 went offline.
日志说明	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

33.4 EVB_VSI_ONLINE

日志内容	VSI [STRING] came online, status is [STRING].
参数解释	$1：VSI接口/VSI聚合接口名称 $2：VSI状态
日志等级	6
举例	EVB/6/EVB_VSI_ONLINE: VSI Schannel-Aggregation1:2.0 came online, status is association.
日志说明	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

34 EVIISIS

本节介绍 EVI IS-IS 模块输出的日志信息。

34.1 EVIISIS_LICENSE_EXPIRED

日志内容	The EVIISIS feature is being disabled, because its license has expired.
参数解释	无
日志等级	3
举例	EVIISIS/3/EVIISIS_LICENSE_EXPIRED: The EVIISIS feature is being disabled, because its license has expired.
日志说明	EVIISIS的License已经过期
处理建议	请更换有效的Licence

34.2 EVIISIS_LICENSE_EXPIRED_TIME

日志内容	The EVIISIS feature will be disabled in [ULONG] days.
参数解释	$1：功能还可使用的天数
日志等级	5
举例	EVIISIS/5/EVIISIS_LICENSE_EXPIRED_TIME: The EVIISIS feature will be disabled in 2 days.
日志说明	EVIISIS的License不可用，EVIISIS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 EVI License，会启动 30 天临时可用定时器
处理建议	若要继续使用EVIISIS功能，请准备新的License

34.3 EVIISIS_LICENSE_UNAVAILABLE

日志内容	The EVIISIS feature has no available license.
参数解释	无
日志等级	3
举例	EVIISIS/3/EVIISIS_LICENSE_UNAVAILABLE: The EVIISIS feature has no available license.
日志说明	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

34.4 EVIISIS_NBR_CHG

日志内容	EVIISIS [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
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
举例	EVIISIS/5/EVIISIS_NBR_CHG: EVIISIS 1, Level-1 adjacency 0011.2200.1501 (Evi-Link0), state changed to down.
日志说明	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

35 FCLINK

本节介绍 FCLINK 模块输出的日志信息。

35.1 FCLINK_FDISC_REJECT_NORESOURCE

日志内容	VSAN [UINT16], Interface [STRING]: An FDISC was rejected because the hardware resource is not enough.
参数解释	$1：VSAN ID $2：接口名称
日志等级	4
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.
日志说明	硬件资源不足时收到了FDISC报文
处理建议	减少节点的数量

35.2 FCLINK_FLOGI_REJECT_NORESOURCE

日志内容	VSAN [UINT16], Interface [STRING]: An FLOGI was rejected because the hardware resource is not enough.
参数解释	$1：VSAN ID $2：接口名称
日志等级	4
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.
日志说明	硬件资源不足时收到了FLOGI报文
处理建议	减少节点的数量

36 FCOE

本节介绍 FCOE 模块输出的日志信息。

36.1 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.
参数解释	$1：聚合接口名称
日志等级	4
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.
日志说明	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
处理建议	无

36.2 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.
参数解释	$1：聚合接口名称
日志等级	4
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.
日志说明	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
处理建议	无

36.3 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.
参数解释	$1：聚合接口名称 $2：以太网接口名称
日志等级	4
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.
日志说明	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 FCZONE

本节介绍 FCZONE 模块输出的日志信息。

37.1 FCZONE_DISTRIBUTE_FAILED

日志内容	-VSAN=[UINT16]; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
参数解释	$1：VSAN ID
日志等级	4
举例	FCZONE/4/FCZONE_DISTRIBUTE_FAILED: -VSAN=2; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
日志说明	扩散失败，Fabric中交换机的zone配置可能因此不一致
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

37.2 FCZONE_HARDZONE_DISABLED

日志内容	-VSAN=[UINT16]; No enough hardware resource for zone rule, switched to soft zoning.
参数解释	$1：VSAN ID
日志等级	4
举例	FCZONE/4/FCZONE_HARDZONE_DISABLED: -VSAN=2; No enough hardware resource for zone rule, switched to soft zoning.
日志说明	硬件资源不足
处理建议	激活一个更小的zone set

37.3 FCZONE_HARDZONE_ENABLED

日志内容	-VSAN=[UINT16]; Hardware resource for zone rule is restored, switched to hard zoning.
参数解释	$1：VSAN ID
日志等级	6
举例	FCZONE/6/FCZONE_HARDZONE_ENABLED: -VSAN=2; Hardware resource for zone rule is restored, switched to hard zoning.
日志说明	硬件资源恢复时，切换到hard zoning
处理建议	无需处理

37.4 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.
参数解释	$1：VSAN ID
日志等级	4
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.
日志说明	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
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

37.5 FCZONE_ISOLATE_CLEAR_ALLVSAN

日志内容	-Interface=[STRING]; Isolation status was cleared in all supported VSANs.
参数解释	$1：接口名称
日志等级	6
举例	FCZONE/6/FCZONE_ISOLATE_CLEAR_ALLVSAN: -Interface=Fc1/0/1; Isolation status was cleared in all supported VSANs.
日志说明	接口在所有支持的VSAN内去隔离
处理建议	无需处理

37.6 FCZONE_ISOLATE_CLEAR_VSAN

日志内容	-Interface=[STRING]-VSAN=[UINT16]; Isolation status was cleared.
参数解释	$1：接口名称 $2：VSAN ID
日志等级	6
举例	FCZONE/6/FCZONE_ISOLATE_CLEAR_VSAN: -Interface=Fc1/0/1-VSAN=2; Isolation status was cleared.
日志说明	接口在指定VSAN内去隔离
处理建议	无需处理

37.7 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].
参数解释	$1：VSAN ID $2：交换机WWN
日志等级	4
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.
日志说明	因与邻居交换机合并失败，隔离与该邻居相连的所有E-Port
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

38 FIB

本节包含 FIB 日志消息。

38.1 FIB_FILE

日志内容	Failed to save the IP forwarding table due to lack of storage resources.
参数解释	无
日志等级	4
举例	FIB/4/FIB_FILE: -MDC=1; Failed to save the IP forwarding table due to lack of storage resources.
日志说明	存储介质剩余空间不足，保存IP FIB信息失败
处理建议	删除其它无用文件，释放存储介质的存储空间

39 FILTER

本节介绍 FILTER 模块输出的日志信息。

39.1 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];
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
举例	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1067)=inbound;AclType(1064)=ACL;Acl(1065)=3000;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1059)=Echo(8);IcmpCode(1060)=0;MatchAclCount(1066)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送ICMP报文过滤日志，之后定时发送该日志
处理建议	无

39.2 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];
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
举例	FILTER/6/FILTER_EXECUTION_ICMPV6: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1067)=inbound;AclType(1064)=ACL;Acl(1065)=3000;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;Icmpv6Type(1064)=Echo(128);Icmpv6Code(1065)=0;MatchAclCount(1066)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送ICMPV6报文过滤日志，之后定时发送该日志
处理建议	无

39.3 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];
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
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;
日志说明	首次命中包过滤时发送报文过滤日志，之后定时发送该日志
处理建议	无

39.4 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];
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
举例	FILTER/6/FILTER_IPV6_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;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;
日志说明	首次命中包过滤时发送报文过滤日志，之后定时发送该日志
处理建议	无

40 FIPSNG

本节介绍 FIP Snooping 模块输出的日志信息。

40.1 FIPSNG_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for FIP snooping rule.
参数解释	N/A
日志等级	4
举例	FIPSNG/4/FIPSNG_HARD_RESOURCE_NOENOUGH: No enough hardware resource for FIP snooping rule.
日志说明	硬件资源不足
处理建议	无

40.2 FIPSNG_HARD_RESOURCE_RESTORE

日志内容	Hardware resource for FIP snooping rule is restored.
参数解释	N/A
日志等级	6
举例	FIPSNG/6/FIPSNG_HARD_RESOURCE_RESTORE: Hardware resource for FIP snooping is restored.
日志说明	硬件资源恢复
处理建议	无

41 FS

本节介绍 FS（File System）模块输出的日志信息。

41.1 FS_UNFORMATTED_PARTITION

日志内容	Partition [%s] is not formatted yet. Please format the partition first.
参数解释	$1：分区名
日志等级	4
举例	FS/4/FS_UNFORMATED_PARTITION: Partition usba0: is not formatted yet. Please format the partition first.
日志说明	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

42 FTP

本节介绍 FTP（File Transfer Protocol）模块输出的日志信息。

42.1 FTP_ACL_DENY

日志内容	The FTP Connection [IPADDR]([STRING]) request was denied according to ACL rules.
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
举例	FTP/5/FTP_ACL_DENY: The FTP Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	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	无

42.2 FTPD_AUTHOR_FAILED

日志内容	Authorization failed for user [STRING]@[STRING].
参数解释	$1：用户名 $2：用户IP地址
日志等级	4
举例	FTP/4/FTPD_AUTHOR_FAILED: Authorization failed for user admin@10.11.115.63.
日志说明	FTP用户授权失败
处理建议	请检查是否配置该用户支持FTP服务

42.3 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]).
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
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).
日志说明	FTP登录用户达到上限。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

43 gRPC

本节介绍 gRPC 模块输出的日志信息。

43.1 GRPC_LOGIN

日志内容	[STRING] logged in from [STRING], session id [INT32].
参数解释	$1：用户名 $2：客户端地址 $3：会话ID
日志等级	6
举例	GRPC/6/GRPC_LOGIN: user logged in from 127.0.0.1, session id 1.
日志说明	用户登录成功
处理建议	无

43.2 GRPC_LOGIN_FAILED

日志内容	[STRING] from [STRING] login failed. 或 [STRING] from [STRING] login failed. [STRING]
参数解释	$1：用户名 $2：客户端地址 $3：失败原因，取值为Number of the gRPC sessions reached the limit.
日志等级	4
举例	GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. Number of the gRPC sessions reached the limit.
日志说明	用户登录失败
处理建议	**77.** 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 **78.** 如果显示 gRPC 会话到达数量上限，请减少 gRPC 客户端连接数

43.3 GRPC_LOGOUT

日志内容	[STRING] logged out, session id [INT32].
参数解释	$1：用户名 $2：会话ID
日志等级	6
举例	GRPC/6/GRPC_LOGOUT: user logged out, session id 1.
日志说明	用户正常登出
处理建议	无

43.4 GRPC_SERVER_FAILED

日志内容	Failed to enable gRPC server.
参数解释	无
日志等级	4
举例	GRPC/4/GRPC_SERVER_FAILED: Failed to enable gRPC server.
日志说明	因端口冲突，无法和gRPC服务器建立连接
处理建议	检查是否端口号被占用

43.5 GRPC_SUBSCRIBE_EVENT_FAILED

日志内容	Failed to subscribe event [STRING].
参数解释	$1：事件名
日志等级	4
举例	GRPC/4/GRPC_SUBSCRIBE_EVENT_FAILED: Failed to subscribe event syslog.
日志说明	订阅事件失败
处理建议	无

43.6 GRPC_RECEIVE_SUBSCRIPTION

日志内容	Received a subscription of module [STRING].
参数解释	$1：模块名
日志等级	6
举例	GRPC/6/GRPC_RECEIVE_SUBSCRIPTION: Received a subscription of module syslog.
日志说明	收到某个模块的一个订阅事件
处理建议	无

44 HA

本节介绍 HA 模块输出的日志信息。

44.1 HA_BATCHBACKUP_FINISHED

日志内容	Batch backup of standby board in [STRING] has finished.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 has finished.
日志说明	主用主控板和备用主控板之间的批量备份完成
处理建议	无

44.2 HA_BATCHBACKUP_STARTED

日志内容	Batch backup of standby board in [STRING] started.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 started.
日志说明	主用主控板和备用主控板之间的批量备份开始
处理建议	无

44.3 HA_STANDBY_NOT_READY

日志内容	Standby board in [STRING] is not ready, reboot ...
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	4
举例	HA/4/HA_STANDBY_NOT_READY: Standby board in slot 1 is not ready, reboot ...
日志说明	主备倒换时，如果备用主控板未准备好，则不会进行主备倒换，而是重启备用主控板和主用主控板，并在备用主控板上打印该信息
处理建议	建议备用主控板批量备份完成前不要进行主备倒换

44.4 HA_STANDBY_TO_MASTER

日志内容	Standby board in [STRING] changed to the master.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	HA/5/HA_STANDBY_TO_MASTER: Standby board in slot 1 changed to the master.
日志说明	发生主备倒换，备用主控板成为主用主控板
处理建议	无

45 HQOS

本节介绍 HQOS（Hierarchical QoS）模块输出的日志信息。

45.1 HQOS_DP_SET_FAIL

日志内容	Failed to set drop profile [STRING] globally.
参数解释	$1：丢弃策略的名称
日志等级	4
举例	HQOS/4/HQOS_DP_SET_FAIL: Failed to set drop profile b globally.
日志说明	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	请检查丢弃策略配置，确保支持并且策略不冲突

45.2 HQOS_FP_SET_FAIL

日志内容	Failed to set [STRING] in forwarding profile [STRING] globally.
参数解释	$1：策略类型，可以为“gts”，“bandwidth”，“queue”或者“drop profile” $2：转发策略的名称
日志等级	4
举例	HQOS/4/HQOS_FP_SET_FAIL: Failed to set gts in forwarding profile b globally.
日志说明	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	请检查转发策略，确保支持并且策略不冲突

45.3 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].
参数解释	$1：调度策略的名称 $2：策略方式，可以为“inbound”或者““outbound” $3：接口名称
日志等级	4
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.
日志说明	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

45.4 HQOS_POLICY_RECOVER_FAIL

日志内容	Failed to recover scheduler policy [STRING] to the [STRING] direction of interface [STRING] due to [STRING].
参数解释	$1：调度策略的名称 $2：策略方式，可以为“inbound”或者“outbound” $3：接口名称 $4：失败原因
日志等级	4
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.
日志说明	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

46 HTTPD

本节介绍 HTTPD（HTTP daemon）模块输出的日志信息。

46.1 HTTPD_CONNECT

日志内容	[STRING] client [STRING] connected to the server successfully.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_CONNECT: HTTP client 192.168.30.117 connected to the server successfully.
日志说明	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	无

46.2 HTTPD_CONNECT_TIMEOUT

日志内容	[STRING] client [STRING] connection idle timeout.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_CONNECT_TIMEOUT: HTTP client 192.168.30.117 connection to server idle timeout.
日志说明	HTTP/HTTPS连接因空闲时间太长而断开
处理建议	无

46.3 HTTPD_DISCONNECT

日志内容	[STRING] client [STRING] disconnected from the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_DISCONNECT: HTTP client 192.168.30.117 disconnected from the server.
日志说明	HTTP/HTTPS 客户端断开了到服务器的连接
处理建议	无

46.4 HTTPD_FAIL_FOR_ACL

日志内容	[STRING] client [STRING] failed the ACL check and could not connect to the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_FAIL_FOR_ACL: HTTP client 192.168.30.117 failed the ACL check and cannot connect to the server.
日志说明	HTTP/HTTPS客户端没有通过ACL检查，无法建立连接
处理建议	无

46.5 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.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_FAIL_FOR_ACP: HTTP client 192.168.30.117 was denied by the certificate attribute access control policy and could not connect to the server.
日志说明	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	无

46.6 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.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
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.
日志说明	已达到最大连接数，无法建立新的连接
处理建议	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

47 IFNET

本节介绍接口管理模块输出的日志信息。

47.1 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].
参数解释	$1：聚合接口名称 $2：成员端口名称
日志等级	3
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.
日志说明	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

47.2 IF_BUFFER_CONGESTION_CLEAR

日志内容	[STRING] congestion on queue [UINT32] of [STRIING] is cleared. [UINT64] packets are discarded.
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
举例	IFNET/5/IF_BUFFER_CONGESTION_CLEAR: Ingress congestion on queue 1 of GigabitEthernet1/0/1 is cleared. 1000 packets are discarded.
日志说明	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

47.3 IF_BUFFER_CONGESTION_OCCURRENCE

日志内容	[STRING] congestion occurs on queue [INTEGER] of [STRING].
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
举例	IFNET/4/IF_BUFFER_CONGESTION_OCCURRENCE: Ingress congestion occurs on queue 1 of GigabitEthernet1/0/1.
日志说明	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

47.4 IF_LINKFLAP_DETECTED

日志内容	Link flapping was detected on [STRING].
参数解释	$1：接口名称
日志等级	3
举例	IFNET/3/IF_LINKFLAP_DETECTED: Link flapping was detected on GigabitEthernet1/0/1.
日志说明	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	**79.** 检查接口（本端或对端）连线是否被频繁插拔 **80.** 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

47.5 IF_MAPPINGIF_STATUS

日志内容	The mapping-interface status of [STRING] changed to [STRING].
参数解释	$1：映射接口名 $2：映射接口状态，取值包括： • backup：使用备用接口转发状态 • block：处于阻塞状态 • normal：处于正常状态 • linkagedown：映射接口对应的后面板接口 down，联动映射接口 down
日志等级	6
举例	IFNET/6/IF_MAPPINGIF_STATUS: The mapping-interface status of GE1/0/1 changed to backup.
日志说明	映射接口状态发生变化

处理建议	无

47.6 INTERFACE_NOTSUPPRESSED

日志内容	Interface [STRING] is not suppressed.
参数解释	$1：接口名称
日志等级	6
举例	IFNET/6/INTERFACE_NOTSUPPRESSED: Interface Ethernet0/0/0 is not suppressed.
日志说明	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

47.7 INTERFACE_SUPPRESSED

日志内容	Interface [STRING] was suppressed.
参数解释	$1：接口名称
日志等级	5
举例	IFNET/5/INTERFACE_SUPPRESSED: Interface Ethernet0/0/0 was suppressed.
日志说明	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	**81.** 检查接口（本端或对端）连线是否被频繁插拔 **82.** 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

47.8 LINK_UPDOWN

日志内容	Line protocol state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：协议状态，up、down
日志等级	5
举例	IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ethernet0/0 changed to down.
日志说明	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

47.9 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].
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
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.
日志说明	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

47.10 PHY_UPDOWN

日志内容	Physical state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：链路状态，up、down
日志等级	3
举例	IFNET/3/PHY_UPDOWN: Physical state on the Ethernet0/0 changed to down.
日志说明	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。.

47.11 PROTOCOL_UPDOWN

日志内容	Protocol [STRING] state on the interface [STRING] changed to [STRING].
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
举例	IFNET/5/PROTOCOL_UPDOWN: Protocol IPX state on the interface Ethernet6/4/1 changed to up.
日志说明	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

47.12 STORM_CONSTRAIN_BELOW

日志内容	[STRING] is in controlled status, [STRING] flux falls below its lower threshold [STRING].
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
举例	IFNET/1/STORM_CONSTRAIN_BELOW: GigabitEthernet1/0/1 is in controlled status, BC flux falls below its lower threshold 90%.
日志说明	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

47.13 STORM_CONSTRAIN_CONTROLLED

日志内容	[STRING] turned into controlled status, port status is controlled, packet type is [STRING], upper threshold is [STRING].
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
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%.
日志说明	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

47.14 STORM_CONSTRAIN_EXCEED

日志内容	[STRING] is in controlled status, [STRING] flux exceeds its upper threshold [STRING].
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
举例	IFNET/1/STORM_CONSTRAIN_EXCEED: GigabitEthernet1/0/1 is in controlled status, BC flux exceeds its upper threshold 90%.
日志说明	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

47.15 STORM_CONSTRAIN_NORMAL

日志内容	[STRING] returned to normal status, port status is [STRING], packet type is [STRING], lower threshold is [STRING].
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
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%.
日志说明	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

47.16 TUNNEL_LINK_UPDOWN

日志内容	Line protocol state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：协议状态，up、down
日志等级	5
举例	IFNET/5/TUNNEL_LINK_UPDOWN: Line protocol state on the interface Tunnel1 changed to down.
日志说明	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

47.17 TUNNEL_PHY_UPDOWN

日志内容	Physical state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：链路状态，up、down
日志等级	3
举例	IFNET/3/TUNNEL_PHY_UPDOWN: Physical state on the Tunnel1 changed to down.
日志说明	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

47.18 VLAN_MODE_CHANGE

日志内容	Dynamic VLAN [INT32] has changed to a static VLAN.
参数解释	$1：VLANID
日志等级	5
举例	IFNET/5/VLAN_MODE_CHANGE: Dynamic VLAN 20 has changed to a static VLAN.
日志说明	创建VLAN接口导致动态VLAN转换成静态VLAN
处理建议	无

48 IKE

本节介绍 IKE 模块输出的日志信息。

48.1 IKE_P1_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 1 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：失败原因： • IKE 提议匹配失败，显示为：no matching proposal • ID 信息无效，显示为：invalid ID information • 证书不可用，显示为：unavailable certificate • 不支持的 DOI，显示为：unsupported DOI • 不支持当前应用场景，显示为：unsupported situation • IKE 提议语法无效，显示为：invalid proposal syntax • SPI 无效，显示为：invalid SPI • 协议 ID 错误，显示为：invalid protocol ID • 证书无效显示为：invalid certificate • 认证失败，显示为：authentication failure • 信息头错误，显示为：invalid message header • 变换载荷 ID 无效，显示为：invalid transform ID • 载荷形式错误，显示为：malformed payload • 重传超时，显示为：retransmission timeout • 配置错误，显示为：incorrect configuration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA for the reason of no matching proposal. The SA's source address is 1.1.1.1 and its destination address is 2.2.2.2.
日志说明	IKE建立第一阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE配置

48.2 IKE_P2_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 2 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：失败原因： • 密钥信息无效，显示为：invalid key information • ID 信息无效，显示为：invalid ID information • IKE 提议不可用，显示为：unavailable proposal • 不支持的 DOI，显示为：unsupported DOI • 不支持当前应用场景，显示为：unsupported situation • IKE 提议语法无效，显示为：invalid proposal syntax • SPI 无效，显示为：invalid SPI • 协议 ID 无效，显示为：invalid protocol ID • 哈希信息无效，显示为：invalid hash information • 信息头无效，显示为：invalid message header • 载荷形式错误，显示为：malformed payload • 重传超时，显示为：retransmission timeout • 配置错误，显示为：incorrect configuration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA for the reason of invalid key information. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IKE建立第二阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE和IPsec配置

48.3 IKE_P2_SA_TERMINATE

日志内容	The IKE phase 2 SA was deleted for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：删除SA的原因，SA过期，显示为SA expiration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted for the reason of SA expiration. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	第二阶段SA由于过期失效而删除
处理建议	无

48.4 IKE_VERIFY_CERT_FAIL

日志内容	Failed to verify the peer certificate. Reason: [STRING].
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
举例	IKE/6/IKE_VERIFY_CERT_FAIL: Failed to verify the peer certificate. Reason: invalid or inconsistent certificate extension.
日志说明	验证证书失败，可能原因，证书格式无效等
处理建议	无

49 IP6ADDR

本节介绍 IPv6 地址模块输出的日志信息。

49.1 IP6ADDR_CREATEADDRESS_ERROR

日志内容	Failed to create an address by the prefix. Reason: [STRING] on [STRING] and [STRING] on [STRING] overlap.
参数解释	$1：IPv6地址前缀 $2：接口名 $3：IPv6地址前缀 $4：接口名
日志等级	4
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.
日志说明	当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，此时输出本日志
处理建议	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

49.2 IP6ADDR_FUNCTION_FAIL

日志内容	Failed to enable IPv6 on interface [STRING]. Reason: [STRING].
参数解释	$1：接口名 $2：使能IPv6功能失败的原因： • 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
举例	IP6ADDR/6/IP6ADDR_FUNCTION_FAIL: Failed to enable IPv6 on interface GigabitEthernet1/0/1. Reason: Insufficient resources.
日志说明	接口通过有状态或无状态方式获取IPv6地址时，或手工指定接口的IPv6地址时，会使能IPv6功能。如果为接口配置IPv6地址失败，即使能IPv6功能失败，则打印此日志。使能IPv6功能失败的原因一般有：资源不足、设备不支持IPv6等
处理建议	• 如果是因为资源不足，可清理设备内存以释放资源，然后重新执行操作 • 如果是未知错误，请联系技术支持

50 IPADDR

本节介绍 IP 地址模块输出的日志信息。

50.1 IPADDR_HA_EVENT_ERROR

日志内容	A process failed HA upgrade because [STRING].

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
举例	IPADDR/4/IPADDR_HA_EVENT_ERROR: A process failed HA upgrade because IPADDR failed the smooth upgrade.
日志说明	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	请联系技术支持

50.2 IPADDR_HA_STOP_EVENT

日志内容	The device received an HA stop event.
参数解释	无
日志等级	4
举例	IPADDR/4/IPADDR_HA_STOP_EVENT: The device received an HA stop event.
日志说明	设备收到HA STOP事件
处理建议	请联系技术支持

51 IPFW

本节包含 IPFW（IP Forwarding）日志信息。

51.1 IPFW_FAILURE

日志内容	The card doesn't support the split horizon forwarding configuration.
参数解释	无
日志等级	5
举例	IPFW/5/IPFW_FAILURE: -MDC=1; The card doesn't support the split horizon forwarding configuration.
日志说明	单板不支持配置转发水平分割
处理建议	**83.** 请确保所属单板支持转发水平分割配置 **84.** 请联系技术支持

日志内容	Failed to configure split horizon forwarding on the card.
参数解释	无
日志等级	5
举例	IPFW/5/IPFW_FAILURE: -MDC=1; Failed to configure split horizon forwarding on the card.
日志说明	单板配置转发水平分割失败
处理建议	请联系技术支持

52 IPSEC

本节介绍 IPsec 模块输出的日志信息。

52.1 IPSEC_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	$1：失败原因
日志等级	4
举例	IPSEC/4/IPSEC_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足等
处理建议	对于硬件资源不足情况，请联系技术支持

52.2 IPSEC_PACKET_DISCARDED

日志内容	IPsec packet discarded, Src IP:[STRING], Dst IP:[STRING], SPI:[UINT32], SN:[UINT32], Cause:[STRING].
参数解释	$1：报文的源IP地址 $2：报文的目的IP地址 $3：SPI（Security Parameter Index，安全参数索引） $4：报文的序列号 $5：报文丢弃的原因： • 抗重放检测失败，显示为：Anti-replay checking failed. • AH 认证失败，显示为：AH authentication failed. • ESP 认证失败，显示为：ESP authentication failed. • SA 无效，显示为：Invalid SA. • ESP 解密失败，显示为：ESP decryption failed. • 报文的源地址匹配不上 SA，显示为：Source address of packet does not match the SA. • 没有匹配的 ACL 规则，显示为：No ACL rule matched.
日志等级	6
举例	IPSEC/6/IPSEC_PACKET_DISCARDED: IPsec packet discarded, Src IP:1.1.1.2, Dest IP:1.1.1.4, SPI:1002, SN:0, Cause:ah authentication failed
日志说明	IPsec报文被丢弃
处理建议	无

52.3 IPSEC_SA_ESTABLISH

日志内容	Established IPsec SA. The SA’s source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	$1：IPsec SA的源IP地址 $2：IPsec SA的目的IP地址 $3：IPsec SA使用的安全协议 $4：IPsec SA的SPI
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH: Established IPsec SA. The SA’s source address is 1.1.1.1, destination address is 2.2.2.2, protocol is AH, and SPI is 2435.
日志说明	IPsec SA创建成功
处理建议	无

52.4 IPSEC_SA_ESTABLISH_FAIL

日志内容	Failed to establish IPsec SA for the reason of [STRING]. The SA’s source address is [STRING], and its destination address is [STRING].
参数解释	$1：IPsec SA创建失败的原因： • 隧道创建失败，显示为：Tunnel establishment failure. • 配置不完整，显示为：Incomplete configuration. • 配置的安全提议无效，显示为：Unavailable transform set. $2：源IP地址 $3：目的IP地址
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA for the reason of creating tunnel failure. The SA’s source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IPsec SA创建失败。触发该日志的原因可能有：隧道创建失败、配置不完整、或者配置的安全提议无效
处理建议	检查本端和对端设备上的IPsec配置

52.5 IPSEC_SA_INITINATION

日志内容	Began to establish IPsec SA. The SA’s source address is [STRING], and its destination address is [STRING].
参数解释	$1：IPsec SA的源IP地址 $2：IPsec SA的目的IP地址
日志等级	6
举例	IPSEC/6/IPSEC_SA_INITINATION: Began to establish IPsec SA. The SA’s source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	开始创建IPsec SA
处理建议	无

52.6 IPSEC_SA_TERMINATE

日志内容	The IPsec SA was deleted for the reason of [STRING]. The SA’s source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	$1：IPsec SA被删除的原因： • SA 空闲超时，显示为：SA idle timeout. • 执行了 reset 命令，显示为：**reset** command executed. $2：源IP地址 $3：目的IP地址 $4：使用的安全协议 $5：SPI
日志等级	6
举例	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted for the reason of SA idle timeout. The SA’s source address is 1.1.1.1, destination address is 2.2.2.2, protocol is ESP, and SPI is 34563.
日志说明	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	无

53 IPSG

本节介绍 IPSG（IP Source Guard）模块输出的日志信息。

53.1 IPSG_ADDENTRY_ERROR

日志内容	Failed to add an IP source guard binding (IP [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
参数解释	$1：IPv4地址或IPv6地址（如果没有指定，则显示N/A） $2：MAC地址（如果没有指定，则显示为N/A） $3：VLAN ID（如果没有指定，则显示为无意义值65535） $4：接口名称（如果没有指定，则显示为N/A） $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
举例	IPSG/6/IPSG_ADDENTRY_ERROR: Failed to add an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Resources not sufficient.
日志说明	下发静态或动态IP Source Guard绑定表项失败，可能的原因有：特性不支持、资源不足、表项达到最大规格或未知错误
处理建议	• 当提示硬件资源不足时，可清理设备内存以释放资源 • 当下发是静态 IP Source Guard 绑定表项时，可重新执行命令下发该表项 • 当下发静态或动态 IP Source Guard 绑定表项失败原因为未知错误时，请联系技术支持

53.2 IPSG_ADDEXCLUDEDVLAN_ERROR

日志内容	Failed to add excluded VLANs (start VLAN [UINT16] to end VLAN [UINT16]). [STRING].
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
举例	IPSG/6/IPSG_ADDEXCLUDEDVLAN_ERROR: -MDC=1-Slot=4; Failed to add excluded VLANs (start VLAN 1 to end VLAN 5). Resources not sufficient.
日志说明	下发免过滤VLAN失败，可能的原因有：特性不支持、资源不足或未知错误
处理建议	• 因硬件资源不足而引起的免过滤 VLAN 下发失败，可清理设备内存以释放资源，然后重新执行命令下发该配置 • 当下发免过滤 VLAN 失败原因为未知错误时，请联系技术支持

53.3 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].
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
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.
日志说明	ARP表项和本地绑定表项的MAC地址冲突。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，则会输出该日志
处理建议	检查ARP表项的来源设备是否存在恶意攻击行为

53.4 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].
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
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.
日志说明	ARP表项和远端绑定表项的MAC地址冲突，有以下情况会输出该日志： • 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且MAC地址发生改变，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，请检查 ARP 表项的来源设备 • 对于漫游用户本地上线，无需处理

53.5 IPSG_DELENTRY_ERROR

日志内容	Failed to delete an IP source guard binding (IP [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
参数解释	$1：IP地址（如果没有指定，则显示N/A） $2：MAC地址（如果没有指定，则显示为N/A） $3：VLAN ID（如果没有指定，则显示为无意义值65535） $4：接口名（如果没有指定，则显示为N/A） $5：失败原因： • Feature not supported： 特性不支持 • Unknown error：未知错误
日志等级	6
举例	IPSG/6/IPSG_DELENTRY_ERROR: Failed to delete an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Unknown error.
日志说明	删除全局静态IP Source Guard绑定表项失败，可能的原因有：特性不支持或者未知错误
处理建议	• 重新执行命令删除该表项 • 当删除全局静态 IP Source Guard 绑定表项失败原因为未知错误时，请联系技术支持

53.6 IPSG_DELEXCLUDEDVLAN_ERROR

日志内容	Failed to delete excluded VLANs (start VLAN [UINT16] to end VLAN [UINT16]). [STRING].
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
举例	IPSG/6/IPSG_DELEXCLUDEDVLAN_ERROR: -MDC=1-Slot=4; Failed to delete excluded VLANs (start VLAN 1 to end VLAN 5). Resources not sufficient.
日志说明	删除免过滤VLAN失败，可能的原因有：特性不支持、资源不足或未知错误
处理建议	• 因硬件资源不足而引起的删除免过滤 VLAN 失败，可清理设备内存以释放资源，然后重新执行命令下发该配置 • 当删除免过滤 VLAN 失败原因为未知错误时，请联系技术支持

53.7 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].
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
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.
日志说明	远端绑定表项和本地绑定表项的MAC地址冲突。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，则会输出该日志
处理建议	无需处理

53.8 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].
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
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.
日志说明	ND表项和本地绑定表项的MAC地址冲突。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，则会输出该日志
处理建议	检查ND表项的来源设备是否存在恶意攻击行为

53.9 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].
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
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.
日志说明	ND表项和远端绑定表项的MAC地址冲突，有以下情况会输出该日志： • 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且 MAC 地址发生改变，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，请检查 ND 表项的来源设备 • 对于漫游用户本地上线，无需处理

53.10 IPSG_IPV4_ALARMCLEAR

日志内容	The packet dropping rate on [STRING] dropped below [UINT32] pps.
参数解释	$1：接口名称 $2：告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV4_ALARMCLEAR: The packet dropping rate on GigabitEthernet1/0/1 dropped below 100 pps.
日志说明	接口上每秒丢弃报文数恢复到告警阈值之内
处理建议	无

53.11 IPSG_IPV4_ALARMEMERGE

日志内容	The packet dropping rate on [STRING] reached or exceeded [UINT32] pps.
参数解释	$1：接口名称 $2：告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV4_ALARMEMERGE: The packet dropping rate on GigabitEthernet1/0/1 reached or exceeded 100 pps.
日志说明	接口上每秒丢弃报文数大于或等于告警阈值
处理建议	检查遭到攻击的接口下的用户是否存在攻击源

53.12 IPSG_IPV6_ALARMCLEAR

日志内容	The packet dropping rate on [STRING] dropped below [UINT32] pps.
参数解释	$1：接口名称 $2：告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV6_ALARMCLEAR: The packet dropping rate on GigabitEthernet1/0/1 dropped below 100 pps.
日志说明	接口上每秒丢弃报文数恢复到告警阈值之内
处理建议	无

53.13 IPSG_IPV6_ALARMEMERGE

日志内容	The packet dropping rate on [STRING] reached or exceeded [UINT32] pps.
参数解释	$1：接口名称 $2：告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV6_ALARMEMERGE: The packet dropping rate on GigabitEthernet1/0/1 reached or exceeded 100 pps.
日志说明	接口上每秒丢弃报文数大于或等于告警阈值
处理建议	检查遭到攻击的接口下是否存在攻击源

54 IRDP

本节介绍 IRDP 模块输出的日志信息。

54.1 IRDP_EXCEED_ADVADDR_LIMIT

日志内容	The number of advertisement addresses on interface [STRING] exceeded the limit 255.
参数解释	$1：接口名称
日志等级	6
举例	IRDP/6/IRDP_EXCEED_ADVADDR_LIMIT: The number of advertisement addresses on interface Ethernet1/1/0/2 exceeded the limit 255.
日志说明	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地址

55 IRF

本节介绍 IRF（Intelligent Resilient Framework，智能弹性架构）模块输出的日志信息。

55.1 IRF_LINK_BLOCK

日志内容	IRF port went blocked.
参数解释	无
日志等级	2
举例	IRF/2/IRF_LINK_BLOCK: IRF port went blocked.
日志说明	IRF端口链路状态变为blocked。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。例如，检测到成员编号冲突时，优先级低的设备上会打印该日志信息
处理建议	请确认组网中是否存在成员编号冲突的设备。如果存在，请将成员编号修改为不同的值

55.2 IRF_LINK_DOWN

日志内容	IRF port went down.
参数解释	无
日志等级	3
举例	IRF/3/IRF_LINK_DOWN: IRF port went down.
日志说明	IRF端口链路状态变为down
处理建议	请确认： • IRF 端口下是否绑定了物理接口 • 绑定的物理接口是否和对端正确连接

55.3 IRF_LINK_UP

日志内容	IRF port came up.
参数解释	无
日志等级	6
举例	IRF/6/IRF_LINK_UP: IRF port came up.
日志说明	IRF端口链路状态变为up
处理建议	无

55.4 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].
参数解释	$1：设备的成员编号 $2：设备的CPU MAC
日志等级	4
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.
日志说明	在同一广播域中发现跟自己成员编号相同的设备时，打印该日志，提示成员冲突
处理建议	根据提示信息，检查IRF中的成员编号，重新设置新加入设备的成员编号

55.5 IRF_MERGE

日志内容	IRF merge occurred.
参数解释	无
日志等级	4
举例	IRF/4/IRF_MERGE: IRF merge occurred.
日志说明	IRF发生合并时，打印该日志信息
处理建议	无

55.6 IRF_MERGE_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system needs a reboot.
参数解释	无
日志等级	4
举例	IRF/4/IRF_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
日志说明	IRF发生合并时，主设备优先级低的IRF需要重启，打印该日志
处理建议	重启主设备优先级低的IRF完成合并

55.7 IRF_MERGE_NOT_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system does not need to reboot.
参数解释	无
日志等级	5
举例	IRF/5/IRF_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
日志说明	IRF发生合并时，主设备优先级高的IRF不需要重启，打印该日志
处理建议	无

56 ISIS

本节介绍 IS-IS 模块输出的日志信息。

56.1 ISIS_LSP_CONFLICT

日志内容	IS-IS [UINT16], [STRING] LSP, LSPID=[STRING], SeqNum=[HEX], system ID conflict might exist.
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
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.
日志说明	网络中可能存在System ID冲突
处理建议	检查产生该LSP的设备的System ID是否和其他设备的System ID冲突

56.2 ISIS_MEM_ALERT

日志内容	ISIS Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	ISIS/5/ISIS_MEM_ALERT: ISIS Process received system memory alert start event.
日志说明	IS-IS模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

56.3 ISIS_NBR_CHG

日志内容	IS-IS [UINT16], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING], Reason: [STRING].
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 $6：邻居状态变化原因
日志等级	5
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.
日志说明	邻居状态发生变化
处理建议	需要关注邻居状态变化原因。当邻居状态变为down时，检查IS-IS配置正确性和网络连通性

57 ISSU

本节介绍 ISSU 模块输出的日志信息。

57.1 ISSU_LOAD_FAILED

日志内容	Failed to execute the issu load command.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_LOAD_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the issu load command.
日志说明	用户执行**issu load**命令进行ISSU升级，操作失败
处理建议	请根据提示信息采取相应措施

57.2 ISSU_LOAD_SUCCESS

日志内容	Executed the issu load command successfully.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_LOAD_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the issu load command successfully.
日志说明	用户执行**issu load**命令进行ISSU升级，操作成功
处理建议	无

57.3 ISSU_PROCESSWITCHOVER

日志内容	Switchover completed. The standby process became the active process.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_PROCESSWITCHOVER: Switchover completed. The standby process became the active process.
日志说明	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
处理建议	无

57.4 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.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	4
举例	ISSU/4/ISSU_ROLLBACKCHECKNORMAL: The rollback might not be able to restore the previous version for chassis 1 slot 2 because the state is not normal.
日志说明	ISSU升级，ISSU状态处理Switching，用户执行**issu rollback**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	无

58 L2PT

本节介绍 L2PT 模块输出的日志信息。

58.1 L2PT_ADD_GROUPMEMBER_FAILED

日志内容	Failed to add [STRING] as a member to the VLAN tunnel group for [STRING].
参数解释	$1：接口名称 $2：协议类型
日志等级	4
举例	L2PT/4/L2PT_ADD_GROUPMEMBER_FAILED: Failed to add GigabitEthernet2/0/1 as a member to the VLAN tunnel group for STP.
日志说明	接口加入协议的VLAN Tunnel组播组失败
处理建议	无

58.2 L2PT_CREATE_TUNNELGROUP_FAILED

日志内容	Failed to create a VLAN tunnel group for [STRING].
参数解释	$1：协议类型
日志等级	4
举例	L2PT/4/L2PT_CREATE_TUNNELGROUP_FAILED: Failed to create a VLAN tunnel group for STP.
日志说明	创建协议的VLAN Tunnel组播组失败
处理建议	无

58.3 L2PT_ENABLE_DROP_FAILED

日志内容	Failed to enable [STRING] packet drop on [STRING].
参数解释	$1：协议类型 $2：接口名称
日志等级	4
举例	L2PT/4/L2PT_ENABLE_DROP_FAILED: Failed to enable STP packet drop on GigabitEthernet2/0/1.
日志说明	接口上使能L2PT Drop功能失败
处理建议	无

58.4 L2PT_SET_MULTIMAC_FAILED

日志内容	Failed to set a tunnel destination MAC address to [MAC].
参数解释	$1：MAC地址
日志等级	4
举例	L2PT/4/L2PT_SET_MULTIMAC_FAILED: Failed to set a tunnel destination MAC address to 010f-e200-0003.
日志说明	配置BPDU Tunnel报文的目的MAC地址失败
处理建议	无

59 L2TPV2

本节介绍 L2TPV2 模块输出的日志信息。

59.1 L2TPV2_SESSION_EXCEED_LIMIT

日志内容	Number of L2TP sessions exceeded the limit.
参数解释	无
日志等级	4
举例	L2TPV2/4/L2TPV2_SESSION_EXCEED_LIMIT: Number of L2TP sessions exceeded the limit.
日志说明	设备上建立的L2TP会话数目已经达到最大值
处理建议	无

59.2 L2TPV2_TUNNEL_EXCEED_LIMIT

日志内容	Number of L2TP tunnels exceeded the limit.
参数解释	无
日志等级	4
举例	L2TPV2/4/L2TPV2_TUNNEL_EXCEED_LIMIT: Number of L2TP tunnels exceeded the limit.
日志说明	设备上建立的L2TP隧道数目已经达到最大值
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

60 L2VPN

本节介绍 L2VPN 模块输出的日志信息。

60.1 L2VPN_BGPVC_CONFLICT_LOCAL

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with local site.
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
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.
日志说明	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

60.2 L2VPN_BGPVC_CONFLICT_REMOTE

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with another remote site.
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
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.
日志说明	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

60.3 L2VPN_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for L2VPN.
参数解释	无
日志等级	4
举例	L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH: No enough hardware resource for L2VPN.
日志说明	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

60.4 L2VPN_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for L2VPN are restored.
参数解释	无
日志等级	6
举例	L2VPN/6/L2VPN_HARD_RESOURCE_RESTORE: Hardware resources for L2VPN are restored.
日志说明	L2VPN硬件资源恢复
处理建议	无

60.5 L2VPN_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for a static PW in [STRING] [STRING] is duplicate.
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
举例	L2VPN/4/L2VPN_LABEL_DUPLICATE: Incoming label 1024 for a static PW in Xconnect-group aaa is duplicate.
日志说明	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

61 LAGG

本节介绍 LAGG 模块输出的日志信息。

61.1 LAGG_ACTIVE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the active state.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_ACTIVE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the active state.
日志说明	聚合组内某成员端口成为激活端口
处理建议	无

61.2 LAGG_AUTO_AGGREGATION

日志内容	Failed to assign automatic assignment-enabled interface [STRING] to an aggregation group. Please check the configuration on the interface.
参数解释	$1：端口名称
日志等级	6
举例	LAGG/6/LAGG_AUTO_AGGREGATON: Failed to assign automatic assignment-enabled interface FGE1/0/1 to an aggregation group. Please check the configuration on the interface.
日志说明	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

61.3 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.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
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.
日志说明	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，该成员端口成为去激活端口
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

61.4 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 was down.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
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.
日志说明	聚合成员端口上的BFD会话down时，该成员端口变为去激活状态
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

61.5 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.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
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.
日志说明	由于聚合组内某成员端口配置限制，该成员端口变为去激活状态
处理建议	无

61.6 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.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
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.
日志说明	由于聚合组内某成员端口的双工模式与参考端口不一致，该成员端口变为去激活状态
处理建议	修改该端口双工模式，使其与参考端口一致

61.7 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.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
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.
日志说明	聚合组内某成员端口因硬件限制与参考端口不一致，该成员端口变为去激活状态
处理建议	无

61.8 LAGG_INACTIVE_LOWER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports is below the lower limit.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_LOWER_LIMIT: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the number of active ports is below the lower limit.
日志说明	因聚合组内激活端口数量未达到配置的最小激活端口数，聚合组内某成员端口变为去激活状态
处理建议	增加激活端口数量，使其达到最小激活端口数

61.9 LAGG_INACTIVE_PARTNER

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_PARTNER: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
日志说明	动态聚合组内，由于对端端口聚合配置不正确变为去激活状态，本端端口变为去激活状态
处理建议	无

61.10 LAGG_INACTIVE_PHYSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the physical state of the port is down.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_PHYSTATE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the physical state of the port is down.
日志说明	聚合组内某成员端口处于down状态，该成员端口变为去激活状态
处理建议	使该端口处于UP状态

61.11 LAGG_INACTIVE_RESOURCE_INSUFICIE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because all aggregate resources are occupied.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_RESOURCE_INSUFICIE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because all aggregate resources are occupied.
日志说明	聚合资源不足导致聚合组内成员端口变为去激活端口
处理建议	无

61.12 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 is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_SPEED: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the speed configuration of the port is incorrect.
日志说明	聚合组内某成员端口速率与参考端口不一致，该端口变为去激活状态
处理建议	修改该端口速率，使其与参考端口一致

61.13 LAGG_INACTIVE_UPPER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports has reached the upper limit.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_UPPER_LIMIT: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the number of active ports has reached the upper limit.
日志说明	动态聚合组内激活端口数量已达到上限。后加入的成员端口成为激活端口，致使某成员端口变为去激活状态
处理建议	无

61.14 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.
参数解释	$1：聚合接口编号
日志等级	4
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.
日志说明	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

62 LDP

本节介绍 LDP 模块输出的日志信息。

62.1 LDP_MPLSLSRID_CHG

日志内容	Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
参数解释	无
日志等级	5
举例	LDP/5/LDP_MPLSLSRID_CHG: -MDC=1; Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
日志说明	公网LDP和VPN实例LDP的LSR ID选择方式为： **85.** 如果配置了 LDP LSR ID，则 LDP 的 LSR ID 为此命令配置的值 **86.** 否则，LDP 的 LSR ID 为 MPLS LSR ID 当公网LDP或VPN实例LDP的LSR ID没配置时，修改MPLS LSR ID，会触发该日志。日志提示用户手动重启公网LDP或VPN实例LDP会话使得新配置的MPLS LSR ID生效
处理建议	当公网LDP或VPN实例LDP的LSR ID没配置时，使用命令**display mpls ldp parameter**查看已生效的LSR ID，与配置的MPLS LSR ID 比较，如果不一致，请手动重启LDP会话

62.2 LDP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
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。如果会话状态是down，则会在括号内显示会话失败的原因
日志等级	5
举例	LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up. LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, VPN instance: vpn1) is down (hello hold timer expired).
日志说明	会话状态改变了
处理建议	当会话状态是up时，无 当会话状态是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 会话失败原因包括： • interface not operational：接口不可用 • MPLS disabled on interface：接口已取消使能 MPLS • LDP disabled on interface：接口已取消使能 LDP • LDP auto-configure disabled on interface：接口已取消使能 LDP 自动配置功能 • VPN instance changed on interface：接口所属的 VPN 实例已更改 • LDP instance deleted：LDP 实例已删除 • targeted peer deleted：LDP 对等体已删除。其中，targeted peer 可以有 4 种方式产生：手动配置、L2VPN 自动注册、TE 隧道自动注册（LDP over TE 功能）、会话保护自动注册 • L2VPN disabled targeted peer：L2VPN 注销 targeted peer • TE tunnel disabled targeted peer：TE 隧道注销 targeted peer • session protection disabled targeted peer：会话保护注销 targeted peer • process deactivated：LDP 进程降级 • failed to receive the initialization message：未收到初始化信息 • graceful restart reconnect timer expired：平滑重启重连时间超时 • failed to recover adjacency by NSR：NSR 恢复邻接关系失败 • failed to upgrade session by NSR：NSR 升级会话失败 • closed the GR session：GR 会话关闭 • keepalive hold timer expired：keepalive 保持时间超时 • adjacency hold timer expired：邻接关系保持时间超时 • session reset manually：手动重启会话 • TCP connection down：TCP 连接断开 • received a fatal notification message ：收到致命的通知信息 • internal error：内部错误 • memory in critical state：内存达到 critical 状态 • transport address changed on interface：接口上的传输地址更改

62.3 LDP_SESSION_GR

日志内容	Session ([STRING], [STRING]): ([STRING]).
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
举例	LDP/5/LDP_SESSION_GR: Session (22.22.22.2:0, VPN instance: vpn1): Start reconnection.
日志说明	当已协商支持对端设备LDP平滑重启的LDP会话down时，触发该日志。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，链路状态和其他相关配置，其他情况无需处理

62.4 LDP_SESSION_SP

日志内容	Session ([STRING], [STRING]): ([STRING]).
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
举例	LDP/5/LDP_SESSION_SP: Session (22.22.22.2:0, VPN instance: vpn1): Hold up the session.
日志说明	当会话的最后一个Link hello邻接关系丢失时，触发该日志。日志显示会话保护过程的状态变化
处理建议	检查接口状态和链路状态

63 LLDP

本节介绍 LLDP 模块输出的日志信息。

63.1 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].
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
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.
日志说明	端口收到新邻居发来的LLDP报文
处理建议	无

63.2 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].
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
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.
日志说明	当邻居被删除时，接口收到删除消息
处理建议	无

63.3 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.
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
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.
日志说明	接口邻居数未达到最大值，还可以为接口增加新邻居
处理建议	无

63.4 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].
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
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.
日志说明	当接口在一段时间内没有收到邻居发来的LLDP报文时，打印本信息
处理建议	检查链路状态，或者检查对端LLDP的接收和发送状态

63.5 LLDP_NEIGHBOR_PROTECTION_BLOCK

日志内容	The status of port [STRING] changed to blocked ([STRING]) for the [STRING] agent.
参数解释	$1：接口名称 $2：接口保护类型，aging或validation $3：代理类型
日志等级	4
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.
日志说明	当接口阻塞时，打印本信息，并且说明阻塞原因
处理建议	• 当接口保护类型是 aging 时：检查链路状态，或者检查两端 LLDP 的接收和发送状态 • 当接口保护类型是 validation 时：检查收到报文的 Chassis ID subtype、Chassis ID 和 Port ID subtype、Port ID 值与配置的邻居识别信息是否一致

63.6 LLDP_NEIGHBOR_PROTECTION_DOWN

日志内容	The status of port [STRING] changed to down (aging) for the [STRING] agent.
参数解释	$1：接口名称 $2：代理类型
日志等级	4
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.
日志说明	当端口接收报文超时关闭端口时，打印本信息，并且说明DOWN原因
处理建议	当接口保护类型是aging时：检查链路状态，或者检查两端LLDP的接收和发送状态

63.7 LLDP_NEIGHBOR_PROTECTION_UNBLOCK

日志内容	The status of port [STRING] changed to unblocked for the [STRING] agent.
参数解释	$1：接口名称 $2：代理类型
日志等级	4
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.
日志说明	当接口由阻塞状态转换为非阻塞状态时，打印本信息
处理建议	无

63.8 LLDP_NEIGHBOR_PROTECTION_UP

日志内容	The status of port [STRING] changed to up for the [STRING] agent.
参数解释	$1：接口名称 $2：代理类型
日志等级	4
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.
日志说明	当接口由DOWN状态转换为UP状态时，打印本信息
处理建议	无

63.9 LLDP_PVID_INCONSISTENT

日志内容	PVID mismatch discovered on [STRING] (PVID [UINT32]), with [STRING] [STRING] (PVID [STRING]).
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
举例	LLDP/5/LLDP_PVID_INCONSISTENT: MDC=1; PVID mismatch discovered on Ten-GigabitEthernet0/2/6 (PVID 1), with Ten-GigabitEthernet0/2/7 (PVID 500).
日志说明	当邻居的PVID信息与接口本地的PVID不同时，打印本信息
处理建议	修改邻居两端的PVID，使其一致

63.10 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.
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
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.
日志说明	当邻居数达到最大值的接口收到LLDP报文时，打印本信息
处理建议	无

64 LOAD

本节介绍 LOAD 模块输出的日志信息。

64.1 BOARD_LOADING

日志内容	Board in chassis [INT32] slot [INT32] is loading software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	4
举例	LOAD/4/BOARD_LOADING: Board in chassis 1 slot 5 is loading software images.
日志说明	单板启动过程中，加载启动软件包
处理建议	无

64.2 LOAD_FAILED

日志内容	Board in chassis [INT32] slot [INT32] failed to load software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	3
举例	LOAD/3/LOAD_FAILED: Board in chassis 1 slot 5 failed to load software images.
日志说明	单板在启动过程中，加载启动软件包失败
处理建议	**87.** 使用 **`display boot-loader`** 命令查看单板使用的下次启动软件包 **88.** 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 **89.** 如果仍不能解决，请联系工程师

64.3 LOAD_FINISHED

日志内容	Board in chassis [INT32] slot [INT32] has finished loading software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	5
举例	LOAD/5/LOAD_FINISHED: Board in chassis 1 slot 5 has finished loading software images.
日志说明	单板完成文件加载
处理建议	无

65 LOGIN

本节介绍 LOGIN（登录管理）模块输出的日志信息。

65.1 LOGIN_FAILED

日志内容	[STRING] failed to login from [STRING].
参数解释	$1：用户名 $2：用户线名和IP地址
日志等级	5
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.
日志说明	用户登录失败
处理建议	无

65.2 LOGIN_INVALID_USERNAME_PWD

日志内容	Invalid username or password from [STRING].
参数解释	$1：用户线名和IP地址
日志等级	5
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.
日志说明	用户输入无效的用户名或密码
处理建议	无

66 LPDT

本节介绍 LPDT 模块输出的日志信息。

66.1 LPDT_LOOPED

日志内容	A loop was detected on [STRING].
参数解释	$1：接口名
日志等级	4
举例	LPDT/4/LPDT_LOOPED: A loop was detected on GigabitEthernet1/0/1.
日志说明	接口首次检测到有VLAN发生环路时，环路检测模块会生成该信息
处理建议	检查网络环路

66.2 LPDT_RECOVERED

日志内容	All loops were removed on [STRING].
参数解释	$1：接口名
日志等级	5
举例	LPDT/5/LPDT_RECOVERED: All loops were removed on GigabitEthernet1/0/1.
日志说明	接口检测到所有VLAN的环路都消除时，环路检测模块会生成该信息
处理建议	无需处理

66.3 LPDT_VLAN_LOOPED

日志内容	A loop was detected on [STRING] in VLAN [UINT16].
参数解释	$1：接口名 $2：VLAN ID
日志等级	4
举例	LPDT/4/LPDT_VLAN_LOOPED: A loop was detected on GigabitEthernet1/0/1 in VLAN 1.
日志说明	接口检测到一个VLAN发生环路时，环路检测模块会生成该信息
处理建议	检查该VLAN的网络环路

66.4 LPDT_VLAN_RECOVERED

日志内容	A loop was removed on [STRING] in VLAN [UINT16].
参数解释	$1：接口名 $2：VLAN ID
日志等级	5
举例	LPDT/5/LPDT_VLAN_RECOVERED: A loop was removed on GigabitEthernet1/0/1 in VLAN 1.
日志说明	接口检测到一个VLAN的环路消除时，环路检测模块会生成该信息
处理建议	无需处理

67 LS

本节包含本地服务器日志信息。

67.1 LOCALSVR_PROMPTED_CHANGE_PWD

日志内容	Please change the password of [STRING] [STRING], because [STRING].
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
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.
日志说明	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

67.2 LS_ADD_USER_TO_GROUP

日志内容	Admin [STRING] added user [STRING] to group [STRING].
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4
举例	LS/4/LS_ADD_USER_TO_GROUP: Admin admin added user user1 to group group1.
日志说明	管理员添加一个用户到一个用户组
处理建议	无

67.3 LS_AUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed authentication. [STRING]
参数解释	$1：用户名 $2：IP地址 $3：失败原因 • 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
日志等级	5
举例	LS/5/LS_AUTHEN_FAILURE: User cwf@system from 192.168.0.22 failed authentication. “User not found.”
日志说明	本地服务器拒绝了一个用户的认证请求
处理建议	无

67.4 LS_AUTHEN_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名 $2：IP地址
日志等级	6
举例	LS/6/LS_AUTHEN_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
日志说明	本地服务器接受了一个用户的认证请求
处理建议	无

67.5 LS_DEL_USER_FROM_GROUP

日志内容	Admin [STRING] delete user [STRING] from group [STRING].
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4
举例	LS/4/LS_DEL_USER_FROM_GROUP: Admin admin delete user user1 from group group1.
日志说明	管理员将用户从用户组里删除
处理建议	无

67.6 LS_DELETE_PASSWORD_FAIL

日志内容	Failed to delete the password for user [STRING].
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_DELETE_PASSWORD_FAIL: Failed to delete the password for user abcd.
日志说明	删除用户密码失败
处理建议	检查文件系统

67.7 LS_PWD_ADDBLACKLIST

日志内容	User [STRING] at [STRING] was added to the blacklist due to multiple login failures, [STRING].
参数解释	$1：用户名 $2：IP地址 $3：结果 • 但是可以做其他的尝试 • 被永久阻塞 • 被临时阻塞指定时间（单位：分钟）
日志等级	4
举例	LS/4/LS_PWD_ADDBLACKLIST: user1 at 192.168.0.22 was added to the blacklist due to multiple login failures, but could make other attempts.
日志说明	用户多次登录失败后被加入了黑名单
处理建议	检查用户的密码

67.8 LS_PWD_CHGPWD_FOR_AGEDOUT

日志内容	User [STRING] changed the password because it was expired.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEDOUT: aaa changed the password because it was expired.
日志说明	用户由于密码已过期而修改了密码
处理建议	无

67.9 LS_PWD_CHGPWD_FOR_AGEOUT

日志内容	User [STRING] changed the password because it was about to expire.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEOUT: aaa changed the password because it was about to expire.
日志说明	用户由于密码即将过期而修改了密码
处理建议	无

67.10 LS_PWD_CHGPWD_FOR_COMPOSITION

日志内容	User [STRING] changed the password because it had an invalid composition.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_COMPOSITION: aaa changed the password because it had an invalid composition.
日志说明	用户由于密码组合错误而修改了密码
处理建议	无

67.11 LS_PWD_CHGPWD_FOR_FIRSTLOGIN

日志内容	User [STRING] changed the password at the first login.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_FIRSTLOGIN: aaa changed the password at the first login.
日志说明	用户首次登录修改了密码
处理建议	无

67.12 LS_PWD_CHGPWD_FOR_LENGTH

日志内容	User [STRING] changed the password because it was too short.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_LENGTH: aaa changed the password because it was too short.
日志说明	用户因为密码太短而修改了密码
处理建议	无

67.13 LS_PWD_FAILED2WRITEPASS2FILE

日志内容	Failed to write the password records to file.
参数解释	无
日志等级	4
举例	LS/4/LS_PWD_FAILED2WRITEPASS2FILE: Failed to write the password records to file.
日志说明	把密码记录写到文件失败
处理建议	无

67.14 LS_PWD_MODIFY_FAIL

日志内容	Admin [STRING] from [STRING] could not modify the password for user [STRING], because [STRING].
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 differnet 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 • 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
日志等级	4
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.
日志说明	修改用户密码失败
处理建议	无

67.15 LS_PWD_MODIFY_SUCCESS

日志内容	Admin [STRING] from [STRING] modify the password for user [STRING] successfully.
参数解释	$1：管理员名 $2：IP地址 $3：用户名
日志等级	6
举例	LS/6/LS_PWD_MODIFY_SUCCESS: Admin admin from 1.1.1.1 modify the password for user abc successfully.
日志说明	管理员成功修改了用户密码
处理建议	无

67.16 LS_REAUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed reauthentication.
参数解释	$1：用户名 $2：IP地址
日志等级	5
举例	LS/5/LS_REAUTHEN_FAILURE: User abcd from 1.1.1.1 failed reauthentication.
日志说明	用户再次认证失败
处理建议	检查旧密码

67.17 LS_UPDATE_PASSWORD_FAIL

日志内容	Failed to update the password for user [STRING].
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_UPDATE_PASSWORD_FAIL: Failed to update the password for user abc.
日志说明	为用户更新密码失败
处理建议	检查文件系统

67.18 LS_USER_CANCEL

日志内容	User [STRING] from [STRING] cancelled inputting the password.
参数解释	$1：用户名 $2：IP地址
日志等级	5
举例	LS/5/LS_USER_CANCEL: User 1 from 1.1.1.1 cancelled inputting the password.
日志说明	用户取消输入密码或者没有在90秒内输入密码
处理建议	无

67.19 LS_USER_PASSWORD_EXPIRE

日志内容	User [STRING]'s login idle timer timed out.
参数解释	$1：用户名
日志等级	5
举例	LS/5/LS_USER_PASSWORD_EXPIRE: User 1's login idle timer timed out.
日志说明	用户登录空闲时间超时
处理建议	无

67.20 LS_USER_ROLE_CHANGE

日志内容	Admin [STRING] [STRING] the user role [STRING] for [STRING].
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
举例	LS/4/LS_USER_ROLE_CHANGE: Admin admin add user role network-admin for user abcd.
日志说明	管理员修改了用户的用户角色
处理建议	无

68 LSPV

本节介绍 LSP 验证模块输出的日志信息。

68.1 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.
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
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.
日志说明	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，检测到LSP隧道或者PW的连通性

69 MAC

本节介绍 MAC 模块输出的日志信息。

69.1 MAC_DRIVER_ADD_ENTRY

日志内容	Driver failed to add MAC address entry: MAC address=[STRING], VLAN=[UINT32], State=[UINT32], interface=[STRING].
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
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.
日志说明	在接口GigabitEthernet1/0/1上添加OpenFlow类型MAC地址失败，MAC地址为1-1-1，所属VLAN为VLAN 1
处理建议	无

69.2 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],
参数解释	$1：MAC地址 $2：协议类型
日志等级	5
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.
日志说明	单板硬件资源不足导致协议报文上送CPU失败
处理建议	无

69.3 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].
参数解释	$1：MAC地址 $2：协议类型 $3：接口名称
日志等级	5
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.
日志说明	单板硬件资源不足导致接口上的协议报文上送CPU失败
处理建议	无

69.4 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].
参数解释	$1：MAC地址 $3：协议类型 $3：VLAN ID
日志等级	5
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.
日志说明	单板硬件资源不足导致VLAN内的协议报文上送CPU失败
处理建议	无

69.5 MAC_TABLE_FULL_GLOBAL

日志内容	The number of MAC address entries exceeded the maximum number [UINT32].
参数解释	$1：最大MAC地址数量
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_GLOBAL: The number of MAC address entries exceeded the maximum number 1024.
日志说明	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	无

69.6 MAC_TABLE_FULL_PORT

日志内容	The number of MAC address entries exceeded the maximum number [UINT32] for interface [STRING].
参数解释	$1：最大MAC地址数量 $2：接口名称
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_PORT: The number of MAC address entries exceeded the maximum number 1024 for interface GigabitEthernet2/0/32.
日志说明	接口对应的MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

69.7 MAC_TABLE_FULL_VLAN

日志内容	The number of MAC address entries exceeded the maximum number [UINT32] in VLAN [UINT32].
参数解释	$1：最大MAC地址数量 $2：VLAN ID
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_VLAN: The number of MAC address entries exceeded the maximum number 1024 in VLAN 2.
日志说明	VLAN对应的MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

69.8 MAC_VLAN_LEARNLIMIT_NORESOURCE

日志内容	The card does not have enough hardware resources to set MAC learning limit for VLAN [UINT16].
参数解释	$1：VLAN ID
日志等级	5
举例	MAC/5/MAC_VLAN_LEARNLIMIT_NORESOURCE: The card does not have enough hardware resources to set MAC learning limit for VLAN 100.
日志说明	单板硬件资源不足导致无法配置VLAN内允许学习的最大MAC地址数量
处理建议	无

69.9 MAC_VLAN_LEARNLIMIT_NOTSUPPORT

日志内容	The card does not support setting MAC learning limit for VLAN [UINT16].
参数解释	$1：VLAN ID
日志等级	5
举例	MAC/5/ MAC_VLAN_LEARNLIMIT_NOTSUPPORT: The card does not support setting MAC learning limit for VLAN 100.
日志说明	单板不支持配置VLAN内允许学习的最大MAC地址数量
处理建议	无

70 MACA

本节介绍 MAC 地址认证模块输出的日志信息。

70.1 MACA_ENABLE_NOT_EFFECTIVE

日志内容	MAC authentication is enabled but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	MACA/3/MACA_ENABLE_NOT_EFFECTIVE: MAC authentication is enabled but is not effective on interface Ethernet3/1/2.
日志说明	MAC地址认证配置在接口上不生效，因为该接口不支持MAC地址认证
处理建议	关闭接口上的MAC地址认证

70.2 MACA_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UserNameFormat=[STRING]; User failed MAC authentication. Reason: [STRING].
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
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.
日志说明	用户MAC地址认证失败
处理建议	查看失败原因并修改相关配置

70.3 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.
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
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.
日志说明	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
处理建议	查看失败原因并修改相关配置；关闭EAD快速部署功能或删除当前接口上的802.1X配置

70.4 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.
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
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.
日志说明	MAC地址认证成功
处理建议	无

70.5 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.
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
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.
日志说明	MAC地址认证失败但通过开放认证模式成功上线
处理建议	无

70.6 MACA_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; MAC authentication user was logged off.
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
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.
日志说明	MAC地址认证用户下线
处理建议	查看下线原因或进行后续操作

70.7 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.
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
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.
日志说明	MAC地址认证open用户下线
处理建议	查看下线原因或进行后续操作

71 MACSEC

本节介绍 MAC Security 模块输出的日志信息。

71.1 MACSEC_MKA_KEEPALIVE_TIMEOUT

日志内容	The live peer with SCI [STRING] and CKN [STRING] aged out on interface [STRING].
参数解释	$1：SCI $2：CKN $3：接口名
日志等级	4
举例	MACSEC/4/MACSEC_MKA_KEEPALIVE_TIMEOUT: The live peer with SCI 00E00100000A0006 and CKN 80A0EA0CB03D aged out on interface GigabitEthernet1/0/1.
日志说明	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	检查本端参与者和对端参与者所在链路是否故障，如果链路故障，则请恢复链路

71.2 MACSEC_MKA_PRINCIPAL_ACTOR

日志内容	The actor with CKN [STRING] became principal actor on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_PRINCIPAL_ACTOR: The actor with CKN 80A0EA0CB03D became principal actor on interface GigabitEthernet1/0/1.
日志说明	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

71.3 MACSEC_MKA_SAK_REFRESH

日志内容	The SAK has been refreshed on interface [STRING].
参数解释	$1：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SAK_REFRESH: The SAK has been refreshed on interface GigabitEthernet1/0/1.
日志说明	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

71.4 MACSEC_MKA_SESSION_REAUTH

日志内容	The MKA session with CKN [STRING] was re-authenticated on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SESSION_REAUTH: The MKA session with CKN 80A0EA0CB03D was re-authenticated on interface GigabitEthernet1/0/1.
日志说明	接口进行802.1X重认证时，触发该日志。重认证过程中，参与者接收到新的CAK，并使用它重建会话
处理建议	无

71.5 MACSEC_MKA_SESSION_SECURED

日志内容	The MKA session with CKN [STRING] was secured on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SESSION_SECURED: The MKA session with CKN 80A020EA0CB03D was secured on interface GigabitEthernet1/0/1.
日志说明	接口上的MKA会话采用密文通信方式。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

71.6 MACSEC_MKA_SESSION_START

日志内容	The MKA session with CKN [STRING] started on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SESSION_START: The MKA session with CKN 80A020EA0CB03D started on interface GigabitEthernet1/0/1.
日志说明	MKA会话协商开始。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

71.7 MACSEC_MKA_SESSION_STOP

日志内容	The MKA session with CKN [STRING] stopped on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	5
举例	MACSEC/5/MACSEC_MKA_SESSION_STOP: The MKA session with CKN 80A020EA0CB03D stopped on interface GigabitEthernet1/0/1.
日志说明	MKA会话终止。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	使用**display mka session**命令查看会话是否存在。如果会话不存在且不是用户删除的，则需要检查会话所在链路是否故障。如果链路故障，则请恢复链路

71.8 MACSEC_MKA_SESSION_UNSECURED

日志内容	The MKA session with CKN [STRING] was not secured on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	5
举例	MACSEC/5/MACSEC_MKA_SESSION_UNSECURED: The MKA session with CKN 80A020EA0CB03D was not secured on interface GigabitEthernet1/0/1.
日志说明	接口上的MKA会话采用明文通信方式。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

72 MBFD

本节介绍 MPLS BFD 模块输出的日志信息。

72.1 MBFD_TRACEROUTE_FAILURE

日志内容	[STRING] is failed. ([STRING].)
参数解释	$1：LSP信息 $2：LSP失败原因
日志等级	5
举例	MBFD/5/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.)
日志说明	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LSP或者MPLS TE隧道出现了故障
处理建议	检查LSP或者MPLS TE隧道的配置情况

73 MBUF

本节介绍 MBUF 模块输出的日志信息。

73.1 MBUF_DATA_BLOCK_CREATE_FAIL

日志内容	Failed to create an MBUF data block because of insufficient memory. Failure count: [UINT32].
参数解释	$1：失败次数
日志等级	2
举例	MBUF/2/MBUF_DATA_BLOCK_CREATE_FAIL: Failed to create an MBUF data block because of insufficient memory. Failure count: 128.
日志说明	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	**90.** 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
	91. 在系统视图下执行 **display memory** 命令查询系统内存总量
	92. 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
	  ○ 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
	  ○ 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

74 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。

74.1 MDC_CREATE

日志内容	MDC [UINT16] was created.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE: MDC 2 was created.
日志说明	MDC成功创建
处理建议	无

74.2 MDC_CREATE_ERR

日志内容	Failed to create MDC [UINT16] for insufficient resources.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE_ERR: -Slot=1; Failed to create MDC 2 for insufficient resources.
日志说明	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	**93.** 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 **94.** 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 **95.** 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

74.3 MDC_DELETE

日志内容	MDC [UINT16] was deleted.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_DELETE: MDC 2 was deleted.
日志说明	MDC成功删除
处理建议	无

74.4 MDC_KERNEL_EVENT_TOOLONG

日志内容	[STRING] [UINT16] kernel event in sequence [STRING] function [STRING] failed to finish within [UINT32] minutes.
参数解释	$1：取值为MDC或Context $2：MDC或Context的编号 $3：内核事件的阶段 $4：内核事件阶段对应的函数的地址 $5：所用时间
日志等级	4
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.
日志说明	某内核事件在长时间内未完成
处理建议	**96.** 重启单板，尝试恢复 **97.** 联系工程师分析解决

74.5 MDC_LICENSE_EXPIRE

日志内容	The MDC feature's license will expire in [UINT32] days.
参数解释	$1：天数，取值范围为1到30天
日志等级	5
举例	MDC/5/MDC_LICENSE_EXPIRE: The MDC feature’s license will expire in 5 days.
日志说明	MDC License将在指定天数后失效
处理建议	安装新的License

74.6 MDC_NO_FORMAL_LICENSE

日志内容	The feature MDC has no formal license.
参数解释	无
日志等级	5
举例	MDC/5/MDC_NO_FORMAL_LICENSE: The feature MDC has no formal license.
日志说明	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	安装正式MDC License

74.7 MDC_NO_LICENSE_EXIT

日志内容	The MDC feature is being disabled, because it has no license.
参数解释	无
日志等级	5
举例	MDC/5/MDC_NO_LICENSE_EXIT: The MDC feature is being disabled, because it has no license.
日志说明	MDC特性被禁用，因为MDC License过期或者被卸载了
处理建议	安装MDC License

74.8 MDC_OFFLINE

日志内容	MDC [UINT16] is offline now.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_OFFLINE: MDC 2 is offline now.
日志说明	MDC停用了
处理建议	无

74.9 MDC_ONLINE

日志内容	MDC [UINT16] is online now.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_ONLINE: MDC 2 is online now.
日志说明	MDC启用了
处理建议	无

74.10 MDC_STATE_CHANGE

日志内容	MDC [UINT16] status changed to [STRING].
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
举例	MDC/5/MDC_STATE_CHANGE: MDC 2 state changed to active.
日志说明	MDC状态发生了变化
处理建议	无

75 MFIB

本节介绍组播转发模块输出的日志信息。

75.1 MFIB_MEM_ALERT

日志内容	MFIB process received system memory alert [STRING] event.
参数解释	$1：内存告警事件类型
日志等级	5
举例	MFIB/5/MFIB_MEM_ALERT: MFIB process receive system memory alert start event.
日志说明	MFIB模块收到了系统发出的内存告警事件
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

76 MGROUP

本节主要介绍与镜像组相关的日志消息。

76.1 MGROUP_APPLY_SAMPLER_FAIL

日志内容	Failed to apply the sampler for mirroring group [UINT16], because the sampler resources are insufficient.
参数解释	$1：镜像组编号
日志等级	3
举例	MGROUP/3/MGROUP_APPLY_SAMPLER_FAIL: Failed to apply the sampler for mirroring group 1, because the sampler resources are insufficient.
日志说明	采样器资源不足时，新镜像组引用采样器失败
处理建议	无

76.2 MGROUP_RESTORE_CPUCFG_FAIL

日志内容	Failed to restore configuration for mirroring CPU of [STRING] in mirroring group [UINT16], because [STRING]
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
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.
日志说明	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，如果是由于系统不支持变化的配置，删除不支持的配置，重新配置镜像组的源CPU

76.3 MGROUP_RESTORE_GROUP_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16], because [STRING]
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
举例	MGROUP/3/MGROUP_RESTORE_GROUP_FAIL: Failed to restore configuration for mirroring group 1, because monitor resources are insufficient.
日志说明	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	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。请删除不需要的镜像配置释放资源，然后重新配置恢复失败的镜像组

76.4 MGROUP_RESTORE_IFCFG_FAIL

日志内容	Failed to restore configuration for interface [STRING] in mirroring group [UINT16], because [STRING]
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
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.
日志说明	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，如果是由于系统不支持变化的配置，删除不支持的配置，重新配置镜像组的源端口

76.5 MGROUP_SYNC_CFG_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16] in [STRING], because [STRING]
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
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.
日志说明	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	删除配置恢复失败的镜像组

77 MPLS

本节介绍 MPLS 模块输出的日志信息。

77.1 MPLS_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for MPLS.
参数解释	无
日志等级	4
举例	MPLS/4/MPLS_HARD_RESOURCE_NOENOUGH: No enough hardware resource for MPLS.
日志说明	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，是则配置获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

77.2 MPLS_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for MPLS are restored.
参数解释	无
日志等级	6
举例	MPLS/6/MPLS_HARD_RESOURCE_RESTORE: Hardware resources for MPLS are restored.
日志说明	MPLS硬件资源恢复
处理建议	无

78 MTLK

本节介绍 Monitor Link 模块输出的日志信息。

78.1 MTLK_UPLINK_STATUS_CHANGE

日志内容	The uplink of monitor link group [UINT32] is [STRING].
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
举例	MTLK/6/MTLK_UPLINK_STATUS_CHANGE: The uplink of monitor link group 1 is up.
日志说明	Monitor Link组上行链路up或down
处理建议	检查故障链路

79 NAT

本节介绍 NAT 模块输出的日志信息。

79.1 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.
参数解释	$1：接口名称
日志等级	4
举例	NAT/4/NAT_ADDR_BIND_CONFLICT: Failed to activate NAT configuration on interface Ethernet0/0/2, because global IP addresses already bound to another service card.
日志说明	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	如果有多个接口引用了相同的外网地址，则这些接口必须指定同一块业务板进行NAT处理。请使用**display nat all**命令检查配置，并修改配置使引用相同外网地址的接口绑定相同的业务板。另外，由于该绑定冲突，失效配置需要先删除，再重新进行配置

79.2 NAT_FAILED_ADD_FLOW_RULE

日志内容	Failed to add flow-table due to: [STRING].
参数解释	$1：失败原因
日志等级	4
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.
日志说明	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	请联系技术支持

79.3 NAT_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	$1：失败原因
日志等级	4
举例	NAT/4/NAT_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足、NAT配置地址存在重叠等
处理建议	对于硬件资源不足情况，请联系技术支持 对于NAT配置地址存在重叠情况，请尽量避免出现部分地址重叠，如果不可避免，请将重叠部分地址和不重叠地址分开，单独配置

79.4 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];
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 $21：日志类型描述信息，包括： • Session created：NAT 会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
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;

日志说明	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

79.5 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.
参数解释	无
日志等级	4
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.
日志说明	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	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。请修改相应接口的NAT服务器配置

79.6 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].
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
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.
日志说明	恢复接口绑定业务板配置失败时触发该日志
处理建议	• 如果提示 NAT 地址已经绑定到其他业务板，则使用 display nat all 检查配置，并修改配置使引用相同外网地址的接口绑定相同的业务板 • 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

80 ND

本节介绍 ND 模块输出的日志信息。

80.1 ND_COMMONPROXY_ENABLE_FAILED

日志内容	Failed to enable common ND proxy on interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	ND/4/ND_COMMONPROXY_ENABLE_FAILED: -MDC=1-Slot=2; Failed to enable common ND proxy on interface Vlan-interface 1.
日志说明	接口下开启普通ND代理失败。如果非主控板的接口下开启普通ND代理失败，则在对应的接口板上打印该日志信息
处理建议	• 检查设备相应单板是否支持本功能 • 确认设备的硬件资源是否充足

80.2 ND_CONFLICT

日志内容	[STRING] is inconsistent.
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
举例	ND/6/ND_CONFLICT: PREFIX VALID TIME is inconsistent.
日志说明	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	检查并保证设备与邻居路由器上的配置一致

80.3 ND_DUPADDR

日志内容	Duplicate address: [STRING] on the interface [STRING].
参数解释	$1：将要分配的IPv6地址 $2：接口名称
日志等级	6
举例	ND/6/ND_DUPADDR: Duplicate address: 33::8 on interface Vlan-interface9.
日志说明	分配给该接口的地址已经被其他设备使用
处理建议	分配一个新的IPv6地址

80.4 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].
参数解释	$1：IPv6地址 $2：接口名 $3：接口名
日志等级	4
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.
日志说明	分配给该接口的地址已经被其他设备使用
处理建议	分配一个新的IPv6地址。如果非法，需要断开该主机网络

80.5 ND_LOCALPROXY_ENABLE_FAILED

日志内容	Failed to enable local ND proxy on interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	ND/4/ND_LOCALPROXY_ENABLE_FAILED: -MDC=1-Slot=2; Failed to enable local ND proxy on interface Vlan-interface 1.
日志说明	接口下开启本地ND代理失败。如果非主控板的接口下开启本地ND代理失败，则在对应的接口板上打印该日志信息
处理建议	• 检查设备相应单板是否支持本功能 • 确认设备的硬件资源是否充足

80.6 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].
参数解释	$1：接收ND报文的接口名 $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
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.
日志说明	**ipv6 nd mac-check enable**命令用来在网关设备上开启ND协议报文源MAC地址一致性检查功能。在网关开启此功能后，会对接收的ND协议报文进行检查，如果ND协议报文中的源MAC地址和源链路层选项地址中的MAC地址不同，则丢弃该报文。若使用**ipv6 nd check log enable**命令来开启ND日志信息功能，会有相关的log信息输出
处理建议	检查链路层源MAC对应主机的合法性

80.7 ND_NETWORKROUTE_DUPLICATE

日志内容	Prefix [STRING] of the IPv6 ND network route matches different ports: [STRING] and [STRING].
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
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.
日志说明	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	检查网络配置，根据实际需求修改网络配置

80.8 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.
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
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.
日志说明	RA Guard检测到攻击，丢弃相应的报文并提示日志信息
处理建议	检查报文源是否合法

80.9 ND_SET_PORT_TRUST_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	6
举例	ND/6/ND_SET_PORT_TRUST_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发端口规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

80.10 ND_SET_VLAN_REDIRECT_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	6
举例	ND/6/ND_VLAN_REDIRECT_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发VLAN规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

80.11 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.
参数解释	无
日志等级	4
举例	ND/4/ND_SNOOPING_LEARN_ALARM: -MDC=1; The total number of ND snooping entries learned in all VLANs reached or exceeded the alarm threshold.
日志说明	所有VLAN学习的总的ND Snooping表项数达到或超过告警阈值
处理建议	检查是否有ND攻击

80.12 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.
参数解释	无
日志等级	4
举例	ND/4/ND_SNOOPING_LEARN_ALARM_RECOVER: -MDC=1; The total number of ND snooping entries learned in all VLANs dropped below the alarm threshold.
日志说明	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

80.13 ND_USER_DUPLICATE_IPV6ADDR

日志内容	Detected a user IPv6 address conflict. New user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) connecting to interface [STRING] and old user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) connecting to interface [STRING] were using the same IPv6 address [IPV6ADDR].
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
举例	ND/6/ND_USER_DUPLICATE_IPV6ADDR: Detected a user IPv6 address conflict. New user (MAC 0010-2100-01e1, SVLAN 100, CVLAN 10) connecting to interface GigabitEthernet1/0/1 and old user (MAC 0120-1e00-0102, SVLAN 100, CVLAN 10) connecting to interface GigabitEthernet1/0/1 were using the same IPv6 address 10::1.
日志说明	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	排查所有终端用户的IPv6地址，解决IPv6地址冲突问题

80.14 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].
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
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.
日志说明	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，如果设备检测到终端用户在接口间迁移，则输出本日志
处理建议	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

80.15 ND_USER_OFFLINE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) was offline from interface [STRING].
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
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.
日志说明	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，如果设备检测到终端用户下线，则输出本日志
处理建议	无需处理

80.16 ND_USER_ONLINE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) was online on interface [STRING].
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
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.
日志说明	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，如果设备检测到终端用户上线，则输出本日志
处理建议	检查上线用户是否是合法用户

81 NETCONF

本节介绍 NETCONF 模块输出的日志信息。

81.1 CLI

日志内容	User ([STRING], [STRING][STRING]) performed an CLI operation: [STRING] operation result=[STRING][STRING]
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
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.
日志说明	CLI配置执行完毕后，输出CLI的执行结果
处理建议	无

81.2 EDIT-CONFIG

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].
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
举例	XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20, session ID 1), message ID=1, operation=create Ifmgr/Interfaces (IfIndex="GigabitEthernet1/0/1"), result=Succeeded. Attributes: Description="This is Desc1", AdminDown=1, Speed=1.
日志说明	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操作支持输入该日志
处理建议	无

81.3 NETCONF_MSG_DEL

日志内容	A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
参数解释	无
日志等级	7
举例	NETCONF/7/NETCONF_MSG_DEL: A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
日志说明	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	**98.** 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 **99.** 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，建议联系技术支持

81.4 THREAD

日志内容	Maximum number of NETCONF threads already reached.
参数解释	无
日志等级	3
举例	XMLCFG/3/THREAD: -MDC=1; Maximum number of NETCONF threads already reached.
日志说明	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

82 NQA

本节介绍 NQA 模块输出的日志信息。

82.1 NQA_LOG_UNREACHABLE

日志内容	Server [STRING] unreachable.
参数解释	$1：NQA服务器的IP地址
日志等级	6
举例	NQA/6/NQA_LOG_UNREACHABLE: Server 192.168.30.117 unreachable.
日志说明	NQA客户端检测到NQA服务器不可达
处理建议	检查网络环境

83 NTP

本节介绍 NTP 模块输出的日志信息。

83.1 NTP_CLOCK_CHANGE

日志内容	System clock changed from [STRING] to [STRING], the NTP server's IP address is [STRING].
参数解释	$1：起始时间 $2：同步后时间 $3：IP地址
日志等级	5
举例	NTP/5/NTP_CLOCK_CHANGE: System clock changed from 02:12:58:345 12/28/2012 to 02:29:12:879 12/28/2012, the NTP server's IP address is 192.168.30.116.
日志说明	NTP客户端的时间已经和NTP服务器同步
处理建议	无

83.2 NTP_LEAP_CHANGE

日志内容	System Leap Indicator changed from [UINT32] to [UINT32] after clock update.
参数解释	$1：起始闰秒标识 $2：当前闰秒标识
日志等级	5
举例	NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 00 to 01 after clock update.
日志说明	• 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 • 系统的闰秒标识会发生变化。例如，NTP 状态会从未同步状态变为已同步状态
处理建议	无

83.3 NTP_SOURCE_CHANGE

日志内容	NTP server's IP address changed from [STRING] to [STRING].
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
举例	NTP/5/NTP_SOURCE_CHANGE: NTP server's IP address changed from 1.1.1.1 to 1.1.1.2.
日志说明	系统改变了时钟源
处理建议	无

83.4 NTP_SOURCE_LOST

日志内容	Lost synchronization with NTP server with IP address [STRING].
参数解释	$1：IP 地址
日志等级	5
举例	NTP/5/NTP_SOURCE_LOST: Lost synchronization with NTP server with IP address 1.1.1.1.
日志说明	NTP交互中的时钟源处于未同步状态或不可达
处理建议	**100.** 检查 NTP 服务器及网络连接 **101.** 若 NTP 服务器故障，请在客户端配置新的服务器作为时钟源

83.5 NTP_STRATUM_CHANGE

日志内容	System stratum changed from [UINT32] to [UINT32] after clock update.
参数解释	$1：起始层 $2：当前层
日志等级	5
举例	NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 6 to 5 after clock update.
日志说明	系统的层数已发生变化
处理建议	无

84 OAP

本节介绍 OAP 模块输出的日志信息。

84.1 OAP_CLIENT_DEREG

日志内容	OAP client [UINT32] on interface [STRING] deregistered.
参数解释	$1：Client ID $2：接口名称
日志等级	5
举例	OAP/5/OAP_CLIENT_DEREG: OAP client 1 on interface GigabitEthernet1/0/24 deregistered.
日志说明	接口上承载的OAP client已取消注册
处理建议	检查OAP client的登录信息

84.2 OAP_CLIENT_TIMEOUT

日志内容	OAP client [UINT32] on interface [STRING] timed out.
参数解释	$1：Client ID $2：接口名称
日志等级	4
举例	OAP/4/OAP_CLIENT_TIMEOUT: OAP client 1 on interface GigabitEthernet1/0/24 timed out.
日志说明	接口上承载的OAP client超时
处理建议	检查故障链路

85 OBJP

本节介绍 OBJP（对象策略）模块输出的日志信息。

85.1 OBJP_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] object-policy [STRING]. The resources are insufficient.
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_NO_RES: Failed to accelerate IPv6 object-policy a. The resources are insufficient.
日志说明	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

85.2 OBJP_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] object-policy [STRING]. Object-policy acceleration is not supported.
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 object-policy a. The operation is not supported.
日志说明	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

85.3 OBJP_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] object-policy [STRING].
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 object-policy a.
日志说明	因系统故障导致对象策略加速失败
处理建议	无

86 OFP

本节介绍 OpenFlow 模块输出的日志信息。

86.1 OFP_ACTIVE

日志内容	Activate openflow instance [UINT16]
参数解释	$1：实例ID
日志等级	5
举例	OFP/5/OFP_ACTIVE: Activate openflow instance 1.
日志说明	收到激活OpenFlow实例的命令
处理建议	无

86.2 OFP_ACTIVE_FAILED

日志内容	Failed to activate instance [UINT16].
参数解释	$1：实例ID
日志等级	4
举例	OFP/4/OFP_ACTIVE_FAILED: Failed to activate instance 1.
日志说明	激活OpenFlow实例失败
处理建议	无

86.3 OFP_CONNECT

日志内容	Openflow instance [UINT16], controller [CHAR] is [STRING].
参数解释	$1：实例ID $2：控制器ID $3：连接状态，显示为connected或disconnected
日志等级	5
举例	OFP/5/OFP_CONNECT: Openflow instance 1, controller 0 is connected.
日志说明	控制器连接状态变化
处理建议	无

86.4 OFP_FAIL_OPEN

日志内容	Openflow instance [UINT16] is in fail [STRING] mode.
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
举例	OFP/5/OFP_FAIL_OPEN: Openflow instance 1 is in fail secure mode.
日志说明	实例激活后无法连接控制器或者从所有控制器断开，显示连接中断模式
处理建议	无

86.5 OFP_FAIL_OPEN_FAILED

日志内容	OpenFlow instance [UINT16]: [STRING] fail-open mode configuration failed and the secure mode is restored.
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
举例	OFP/4/OFP_FAIL_OPEN_FAILED: OpenFlow instance 1: standalone fail-open mode configuration failed and the secure mode is restored.
日志说明	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	请联系技术支持

86.6 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].
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
举例	OFP/5/OFP_FLOW_ADD: Openflow instance 1 controller 0: add flow entry 1, xid 0x1, cookie 0x0, table id 0.
日志说明	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

86.7 OFP_FLOW_ADD_ARP_FAILED

日志内容	Failed to add OpenFlow ARP entry: IPAddr=[STRING], OutIfIndex=[UINT32], MACAddr=[STRING].
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
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.
日志说明	OpenFlow ARP表项添加失败
处理建议	请联系技术支持

86.8 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].
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
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.
日志说明	表项重复添加
处理建议	无

86.9 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.
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
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.
日志说明	由于资源不足，添加流表项失败
处理建议	请联系技术支持

86.10 OFP_FLOW_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32], table id [CHAR].
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
举例	OFP/4/OFP_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry 1, table id 0.
日志说明	添加流表项失败
处理建议	请联系技术支持

86.11 OFP_FLOW_ADD_ND_FAILED

日志内容	Failed to add OpenFlow ND entry: IPv6Addr=[STRING], OutIfIndex=[UINT32], MACAddr=[STRING].
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
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.
日志说明	OpenFlow ND表项添加失败
处理建议	请联系技术支持

86.12 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].
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
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.
日志说明	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

86.13 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].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
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.
日志说明	添加miss规则失败
处理建议	无

86.14 OFP_FLOW_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
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
举例	OFP/5/OFP_FLOW_DEL: Openflow instance 1 controller 0: delete flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	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

86.15 OFP_FLOW_DEL_L2VPN_DISABLE

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because L2VPN was disabled.
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
举例	OFP/5/OFP_FLOW_DEL_L2VPN_DISABLE: 2 flow entries in table 1 of instance 1 were deleted because L2VPN was disabled.
日志说明	L2VPN功能关闭导致多个流表项被删除
处理建议	无

86.16 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].
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
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.
日志说明	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

86.17 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].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
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.
日志说明	删除miss规则失败
处理建议	无

86.18 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.
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
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.
日志说明	VXLAN隧道被删除导致多个流表项被删除
处理建议	无

86.19 OFP_FLOW_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
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
举例	OFP/5/OFP_FLOW_MOD: Openflow instance 1 controller 0: modify flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	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

86.20 OFP_FLOW_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_MOD_FAILED: Openflow instance 1 controller 0: failed to modify flow entry, table id 0.
日志说明	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

86.21 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].
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
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.
日志说明	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

86.22 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].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
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.
日志说明	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

86.23 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.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
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.
日志说明	Group删除导致的表项删除
处理建议	无

86.24 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.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
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.
日志说明	Hard-time超时导致的表项删除
处理建议	无

86.25 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.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
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.
日志说明	Idle-time超时导致的表项删除
处理建议	无

86.26 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.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance1 was deleted with a meter_mod message.
日志说明	Meter删除导致的表项删除
处理建议	无

86.27 OFP_FLOW_UPDATE_FAILED

日志内容	OpenFlow instance [UINT16] table [CHAR]: failed to update or synchronize flow entry [UINT32].
参数解释	$1：实例ID $2：流表ID $3：流表项ID
日志等级	4
举例	OFP/4/OFP_FLOW_SMOOTH_FAILED: OpenFlow instance 1 table 0: failed to update or synchronize flow entry 10000.
日志说明	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

86.28 OFP_GROUP_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add group [STRING], xid 0x[HEX].
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
举例	OFP/5/OFP_GROUP_ADD: Openflow instance 1 controller 0: add group 1, xid 0x1.
日志说明	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

86.29 OFP_GROUP_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add group [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_ADD_FAILED: Openflow Instance 1 controller 0: failed to add group 1.
日志说明	添加group表项失败
处理建议	请联系技术支持

86.30 OFP_GROUP_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete group [STRING], xid [HEX].
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
举例	OFP/5/OFP_GROUP_DEL: Openflow instance 1 controller 0: delete group 1, xid 0x1.
日志说明	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

86.31 OFP_GROUP_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify group [STRING], xid 0x[HEX].
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
举例	OFP/5/OFP_GROUP_MOD: Openflow instance 1 controller 0: modify group 1, xid 0x1.
日志说明	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

86.32 OFP_GROUP_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify group [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_MOD_FAILED: Openflow instance 1 controller 0: failed to modify group 1.
日志说明	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

86.33 OFP_GROUP_REFRESH_FAILED

日志内容	Openflow instance [STRING]:Failed to refresh group [STRING].
参数解释	$1：实例ID $2：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_REFRESH_FAILED: Openflow instance 1:Failed to refresh group 1.
日志说明	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	请联系技术支持

86.34 OFP_GROUP_ROLLBACK_FAILED

日志内容	Openflow instance [STRING]:Failed to roll back group [STRING].
参数解释	$1：实例ID $2：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_ROLLBACK_FAILED: Openflow instance 1:Failed to roll back group 1.
日志说明	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	请联系技术支持

86.35 OFP_METER_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add meter [STRING], xid 0x[HEX].
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
举例	OFP/5/OFP_METER_ADD: Openflow instance 1 controller 0: add meter 1, xid 0x1.
日志说明	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

86.36 OFP_METER_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add meter [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4
举例	OFP/4/OFP_METER_ADD_FAILED: Openflow Instance 1 controller 0: failed to add meter 1.
日志说明	添加meter表项失败
处理建议	请联系技术支持

86.37 OFP_METER_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete meter [STRING], xid 0x[HEX].
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
举例	OFP/5/OFP_METER_DEL: Openflow instance 1 controller 0: delete meter 1, xid 0x1.
日志说明	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

86.38 OFP_METER_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify meter [STRING], xid 0x[HEX].
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
举例	OFP/5/OFP_METER_MOD: Openflow Instance 1 controller 0: modify meter 1, xid 0x1.
日志说明	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

86.39 OFP_METER_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify meter [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4
举例	OFP/4/OFP_METER_MOD_FAILED: Openflow instance 1 controller 0: failed to modify meter 1.
日志说明	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

86.40 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.
参数解释	$1：流表ID $2：实例ID
日志等级	5
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.
日志说明	Group删除导致的table-miss表项删除
处理建议	无

86.41 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.
参数解释	$1：流表ID $2：实例ID
日志等级	5
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.
日志说明	Hard-time超时导致的table-miss表项删除
处理建议	无

86.42 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.
参数解释	$1：流表ID $2：实例ID
日志等级	5
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.
日志说明	Idle-time超时导致的table-miss表项删除
处理建议	无

86.43 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.
参数解释	$1：流表ID $2：实例ID
日志等级	5
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.
日志说明	Meter删除导致的table-miss表项删除
处理建议	无

86.44 PORT_MOD

日志内容	Port modified. InstanceID =[UINT16], IfIndex =[UINT32], PortDown=[STRING], NoRecv=[STRING], NoFwd=[STRING], NoPktIn=[STRING], Speed=[STRING], Duplex=[STRING].
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
举例	OFP/5/PORT_MOD: Port modified. InstanceID =1, IfIndex =2, PortDown=True, NoRecv=NoChange, NoFwd=NoChange, NoPktIn=NoChange, Speed=, Duplex=.
日志说明	控制器修改了OpenFlow实例中的接口
处理建议	无

86.45 OFP_RADARDETECTION

日志内容	inIfIndex = [UINT32], packageId = [UINT16], innerTTL = [CHAR], outerTTL = [CHAR].
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
举例	OFP/5/OFP_RADARDETECTION: inIfIndex = 1, packageId = 1, innerTTL = 128, outerTTL = 128.
日志说明	收到用于雷达探测或VM仿真功能的报文
处理建议	无

87 OPENSRC（FreeRADIUS）

本节介绍 OPENSRC 模块输出的开源软件 FreeRADIUS 日志信息。

87.1 HUP事件

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
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，详见表87-1
日志等级	6
举例	OPENSRC/6/SYSLOG: Jan 1 01:14:04 radiusd[427]: Received HUP sign
日志说明	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；收到此HUP信号间隔小于5秒，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，详见表87-1

表87-1 HUP 事件的详细说明列表

HUP 事件	说明	处理建议
Received HUP sign	收到HUP信号	不需要处理
Module: Reloaded module "files"	重新加载模块配置文件	不需要处理
HUP - Files loaded by a module have changed.	收到HUP信号，完成配置文件加载	不需要处理
Ignoring HUP (less than 5s since last one)	收到此HUP信号间隔小于5秒，忽略	如果希望5秒内配置的新用户生效，执行激活命令 **radius-server activate**

87.2 进程重启

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
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
日志等级	6
举例	OPENSRC/6/SYSLOG: Jan 1 02:00:02 radiusd[427]: Signalled to terminate
日志说明	终结当前进程并重新启动
处理建议	请根据进程重启事件的详细说明选择相应的处理方式，详见表87-2

表87-2 进程重启事件的详细说明列表（日志等级为 6）

进程重启事件	说明	处理建议
Signalled to terminate	收到终结进程信号	不需要处理
Exiting normally	进程关闭	不需要处理
Debugger not attached	进程对应的调试信息开关处于关闭状态	不需要处理
Loaded virtual server <default>	加载虚拟服务器	不需要处理
Loaded virtual server inner-tunnel	加载虚拟服务器内部通道	不需要处理
Loaded virtual server default	加载虚拟服务器默认配置	不需要处理
Ready to process requests	准备开始处理认证报文	不需要处理

87.3 进程启动

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
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
日志等级	4
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".
日志说明	进程启动时，系统加载默认检查项
处理建议	请根据进程启动的详细说明选择相应的处理方式，详见表87-3

表87-3 进程启动的详细说明列表（日志等级为 4）

进程启动事件	说明	处理建议
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	不需要处理
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	不需要处理
Ignoring "sql" (see raddb/mods-available/README.rst)	忽略SQL处理	不需要处理
Ignoring "ldap" (see raddb/mods-available/README.rst)	忽略LDAP处理	不需要处理

87.4 用户认证

日志内容	[DATE] [TIME] radiusd[UINT32]: ([UINT32]) [STRING]: [[STRING]] (from client [IPADDR] port [UINT32] cli [MAC])
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 $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
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)
日志说明	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，详见表87-4

表87-4 认证结果的详细说明列表

认证结果	说明	处理建议
Login OK	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**

认证结果	说明	处理建议
		authentication 命令配置 ○ 服务器端共享密钥通过 **radius-server client ip** 命令配置
Login incorrect (pap: Cleartext password does not match "known good" password)	PAP认证密码错误	用户重新输入正确的密码
Login incorrect (chap: Password comparison failed: password is incorrect)	CHAP认证密码错误	用户重新输入正确的密码
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	• 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
Login incorrect (chap: &control:Cleartext-Password is required for authentication)	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）
Invalid user (expiration: Account expired at 'Jan 1 2013 02:19:00 UTC')	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])
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
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)
日志说明	不支持Login类型的用户认证
处理建议	不需要处理

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
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
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
日志说明	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

88 OPTMOD

本节介绍 OPTMOD 模块输出的日志信息。

88.1 BIAS_HIGH

日志内容	[STRING]: Bias current is high.
参数解释	$1：端口类型和编号
日志等级	2
举例	OPTMOD/2/BIAS_HIGH: GigabitEthernet1/0/1: Bias current is high.
日志说明	光模块的偏置电流超过上限
处理建议	**102.** **display transceive diagnosis interface** 命令查看当前偏置电流值是否已经超过高告警门限 **103.** **display transceive alarm interface** 命令查看当前是否确实有偏置电流值高的告警 **104.** 如果确实超过门限了，模块有问题，更换模块

88.2 BIAS_LOW

日志内容	[STRING]: Bias current is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/BIAS_LOW: GigabitEthernet1/0/1: Bias current is low.
日志说明	光模块的偏置电流低于下限
处理建议	**105.** **display transceive diagnosis interface** 命令查看当前偏置电流值是否已经超过低告警门限 **106.** **display transceive alarm interface** 命令查看当前是否确实有偏置电流高的告警 **107.** 如果低于低告警门限，模块有问题，更换模块

88.3 BIAS_NORMAL

日志内容	[STRING]: Bias current is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/BIAS_NORMAL: GigabitEthernet1/0/1: Bias current is normal.
日志说明	光模块的偏置电流恢复至正常范围
处理建议	无

88.4 CFG_ERR

日志内容	[STRING]: Transceiver type and port configuration mismatched.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/CFG_ERR: GigabitEthernet1/0/1: Transceiver type and port configuration mismatched.
日志说明	光模块类型与端口配置不匹配
处理建议	检查端口当前配置与光模块类型，如果确实不匹配，则更换匹配模块，或更新配置

88.5 CHKSUM_ERR

日志内容	[STRING]: Transceiver information checksum error.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/CHKSUM_ERR: GigabitEthernet1/0/1: Transceiver information checksum error .
日志说明	光模块寄存器信息校验失败
处理建议	更换光模块，或联系工程师解决

88.6 FIBER_SFPMODULE_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.
参数解释	$1：端口类型和编号 $2：光模块失效天数
日志等级	4
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.
日志说明	光模块与接口卡不匹配
处理建议	更换光模块

88.7 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.
参数解释	$1：端口类型和编号
日志等级	4
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.
日志说明	不支持该光模块
处理建议	更换光模块

88.8 IO_ERR

日志内容	[STRING]: The transceiver information I/O failed.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/IO_ERR: GigabitEthernet1/0/1: The transceiver information I/O failed.
日志说明	设备读取光模块寄存器信息失败
处理建议	执行**display transceive diagnosis interface**或者**display transceive alarm interface**命令，如果都显示fail，则表示光模块故障，请更换

88.9 MOD_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：故障类型
日志等级	5
举例	OPTMOD/5/MOD_ALM_OFF: GigabitEthernet1/0/1: Module_not_ready was removed.
日志说明	光模块的某故障被清除
处理建议	无

88.10 MOD_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：故障类型
日志等级	5
举例	OPTMOD/5/MOD_ALM_ON: GigabitEthernet1/0/1: Module_not_ready wasdetected.
日志说明	检测到光模块一故障
处理建议	执行**display transceive alarm interface**命令，如果仍然显示Module not ready，则表示光模块有问题，请更换

88.11 MODULE_IN

日志内容	[STRING]: The transceiver is [STRING].
参数解释	$1：端口类型和编号 $2：光模块类型
日志等级	4
举例	OPTMOD/4/MODULE_IN: GigabitEthernet1/0/1: The transceiver is 1000_BASE_T_AN_SFP.
日志说明	光模块类型。当一光模块插入某端口时，设备生成此日志信息
处理建议	无

88.12 MODULE_OUT

日志内容	[STRING]: Transceiver absent.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/MODULE_OUT: GigabitEthernet1/0/1: The transceiver is absent.
日志说明	光模块被拔出
处理建议	无

88.13 PHONY_MODULE

日志内容	[STRING]: This transceiver is not sold by H3C. H3C does not guarantee the correct operation of the module or assume maintenance responsibility.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/PHONY_MODULE: GigabitEthernet1/0/1: This transceiver is not sold by H3C. H3C does not guarantee the correct operation of the module or assume maintenance responsibility.
日志说明	光模块非H3C生产
处理建议	更换光模块

88.14 RX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：RX故障类型
日志等级	5
举例	OPTMOD/5/RX_ALM_OFF: GigabitEthernet1/0/1: RX_not_ready was removed.
日志说明	光模块RX故障被清除
处理建议	无

88.15 RX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：RX故障类型
日志等级	5
举例	OPTMOD/5/RX_ALM_ON: GigabitEthernet1/0/1: RX_not_ready was detected.
日志说明	检测到光模块RX故障
处理建议	使用**display transceive alarm interface**命令可查看到这个故障，确认是模块问题，更换模块

88.16 RX_POW_HIGH

日志内容	[STRING]: RX power is high.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/RX_POW_HIGH: GigabitEthernet1/0/1: RX power is high.
日志说明	光模块RX功率超过上限
处理建议	**108.** **display transceive diagnosis interface** 命令查看功率是否已经超过高告警门限 **109.** **display transceive alarm interface** 命令查看当前是否确实有功率高的告警 **110.** 如果确实超过门限了，模块有问题，更换模块

88.17 RX_POW_LOW

日志内容	[STRING]: RX power is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/RX_POW_LOW: GigabitEthernet1/0/1: RX power is low.
日志说明	光模块RX功率低于下限
处理建议	**111.** **display transceive diagnosis interface** 命令查看功率是否已经低于低告警门限 **112.** **display transceive alarm interface** 命令查看当前是否确实有功率低告警 **113.** 如果确实低于门限了，模块有问题，更换模块

88.18 RX_POW_NORMAL

日志内容	[STRING]: RX power is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/RX_POW_NORMAL: GigabitEthernet1/0/1: RX power is normal.
日志说明	光模块RX功率恢复至正常范围
处理建议	无

88.19 TEMP_HIGH

日志内容	[STRING]: Temperature is high.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TEMP_HIGH: GigabitEthernet1/0/1: Temperature is high.
日志说明	光模块温度超过上限
处理建议	检查设备风扇是否工作正常，安装风扇或更换故障风扇 检查环境温度，如果温度确实过高就调节温度 如果设备风扇正常，且环境温度正常，则模块故障，更换模块

88.20 TEMP_LOW

日志内容	[STRING]: Temperature is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TEMP_LOW: GigabitEthernet1/0/1: Temperature is low.
日志说明	光模块温度低于下限
处理建议	检查环境温度，如果温度确实过低高就调节温度，如果环境温度正常，就是模块故障，更换模块

88.21 TEMP_NORMAL

日志内容	[STRING]: Temperature is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TEMP_NORMAL: GigabitEthernet1/0/1: Temperature is normal.
日志说明	光模块温度恢复至正常范围
处理建议	无

88.22 TX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：TX故障类型
日志等级	5
举例	OPTMOD/5/TX_ALM_OFF: GigabitEthernet1/0/1: TX_fault was removed.
日志说明	光模块TX故障被清除
处理建议	无

88.23 TX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：TX故障类型
日志等级	5
举例	OPTMOD/5/TX_ALM_ON: GigabitEthernet1/0/1: TX_fault was detected.
日志说明	检测到光模块TX故障
处理建议	使用**display transceive alarm interface**命令可查看到这个故障，确认是模块问题，更换模块

88.24 TX_POW_HIGH

日志内容	[STRING]: TX power is high.
参数解释	$1：端口类型和编号
日志等级	2
举例	OPTMOD/2/TX_POW_HIGH: GigabitEthernet1/0/1: TX power is high.
日志说明	光模块TX功率超过上限
处理建议	114. **display transceive diagnosis interface** 命令查看功率是否已经超过高告警门限 115. **display transceive alarm interface** 命令查看当前是否确实有功率高告警 116. 如果确实超过门限了，模块有问题，更换模块

88.25 TX_POW_LOW

日志内容	[STRING]: TX power is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TX_POW_LOW: GigabitEthernet1/0/1: TX power is low.
日志说明	光模块TX功率低于下限
处理建议	117. **display transceive diagnosis interface** 命令查看功率是否已经低于低告警门限 118. **display transceive alarm interface** 命令查看当前是否确实有功率低告警 119. 如果确实低于门限了，模块有问题，更换模块

88.26 TX_POW_NORMAL

日志内容	[STRING]: TX power is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TX_POW_NORMAL: GigabitEthernet1/0/1: TX power is normal.
日志说明	光模块TX功率恢复至正常范围
处理建议	无

88.27 TYPE_ERR

日志内容	[STRING]: The transceiver type is not supported by port hardware.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TYPE_ERR: GigabitEthernet1/0/1: The transceiver type is not supported by port hardware.
日志说明	端口硬件不支持光模块类型
处理建议	更换光模块

88.28 VOLT_HIGH

日志内容	[STRING]: Voltage is high.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/VOLT_HIGH: GigabitEthernet1/0/1: Voltage is high.
日志说明	光模块电压超过上限
处理建议	**120.** **display transceive diagnosis interface** 命令查看电压是否已经超过高告警门限 **121.** **display transceive alarm interface** 命令查看当前是否确实有电压高告警 **122.** 如果确实超过门限了，模块有问题，更换模块

88.29 VOLT_LOW

日志内容	[STRING]: Voltage is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/VOLT_LOW: GigabitEthernet1/0/1: Voltage is low.
日志说明	光模块电压低于下限
处理建议	**123.** **display transceive diagnosis interface** 命令查看电压是否已经超过低告警门限 **124.** **display transceive alarm interface** 命令查看当前是否确实有电压低告警 **125.** 如果确实超过门限了，模块有问题，更换模块

88.30 VOLT_NORMAL

日志内容	[STRING]: Voltage is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/VOLT_NORMAL: GigabitEthernet1/0/1: Voltage is normal!
日志说明	光模块电压恢复至正常范围
处理建议	无

89 OSPF

本节介绍 OSPF 模块输出的日志信息。

89.1 OSPF_DUP_RTRID_NBR

日志内容	OSPF [UINT16] Duplicate router ID [STRING] on interface [STRING], sourced from IP address [IPADDR].
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
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.
日志说明	检测到两台直连设备配置了相同的路由器ID
处理建议	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

89.2 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].
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
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.
日志说明	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	在确保同一OSPF区域内不存在Router ID冲突的情况下，修改IP地址配置

89.3 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]
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：原因
日志等级	6
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.
日志说明	最近一次OSPF邻居down事件
处理建议	检查OSPF邻居down事件的原因，根据具体原因进行处理： • 如果是配置相关命令导致邻居 down，如接口参数变化等，请检查配置是否正确 • 如果是超时邻居 down，检查网络状况或者配置的超时时间是否合理 • 如果是 BFD 检测导致的邻居 down，检查网络状况或者 BFD 检测时间配置是否合理 • 如果是接口状态变化导致的邻居 down，检查网络连接情况

89.4 OSPF_MEM_ALERT

日志内容	OSPF Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	OSPF/5/OSPF_MEM_ALERT: OSPF Process received system memory alert start event.
日志说明	OSPF模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存，对占用内存较多的模块进行调整，尽量释放可用内存

89.5 OSPF_NBR_CHG

日志内容	OSPF [UINT32] Neighbor [STRING] ([STRING]) changed from [STRING] to [STRING]
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
举例	OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 2.2.2.2 (Vlan-interface100) changed from Full to Down.
日志说明	接口OSPF邻接状态改变
处理建议	当某接口与邻居邻接状态从Full变为其他状态时，检查OSPF配置正确性和网络连通性

89.6 OSPF_RT_LMT

日志内容	OSPF [UINT32] route limit reached.
参数解释	$1：OSPF进程ID
日志等级	4
举例	OSPF/4/OSPF_RT_LMT: OSPF 1 route limit reached.
日志说明	OSPF进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

89.7 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.
参数解释	$1：OSPF进程ID
日志等级	5
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.
日志说明	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	使用**reset ospf process**命令使新的路由器ID生效

89.8 OSPF_RTRID_CONFLICT_INTER

日志内容	OSPF [UINT16] Received newer self-originated ase-LSAs. Possible conflict of router ID [STRING].
参数解释	$1：OSPF进程ID $2：路由器ID
日志等级	6
举例	OSPF/6/OSPF_RTRID_CONFILICT_INTER: OSPF 1 Received newer self-originated ase-LSAs. Possible conflict of router ID 11.11.11.11.
日志说明	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	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

89.9 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].
参数解释	$1：OSPF进程ID $2：路由器ID $3：OSPF区域ID
日志等级	6
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.
日志说明	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	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

89.10 OSPF_VLINKID_CHG

日志内容	OSPF [UINT32] Router ID changed, reconfigure Vlink on peer
参数解释	$1：OSPF进程ID
日志等级	5
举例	OSPF/5/OSPF_VLINKID_CHG:OSPF 1 Router ID changed, reconfigure Vlink on peer
日志说明	新的OSPF路由器ID生效。需要根据新的路由器ID检查并修改对端路由器的虚连接配置
处理建议	根据新的路由器ID检查并修改对端路由器的虚连接配置

90 OSPFV3

本节介绍 OSPFv3 模块输出的日志信息。

90.1 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].
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：原因
日志等级	6
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.
日志说明	最近一次OSPFv3邻居down事件
处理建议	检查OSPFV3邻居down事件的原因，根据具体原因进行处理： • 如果是配置相关命令导致邻居 down，如接口参数变化等，请检查配置是否正确 • 如果是超时邻居 down，检查网络状况或者配置的超时时间是否合理 • 如果是 BFD 检测导致的邻居 down，检查网络状况或者 BFD 检测时间配置是否合理 • 如果是接口状态变化导致的邻居 down，检查网络连接情况

90.2 OSPFV3_MEM_ALERT

日志内容	OSPFV3 Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	OSPFV3/5/OSPFV3_MEM_ALERT: OSPFV3 Process received system memory alert start event.
日志说明	OSPFv3模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

90.3 OSPFV3_NBR_CHG

日志内容	OSPFv3 [UINT32] Neighbor [STRING] ([STRING]) received [STRING] and its state from [STRING] to [STRING].
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
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.
日志说明	接口OSPFv3邻接状态改变
处理建议	当某接口与邻居邻接状态从Full变为其他状态时，检查OSPFv3配置正确性和网络连通性

90.4 OSPFV3_RT_LMT

日志内容	OSPFv3 [UINT32] route limit reached.
参数解释	$1：OSPFv3进程ID
日志等级	5
举例	OSPFV3/5/OSPFV3_RT_LMT:OSPFv3 1 route limit reached.
日志说明	OSPFv3进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

91 PBB

本节介绍 PBB 模块输出的日志信息。

91.1 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.
参数解释	$1：聚合组名称 $2：接口名称
日志等级	4
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.
日志说明	将不支持PBB的接口加入已经配置了PBB的聚合组会引发处理错误，配置为PBB实例上行口的聚合组的成员端口都需支持PBB
处理建议	将该接口从聚合组中删除

92 PBR

本节介绍 PBR 模块输出的日志信息。

92.1 PBR_HARDWARE_ERROR

日志内容	Failed to update policy [STRING] due to [STRING].
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： • 硬件资源不足 • 系统不支持该操作 • 硬件资源不足且系统不支持
日志等级	4
举例	PBR/4/PBR_HARDWARE_ERROR: Failed to update policy aaa due to insufficient hardware resources and not supported operations.
日志说明	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

93 PCE

本节介绍 PCE 模块输出的日志信息

93.1 PCE_PCEP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
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	5
举例	PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is up. PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is down (dead timer expired).
日志说明	显示会话的状态变化以及会话down的原因 down 的原因可能包括： • 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

93.2 PEX（IRF3）

本节介绍 PEX（Port Extender）模块输出的日志信息。

93.3 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].
参数解释	$1：PEX端口编号 $2：父设备侧配置的associate ID $3：实际连接的邻居PEX设备associate ID
日志等级	5
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.
日志说明	用户配置的associate ID 与实际连接的PEX设备associate ID不一致
处理建议	请检查组网连接

93.4 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]).
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
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.
日志说明	PEX设备启动前必须通过**associate**命令配置虚拟槽位号或虚拟框号 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的槽号修改到正确的虚拟槽位号/虚拟框号范围内

93.5 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.
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
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.
日志说明	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

93.6 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.
参数解释	$1：PEX设备associate ID $2：PEX设备associate ID
日志等级	5
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.
日志说明	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

93.7 PEX_LINK_BLOCK

日志内容	Status of [STRING] changed from [STRING] to blocked.
参数解释	$1：端口名称 $2：端口的链路状态，如forwarding、down
日志等级	4
举例	PEX/4/PEX_LINK_BLOCK: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to blocked.
日志说明	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中

93.8 PEX_LINK_DOWN

日志内容	Status of [STRING] changed from [STRING] to down.
参数解释	$1：端口名称 $2：端口的链路状态，如forwarding、blocked
日志等级	4
举例	PEX/4/PEX_LINK_DOWN: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to down.
日志说明	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

93.9 PEX_LINK_FORWARD

日志内容	Status of [STRING] changed from [STRING] to forwarding.
参数解释	$1：端口名称 $2：端口的链路状态，如blocked
日志等级	5
举例	PEX/5/PEX_LINK_FORWARD: Status of Ten-GigabitEthernet2/0/1 changed from blocked to forwarding.

日志说明	• 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	正常状态，无需任何处理

93.10 PEX_REG_JOININ

日志内容	PEX ([STRING]) registered successfully on PEX port [UINT32].
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
举例	PEX/5/PEX_REG_JOININ: PEX (slot 101) registered successfully on PEX port 1.
日志说明	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	正常事件，无需任何处理

93.11 PEX_REG_LEAVE

日志内容	PEX ([STRING]) unregistered on PEX port [UINT32].
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
举例	PEX/4/PEX_REG_LEAVE: PEX (slot 101) unregistered on PEX port 1.
日志说明	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	**126.** 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 **127.** 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，以及 **display pex-port** 检查 PEX 端口配置是否存在，或者 PEX 物理端口状态是否全部为 down 或者全部 blocked **128.** 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

93.12 PEX_REG_REQUEST

日志内容	Received a REGISTER request on PEX port [UINT32] from PEX ([STRING]).
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
举例	PEX/5/PEX_REG_REQUEST: Received a REGISTER request on PEX port 1 from PEX (slot 101).
日志说明	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	正常事件，无需任何处理

93.13 PEX_STACKCONNECTION_ERROR

日志内容	A device was connected to a PEX that already had two neighboring devices.
参数解释	无
日志等级	5
举例	PEX/5/PEX_STACKCONNECTION_ERROR: A device was connected to a PEX that already had two neighboring devices.
日志说明	系统中存在连接错误，有一条链路连接到了一个PEX，这个PEX已经存在两个邻居设备
处理建议	请检查组网连接

94 PEX（IRF3.1）

本节介绍 IRF3.1 PEX（Port Extender）模块输出的日志信息。

94.1 PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER

日志内容	[STRING] was assigned to [STRING].
参数解释	$1：物理接口名称 $2：二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER: GigabitEthernet 1/2/0/1 was assigned to Bridge-Aggregation10.
日志说明	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	不需要处理

94.2 PEX_AUTOCONFIG_BAGG_CREATE

日志内容	[STRING] was created by the PEX auto-config feature.
参数解释	$1：二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_CREATE: Bridge-Aggregation10 was created by the PEX auto-config feature.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动创建二层聚合接口用来作级联接口
处理建议	不需要处理

94.3 PEX_AUTOCONFIG_BAGG_NORESOURCE

日志内容	Not enough resources to create a Layer 2 aggregate interface.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_NORESOURCE: Not enough resources to create a Layer 2 aggregate interface.
日志说明	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	删除设备上不需要使用的聚合接口，释放资源

94.4 PEX_AUTOCONFIG_BAGG_REMOVEMEMBER

日志内容	[STRING] was removed from [STRING].
参数解释	$1：物理接口名称 $2：二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_REMOVEMEMBER: GigabitEthernet 1/2/0/1 was removed from Bridge-Aggregation10.
日志说明	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	不需要处理

94.5 PEX_AUTOCONFIG_CAPABILITY_ENABLE

日志内容	PEX connection capability was enabled on [STRING] and the interface was assigned to PEX group [UINT32].
参数解释	$1：二层聚合接口名称 $2：PEX组编号
日志等级	5
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.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动开启连接PEX的二层聚合接口的PEX连接能力，并将该接口加入PEX组中
处理建议	不需要处理

94.6 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.
参数解释	$1：二层聚合接口名称 $2：PEX组编号
日志等级	5
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.
日志说明	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	删除该组中空闲的级联接口，释放资源

94.7 PEX_AUTOCONFIG_CONNECTION_ERROR

日志内容	A PEX connected to more than one upper-tier PEXs.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CONNECTION_ERROR: A PEX connected to more than one upper-tier PEXs.
日志说明	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

94.8 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.
参数解释	$1：二层聚合接口名称 $2：PEX组编号 $3：PEX组编号
日志等级	5
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.
日志说明	父设备运行IRF3.1系统自动配置功能，开启PEX二层聚合接口连接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，请修改配置

94.9 PEX_AUTOCONFIG_DYNAMICBAGG_STP

日志内容	[STRING] was automatically set to dynamic aggregation mode and configured as an STP edge port.
参数解释	$1：二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_DYNAMICBAGG_STP: Bridge-Aggregation10 was automatically set to dynamic aggregation mode and configured as an STP edge port.
日志说明	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	不需要处理

94.10 PEX_AUTOCONFIG_GROUP_CREATE

日志内容	PEX group [UINT32] was created.
参数解释	$1：PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_GROUP_CREATE: PEX group 1 was created.
日志说明	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	不需要处理

94.11 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.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NONUMBERRESOURCE: No virtual slot numbers are available.
日志说明	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	删除空闲级联接口或在空闲级联接口上取消分配虚拟槽位号/虚拟框号的配置，释放资源

94.12 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.
参数解释	$1：物理接口名称 $2：二层聚合接口名称 $3：物理接口名称 $4：二层聚合接口名称
日志等级	5
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.
日志说明	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	将物理接口从聚合组中退出或更换其他物理接口

94.13 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].
参数解释	形式一： $1：虚拟槽位号 $2：二层聚合接口名称 形式二： $1：虚拟框号 $2：二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NUMBER_ASSIGN: Virtual slot number 100 was assigned on Bridge-Aggregation 10.
日志说明	父设备运行IRF3.1系统自动配置功能时，在连接PEX的二层聚合接口上，自动为PEX分配虚拟槽位号/虚拟框号
处理建议	不需要处理

94.14 PEX_LLDP_DISCOVER

日志内容	Discover peer device on interface [STRING]: MAC=STRING, priority=UINT32.
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
举例	PEX/5/PEX_LLDP_DISCOVER: Discover peer device on interface Ten-GigabitEthernet1/0/1: MAC=20f4-9cb6-0100, priority=0.
日志说明	父设备或PEX设备通过LLDP协议发现对端
处理建议	正常状态，无需任何处理

94.15 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.
参数解释	$1：接口名称
日志等级	4
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.
日志说明	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	请检查PEX设备的IRF成员编号是否在1～4范围之内。如果不是，用户可登录PEX设备，用**irf member renumber**命令修改PEX设备的成员编号

94.16 PEX_PECSP_OPEN_RCVD

日志内容	Received a CSP Open message on interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	PEX/5/PEX_PECSP_OPEN_RCVD: Received a CSP Open message on interface Bridge-Aggregation1.
日志说明	接口收到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	正常状态，无需任何处理

94.17 PEX_PECSP_OPEN_SEND

日志内容	Sent a CSP Open message on interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	PEX/5/PEX_PECSP_OPEN_SEND: Sent a CSP Open message on interface Bridge-Aggregation1.
日志说明	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	正常状态，无需任何处理

94.18 PEX_PECSP_TIMEOUT

日志内容	PE CSP timed out on interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	PEX/4/PEX_PECSP_TIMEOUT: PE CSP timed out on interface Bridge-Aggregation1.
日志说明	PE CSP协议超时，PEX设备和父设备无法建立连接
处理建议	请检查父设备和PEX之间链路和IRF3.1相关配置

95 PFILTER

本节介绍报文过滤模块输出的日志信息。

95.1 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.
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
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.
日志说明	IPv4、IPv6、MAC类型的ACL在某方向上全局应用了，系统无法在此方向上全局应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

95.2 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.
参数解释	$1：流量方向
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.3 PFILTER_GLB_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	无

95.4 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.
参数解释	$1：流量方向
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	使用display qos-acl resource命令检查硬件资源使用情况

95.5 PFILTER_GLB_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	无

95.6 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.
参数解释	$1：流量方向
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	使用display qos-acl resource命令检查硬件资源使用情况

95.7 PFILTER_GLB_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	无

95.8 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.
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
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.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.9 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.
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
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.
日志说明	因系统不支持ACL规则而导致无法在某个方向上全局应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

95.10 PFILTER_GLB_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally.
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
举例	PFILTER/3/PFILTER_GLB_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新ACL
处理建议	无

95.11 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.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	使用display qos-acl resource命令检查硬件资源使用情况

95.12 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].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
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.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	无

95.13 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.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.14 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].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
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.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	无

95.15 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.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.16 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].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
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.
日志说明	因故障系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	无

95.17 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.
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
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.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.18 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.
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
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.
日志说明	因系统不支持ACL规则而导致无法在接口的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

95.19 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.
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
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.
日志说明	IPv4、IPv6、MAC类型的ACL在接口某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

95.20 PFILTER_IF_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING].
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
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.
日志说明	因故障系统无法在接口的某个方向上应用或更新ACL规则
处理建议	无

95.21 PFILTER_IPV4_FLOW_INFO

日志内容	ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
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
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).
日志说明	报文过滤引用的IPv4高级ACL规则匹配的首个报文的信息
处理建议	无

95.22 PFILTER_IPV4_FLOW_STATIS

日志内容	ACL [STRING] [STRING] rule [STRING] [STRING], [UINT64] packet(s).
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
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.
日志说明	报文过滤引用的IPv4 高级ACL规则匹配报文的信息和统计信息
处理建议	无

95.23 PFILTER_IPV6_FLOW_INFO

日志内容	IPv6 ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
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
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).
日志说明	报文过滤引用的IPv6高级ACL规则匹配的首个报文的信息
处理建议	无

95.24 PFILTER_IPV6_FLOW_STATIS

日志内容	IPv6 ACL [STRING] [STRING] rule [STRING] [STRING], [UINT64] packet(s).
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
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.
日志说明	报文过滤引用的IPv6高级ACL规则匹配报文的信息和统计信息
处理建议	无

95.25 PFILTER_IPV6_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter IPv6 [UINT32] [STRING] [STRING] [UINT64] packet(s).
参数解释	$1：ACL应用的位置 $2：流量方向 $3：ACL编号或名称 $4：ACL规则的编号ID及内容 $5：ACL规则匹配的报文个数
日志等级	6
举例	PFILTER/6/PFILTER_IPV6_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter IPv6 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
日志说明	ACL规则在报文过滤日志发送周期结束后匹配的报文个数
处理建议	无

95.26 PFILTER_MAC_FLOW_INFO

日志内容	MAC ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
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
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.
日志说明	报文过滤引用的二层ACL规则匹配的首个报文的信息
处理建议	无

95.27 PFILTER_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL应用的位置 $2：流量方向 $3：ACL编号或名称 $4：ACL规则的编号及内容 $5：ACL规则匹配的报文个数
日志等级	6
举例	PFILTER/6/PFILTER_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	ACL规则在报文过滤日志发送周期结束后匹配的报文个数
处理建议	无

95.28 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.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.29 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].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
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.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新IPv4缺省动作
处理建议	无

95.30 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.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.31 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].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
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.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新IPv6缺省动作
处理建议	无

95.32 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.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
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.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.33 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].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
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.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新MAC缺省动作
处理建议	无

95.34 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.
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
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.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

95.35 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.
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
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.
日志说明	因系统不支持ACL规则而导致无法在VLAN的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

95.36 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.
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
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.
日志说明	IPv4、IPv6、MAC类型的ACL已经在VLAN的某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

95.37 PFILTER_VLAN_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16].
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
举例	PFILTER/3/PFILTER_VLAN_UNK_ERR: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新ACL规则
处理建议	无

96 PIM

本节介绍 PIM 模块输出的日志信息。

96.1 PIM_NBR_DOWN

日志内容	[STRING]: Neighbor [STRING] ([STRING]) is 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
举例	PIM/5/PIM_NBR_DOWN: Neighbor 10.1.1.1(Vlan-interface10) is down.
日志说明	PIM邻居的状态变为down
处理建议	检查PIM配置是否错误，检查网络是否发生拥塞

96.2 PIM_NBR_UP

日志内容	[STRING]: Neighbor [STRING] ([STRING]) is 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
举例	PIM/5/PIM_NBR_UP: Neighbor 10.1.1.1(Vlan-interface10) is up.
日志说明	PIM邻居的状态变为up
处理建议	无

97 PING

本节介绍 ping 模块输出的日志信息。

97.1 PING_STATISTICS

日志内容	[STRING] statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
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
举例	PING/6/PING_STATISTICS: Ping statistics for 192.168.0.115: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
日志说明	用户执行**ping**命令查看公网中对端是否可达
处理建议	如果没有收到报文，请检查接口是否DOWN，并查找路由表，看是否存在有效路由

97.2 PING_VPN_STATISTICS

日志内容	[STRING] statistics for [STRING] in VPN instance [STRING] : [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
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
举例	PING/6/PING_VPN_STATISTICS: Ping statistics for 192.168.0.115 in VPN instance vpn1: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
日志说明	用户执行**ping**命令查看VPN中的对端是否可达
处理建议	如果没有收到报文，请检查接口是否DOWN，并查找路由表，看是否存在有效路由

98 PKG

本节介绍包管理模块输出的日志信息。

98.1 PKG_BOOTLOADER_FILE_FAILED

日志内容	Failed to execute the boot-loader file command.
参数解释	无
日志等级	5
举例	PKG/5/PKG_BOOTLOADER_FILE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the boot-loader file command.
日志说明	用户执行**boot-loader file**命令配置设备下次启动时使用的软件包，操作失败
处理建议	请根据提示信息采取相应措施

98.2 PKG_BOOTLOADER_FILE_SUCCESS

日志内容	Executed the boot-loader file command successfully.
参数解释	无
日志等级	5
举例	PKG/5/PKG_BOOTLOADER_FILE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the boot-loader file command successfully.
日志说明	用户执行**boot-loader file**命令配置设备下次启动时使用的软件包，操作成功
处理建议	无

98.3 PKG_INSTALL_ACTIVATE_FAILED

日志内容	Failed to execute the install activate command.
参数解释	无
日志等级	5
举例	PKG/5/PKG_INSTALL_ACTIVATE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the install activate command.
日志说明	用户执行**install activate**命令用来激活或查看软件包，操作失败
处理建议	请根据提示信息采取相应措施

98.4 PKG_INSTALL_ACTIVATE_SUCCESS

日志内容	Executed the install activate command successfully.
参数解释	无
日志等级	5
举例	PKG/5/PKG_INSTALL_ACTIVATE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the install activate command successfully.
日志说明	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

99 PKI

本节包含 PKI 日志消息。

99.1 GET_CERT_FROM_CA_SERVER_FAIL

日志内容	Failed to get the CA or RA certificate from the CA server. Reason: [STRING].
参数解释	$1：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
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.
日志说明	命令行从CA服务器获取CA/RA证书时失败
处理建议	无

99.2 IMPORT_CERT_FAIL

日志内容	Failed to import the certificate. Reason: [STRING].
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
举例	PKI/5/IMPORT_CERT_FAIL: failed to import the certificate. Reason: invalid CA certificate.
日志说明	执行导入命令时可能的失败，原因为证书无效等
处理建议	无

99.3 REQUEST_CERT_FAIL

日志内容	Failed to request certificate of domain [STRING].
参数解释	$1：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_FAIL: Failed to request certificate of domain abc.
日志说明	为PKI域申请证书失败
处理建议	检查设备和CA服务器的配置和其间的网络

99.4 REQUEST_CERT_SUCCESS

日志内容	Request certificate of domain [STRING] successfully.
参数解释	$1：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_SUCCESS: Request certificate of domain abc successfully.
日志说明	为PKI域申请证书成功
处理建议	无

99.5 RETRIEVE_CRL_FAIL

日志内容	Failed to retrieve the CRL. Reason: [STRING].
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
举例	PKI/5/RETRIEVE_CRL_FAIL: Failed to retrieve the CRL. Reason: CRL has expired.
日志说明	取回CRL时的失败原因
处理建议	无

99.6 VALIDATE_CERT_FAIL

日志内容	Failed to validate the certificate. Reason: [STRING].
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
举例	PKI/5/VALIDATE_CERT_FAIL: Failed to validate certificate. Reason: Invalid CA certificate.
日志说明	执行验证命令时可能的失败，原因为证书无效等
处理建议	无

100 PKT2CPU

本节包含 PKT2CPU 日志消息。

100.1 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.
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
举例	PKT2CPU/4/PKT2CPU_NO_RESOURCE: -Interface=Ethernet0/0/2-ProtocolType=21-MacAddr=0180-c200-0014; The resources are insufficient.
日志说明	硬件资源不足
处理建议	取消配置

101 PKTCPT

本节介绍 PKTCPT（Packet Capture）模块输出的日志信息。

101.1 PKTCPT_AP_OFFLINE

日志内容	Failed to start packet capture. Reason: AP was offline.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_AP_OFFLINE: Failed to start packet capture. Reason: AP was offline.
日志说明	指定报文捕获的AP没有上线，报文捕获启动失败
处理建议	检查配置，AP上线后再次开启报文捕获

101.2 PKTCPT_AREADY_EXIT

日志内容	Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_AREADY_EXIT: Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
日志说明	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

101.3 PKTCPT_CONN_FAIL

日志内容	Failed to start packet capture. Reason: Failed to connect to the FTP server.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_CONN_FAIL: Failed to start packet capture. Reason: Failed to connect to the FTP server.
日志说明	无法连接到与设备在同一网段的FTP服务器，报文捕获功能启动失败
处理建议	• 检查 URL 是否合法。可能情况包括：指定的 FTP 服务器的 IP 地址不存在；指定的 IP 地址不是 FTP 服务器的地址；指定的 FTP 服务器的接口处于关闭状态 • 检查 URL 中域名解析是否成功 • 检查开启报文捕获服务设备与 FTP 服务器是否可达 • 检查 FTP 服务器是否上线

101.4 PKTCPT_INVALID_FILTER

日志内容	Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_INVALD_FILTER: Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
日志说明	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

101.5 PKTCPT_LOGIN_DENIED

日志内容	Packet capture aborted. Reason: FTP server login failure.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_LOGIN_DENIED: Packet capture aborted. Reason: FTP server login failure.
日志说明	登录FTP服务器失败，报文捕获退出
处理建议	检查用户名密码是否正确

101.6 PKTCPT_MEMORY_ALERT

日志内容	Packet capture aborted. Reason: Memory threshold reached.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_MEMORY_ALERT: Packet capture aborted. Reason: Memory threshold reached.
日志说明	设备达到内存门限时，报文捕获功能退出
处理建议	无

101.7 PKTCPT_OPEN_FAIL

日志内容	Failed to start packet capture. Reason: File for storing captured frames not opened.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_OPEN_FAIL: Failed to start packet capture. Reason: File for storing captured frames not opened.
日志说明	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	• 若用户不具有写文件权限，请配置写权限 • 若指定的文件名是已经存在并被其它程序占用，请使用其它文件名

101.8 PKTCPT_OPERATION_TIMEOUT

日志内容	Failed to start or continue packet capture. Reason: Operation timed out.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_OPERATION_TIMEOUT: Failed to start or continue packet capture. Reason: Operation timed out.
日志说明	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	• 检查 FTP 服务器是否可达 • 检查 FTP 服务器是否在线

101.9 PKTCPT_SERVICE_FAIL

日志内容	Failed to start packet capture. Reason: TCP or UDP port binding faults.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_SERVICE_FAIL: Failed to start packet capture. Reason: TCP or UDP port binding faults.
日志说明	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	• 如果之前打开的报文捕获客户端（第三方软件 wireshark）没有关闭，请关闭后重新启动报文捕获功能 • 绑定新的端口号，重新启动报文捕获功能

101.10 PKTCPT_UNKNOWN_ERROR

日志内容	Failed to start or continue packet capture. Reason: Unknown error.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_UNKNOWN_ERROR: Failed to start or continue the packet capture. Reason: Unknown error.
日志说明	其它未知原因导致服务启动失败或者退出
处理建议	无

101.11 PKTCPT_UPLOAD_ERROR

日志内容	Packet capture aborted. Reason: Failed to upload captured frames.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_UPLOAD_ERROR: Packet capture aborted. Reason: Failed to upload captured frames.
日志说明	由于上传捕获的数据报文失败，导致报文捕获退出
处理建议	• 检查是否试图改变 FTP 的工作目录 • 检查指定 FTP 服务器上文件是否有写权限 • 检查 FTP 服务器是否下线 • 检查与 FTP 服务器是否可达 • 检查 FTP 服务器是否已满 • 检查报文捕获服务是否退出

101.12 PKTCPT_WRITE_FAIL

日志内容	Packet capture aborted. Reason: Not enough space to store captured frames.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_WRITE_FAIL: Packet capture aborted. Reason: Not enough space to store captured frames.
日志说明	报文文件保存到FLASH时，FLASH已满，报文捕获功能退出
处理建议	删除无用文件释放磁盘空间

102 PoE

本节介绍 PoE 模块输出的日志信息。

102.1 POE_SHUTDOWN_POWEROFF

日志内容	Stopping power supply for PoE port [STRING]. Reason: The port has stopped power supply because of port shutdown.
参数解释	$1：PoE接口名称
日志等级	5
举例	POE/5/POE_SHUTDOWN_POWEROFF: Stopping power supply for PoE port GigabitEthernet1/0/1. Reason: The port has stopped power supply because of port shutdown.
日志说明	开启PoE和接口shutdown联动功能后，处于供电状态的接口，接口下执行**shutdown**命令或者接口被上层业务模块关闭后，PoE模块会自动停止给PoE接口供电
处理建议	使用**display interface**命令，通过Current state字段了解接口被关闭的原因，根据原因进一步定位问题根源

102.2 POE_SHUTDOWN_POWERON

日志内容	Stopping power supply for PoE port [STRING]. Reason: The port has recovered power supply because of port up.
参数解释	$1：PoE接口名称
日志等级	5
举例	POE/5/POE_SHUTDOWN_POWERON: Recovering power supply for PoE port GigabitEthernet1/0/1. Reason: The port has recovered power supply because of port up.
日志说明	开启PoE和接口shutdown联动功能后，处于供电状态的接口，接口下执行**undo shutdown**命令或者被上层业务模块恢复up后，PoE模块会自动恢复给PoE接口供电
处理建议	无

103 PORTAL

本节介绍 PORTAL 模块输出的日志信息。

103.1 PORTAL_RULE_FAILED

日志内容	Failed to assign a portal rule. Reason=[STRING].
参数解释	$1：Portal规则下发失败的原因
日志等级	4
举例	PORTAL/4/PORTAL_RULE_FAILED: -Slot=10; Failed to assign a portal rule. Reason=Not enough resources.
日志说明	Portal规则下发失败
处理建议	请根据规则下发失败的原因选择相应的处理方式，详见表103-1

表103-1 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	请将相关日志信息保存到本地，并联系H3C技术支持
Input parameters in the rule are incorrect.	下发驱动的规则的参数有问题	请将相关日志信息保存到本地，并联系H3C技术支持
The rule already exists.	驱动已经存在该条规则	请将相关日志信息保存到本地，并联系H3C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，请保存相关日志信息并联系H3C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

104 PORTSEC

本节介绍端口安全模块输出的日志信息。

104.1 PORTSEC_ACL_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; ACL authorization failed because[STRING].
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： • the specified ACL didn't exist.：下发的 ACL 不存在 • this type of ACL is not supported.：不支持此 ACL 类型 • hardware resources were insufficient.：内存不足 • 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 • the specified ACL didn't contain any rules.：下发的 ACL 中未包含规则
日志等级	4
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.
日志说明	下发授权ACL失败，及其原因
处理建议	根据失败原因修改配置

104.2 PORTSEC_CAR_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign CAR attributes to driver.
参数解释	$1：接口名 $2：MAC地址
日志等级	5
举例	PORTSEC/5/PORTSEC_CAR_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign CAR attributes to driver.
日志说明	下发CAR到驱动失败
处理建议	无

104.3 PORTSEC_CREATEAC_FAILURE

日志内容	-IfName=[STRING]-VLANID=[STRING]-MACAddr=[STRING]-VSIName=[STRING]; Failed to map an Ethernet service instance to the VSI.
参数解释	$1：接口名 $2：VLAN $3：MAC地址 $4：VSI 名称
日志等级	3
举例	PORTSEC/3/PORTSEC_CREATEAC_FAILURE:-IfName=GigabitEthernet1/0/4-VLANID=444-MACAddr=0010-8400-22b9-VSIName=aaa; Failed to map an Ethernet service instance to the VSI.
日志说明	端口安全模块接收到相关授权信息或者从其子线程模块收到将以太网服务实例与VSI绑定的信息后，执行该操作，如果操作失败则输出此日志信息
处理建议	使用**display l2vpn vsi**命令查询VSI Name是否存在，如果不存在，请通过**vsi**命令创建对应的VSI

104.4 PORTSEC_LEARNED_MACADDR

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; A new MAC address was learned.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID
日志等级	6
举例	PORTSEC/6/PORTSEC_LEARNED_MACADDR:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444; A new MAC address was learned.
日志说明	学到一个新的安全MAC地址
处理建议	无

104.5 PORTSEC_NTK_NOT_EFFECTIVE

日志内容	The NeedToKnow feature is configured but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	PORTSEC/3/PORTSEC_NTK_NOT_EFFECTIVE: The NeedToKnow feature is configured but is not effective on interface Ethernet3/1/2.
日志说明	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	无

104.6 PORTSEC_PORTMODE_NOT_EFFECTIVE

日志内容	The port security mode is configured but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	PORTSEC/3/PORTSEC_PORTMODE_NOT_EFFECTIVE: The port security mode is configured but is not effective on interface Ethernet3/1/2.
日志说明	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
处理建议	改变端口安全模式或关闭接口的端口安全特性

104.7 PORTSEC_PROFILE_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign a user profile to driver.
参数解释	$1：接口名 $2：MAC地址
日志等级	5
举例	PORTSEC/5/PORTSEC_PROFILE_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign a user profile to driver.
日志说明	下发User Profile到驱动失败
处理建议	无

104.8 PORTSEC_URL_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; URL authorization failed because [STRING].
参数解释	$1：接口名 $2：MAC地址 $3：下发URL失败的原因 o this operation was not supported：不支持授权 URL o hardware resources were insufficient：资源不足 o parameters were invalid：参数错误 o an unknown error existed：其它错误
日志等级	4
举例	PORTSEC/5/PORTSEC_URL_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; URL authorization failed because hardware resources were insufficient.
日志说明	下发授权URL失败
处理建议	根据失败原因修改配置

104.9 PORTSEC_VIOLATION

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-IfStatus=[STRING]; Intrusion protection was triggered.
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
举例	PORTSEC/5/PORTSEC_VIOLATION:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-IfStatus=Up; Intrusion protection was triggered.
日志说明	触发入侵检测
处理建议	检查配置情况或改变端口安全模式

104.10 PORTSEC_VLANMACLIMIT

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; Maximum number of MAC addresses already reached in the VLAN.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID
日志等级	5
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.
日志说明	VLAN内同时接入的MAC地址数量达到上限，不允许新MAC地址用户接入
处理建议	检查是否存在来自未知源MAC的报文攻击端口

105 PPP

本节介绍 PPP 模块输出的日志信息。

105.1 IPPOOL_ADDRESS_EXHAUSTED

日志内容	The address pool [STRING] was exhausted.
参数解释	$1：地址池名称
日志等级	5
举例	PPP/5/IPPOOL_ADDRESS_EXHAUSTED: The address pool aaa was exhausted.
日志说明	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	向地址池里添加地址

105.2 PPP_USER_LOGOFF

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User logged off.
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105-1
日志等级	6
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.
日志说明	用户下线
处理建议	无

表105-1 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

下线原因	说明
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

105.3 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.
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105-2
日志等级	5
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.
日志说明	用户上线失败
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105-2 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

上线失败原因	说明
Accounting failed	计费失败

105.4 PPP_USER_LOGON_SUCCESS

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]; User got online successfully.
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
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.
日志说明	用户上线成功
处理建议	无

106 PTP

本节介绍 PTP 模块输出的日志信息。

106.1 PTP_MASTER_CLOCK_CHANGE

日志内容	In PTP instance [UINT16], PTP master clock property changed. (OldMasterClockId=[STRING], CurrentMasterClockId=[STRING], NewSourceIfIndex=[UINT16], OldSourcePortNum=[UINT16], CurrentSourcePortNum=[UINT16], OldSourcePortName=[STRING], CurrentSourcePortName=[STRING])
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：原来主时钟ID $3：当前主时钟ID $4：新的时钟源索引 $5：曾为本设备提供时钟源的接口编号 $6：当前为本设备提供时钟源的接口编号 $7：曾为本设备提供时钟源的接口名称 $8：当前为本设备提供时钟源的接口名称
日志等级	4
举例	PTP/4/PTP_MASTER_CLOCK_CHANGE: In PTP instance 1, PTP master clock property changed. (OldMasterClockId=000FE2-FFFE-FF0000, CurrentMasterClockId=000FE2-FFFE-FF0000, NewSourceIfIndex=1, OldSourcePortNum=2, CurrentSourcePortNum=1, OldSourcePortName=GigabitEthernet1/0/2, CurrentSourcePortName=GigabitEthernet1/0/1)
日志说明	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	使用**display ptp interface brief**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；收集告警、日志和配置信息，联系技术支持
	• 若不存在接口处于 Disabled 状态，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

106.2 PTP_PKTLOST

日志内容	In PTP instance [UINT16], PTP packets were lost. (PortName=[STRING], PktType=[STRING])
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：接口名称 $3：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
举例	PTP/4/PTP_PKTLOST: In PTP instance 1, PTP packets were lost. (PortName=GigabitEthernet1/0/1, PktType=Announce)
日志说明	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 ○ 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 ○ 若不增长，则收集告警、日志和配置信息，联系技术支持

106.3 PTP_PKTLOST_RECOVER

日志内容	In PTP instance [UINT16], PTP packets lost were recovered. (PortName=[STRING], PktType=[STRING])
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：接口名称 $3：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
举例	PTP/4/PTP_PKTLOST_RECOVER: In PTP instance 1, PTP packets lost were recovered. (PortName=GigabitEthernet1/0/1, PktType =Announce)
日志说明	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

106.4 PTP_PORT_BMCINFO_CHANGE

日志内容	In PTP instance [UINT16], PTP BMC info for port [UINT16] changed. (PortName=[STRING], PortSourceId=[STRING], PortSourcePortNum=[UINT16], PortSourceStepsRemoved=[UINT16], CurrentMasterClockId=[STRING])
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：PTP接口索引 $3：PTP接口名称 $4：PTP接口接收到的时钟源ID $5：PTP接口接收到的时钟源端口号 $6：PTP接口接收到的时钟源跳数 $7：设备当前主时钟ID
日志等级	5
举例	PTP/5/PTP_PORT_BMCINFO_CHANGE: In PTP instance 1, PTP BMC info for port 1 changed. (PortName=GigabitEthernet1/0/1, PortSourceId=000FE2-FFFE-FF0001, PortSourcePortNum=1, PortSourceStepsRemoved=5, CurrentMasterClockId=000FE2-FFFE-FF0000)
日志说明	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

106.5 PTP_PORT_STATE_CHANGE

日志内容	In PTP instance [UINT16], PTP port state changed. (IfIndex=[UINT16], PortName=[STRING], PortState=[STRING], OldPortState=[STRING])
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：PTP接口索引 $3：PTP接口名称 $4：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 $5：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
举例	PTP/5/PTP_PORT_STATE_CHANGE: In PTP instance 1, PTP port state changed. (IfIndex=1, PortName=GigabitEthernet1/0/1, PortState=Slave, OldPortState=Master)
日志说明	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	使用**display ptp interface brief**命令查看是否存在PTP接口处于Fault状态

	• 若存在接口处于 Fault 状态，则表示链路故障或接口 DOWN，排除故障恢复链路
	• 若不存在接口处于 Fault 状态，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

106.6 PTP_SRC_CHANGE

日志内容	In PTP instance [UINT16], PTP clock source property changed. (SourceName=[STRING], Priority1=[UCHAR], Priority2=[UCHAR], ClockClass=[UINT16], ClockAccuracy=[UINT16]], ClockSourceType=[STRING])

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：时钟源，取值包括：
	  ○ Local：本地时钟
	  ○ Tod1：第一路 ToD 时钟
	  ○ Tod2：第二路 ToD 时钟
	$3：第一优先级
	$4：第二优先级
	$5：时钟源的时间等级
	$6：时钟源的时间精度
	$7：最优时钟的时钟类别，取值包括：
	  ○ Atomic clock：原子时钟
	  ○ GPS：Global Positioning System，全球定位系统
	  ○ Handset：手持设备
	  ○ Internal oscillator：内部震荡器
	  ○ NTP：Network Time Protocol，网络时间协议
	  ○ Other：其他
	  ○ PTP：Precision Time Protocol，精确时间协议
	  ○ Terrestrial radio：陆基无线电
	  ○ Unknown：未知

日志等级	5
举例	PTP/5/PTP_SRC_CHANGE: In PTP instance 1, PTP clock source property changed. (SourceName=Tod1, Priority1=1, Priority2=2, ClockClass=6, ClockAccuracy=20, ClockSourceType=Atomic clock)
日志说明	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

106.7 PTP_SRC_SWITCH

日志内容	In PTP instance [UINT16], PTP clock source switched. (LastClockID=[STRING], CurrentClockID=[STRING])
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：原来的时钟源ID $3：当前的时钟源ID
日志等级	4
举例	PTP/4/PTP_SRC_SWITCH: In PTP instance 1, PTP clock source switched.(LastSource=000FE2-FFFE-FF0000, CurrentSource=000FE2-FFFE-FF0001)
日志说明	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

106.8 PTP_TIME_LOCK

日志内容	Time resumed to locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_LOCK: Time resumed to locked state.
日志说明	时钟从失锁状态中恢复为正常
处理建议	无

106.9 PTP_TIME_NOT_LOCK

日志内容	Time not in locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_NOT_LOCK: Time not in locked state.
日志说明	时钟失锁告警，原因包括： • 频率失锁 • 子卡或者时钟扣板故障 • DSP 收到的时间戳不变或者错误

处理建议	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
	• 接口正常，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

106.10 PTP_TIME_SYNC

日志内容	Time resumed to synchronized state.
参数解释	无
日志等级	4
举例	PTP/4/PTP_TIME_SYNC: Time resumed to synchronized state.
日志说明	设备恢复到时钟同步的正常状态
处理建议	无

106.11 PTP_TIME_UNSYNC

日志内容	Time changed to unsynchronized state.
参数解释	无
日志等级	4
举例	PTP/4/PTP_TIME_UNSYNC: Time changed to unsynchronized state.
日志说明	设备处于无法进行时钟同步的状态，原因包括： • 链路故障或者接口 DOWN 导致设备没有跟踪的时钟源 • 本设备时钟源优先级配置得太高，使得本设备处于 local 状态，无法同步其他设备的时间信号
处理建议	**129.** 使用 **displsy ptp interface brief** 命令查看设备是否存在 PTP Slave 接口 o 是：请联系技术支持 o 否：执行步骤 2 **130.** 使用 **display ptp clock** 命令，查看 Clock type 字段显示是否为 ToD 外接时钟源类型 o 是：执行步骤 3 o 否：设备没有时钟源可以同步，正常打印 **131.** 检查是否通过 **ptp { tod0 | tod1 } input** 命令配置了 ToD 时钟信号的入方向接收延迟校正时间 o 是：请联系技术支持 o 否：执行步骤 4 **132.** 执行 **ptp { tod0 | tod1 } input** 命令校正 ToD 时钟信号为入方向接收延迟校正时间，查看设备是否打印 PTP_TIME_SYNC 日志 o 是：问题解决 o 否：收集告警、日志和配置信息，联系技术支持

107 PWDCTL

本节介绍 Password control 模块输出的日志信息。

107.1 PWDCTL_ADD_BLACKLIST

日志内容	[STRING] was added to the blacklist for failed login attempts.
参数解释	$1：用户名
日志等级	6
举例	PWDCTL/6/PWDCTRL_ADD_BLACKLIST: hhh was added to the blacklist for failed login attempts.
日志说明	因为用户输入密码错误，用户登录设备失败，被加入密码控制黑名单
处理建议	无

107.2 PWDCTL_CHANGE_PASSWORD

日志内容	[STRING] changed the password because [STRING].
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
举例	PWDCTL/6/PWDCTL_CHANGE_PASSWORD: hhh changed the password because it was the first login of the account.
日志说明	由于某种原因，用户改变用户密码。例如该用户的账户第一次登录设备
处理建议	无

107.3 PWDCTL_FAILED_TO_WRITEPWD

日志内容	Failed to write the password records to file.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.
日志说明	设备无法将用户密码写入密码记录文件
处理建议	请检查设备文件系统存储空间是否充足

107.4 PWDCTL_FAILED_TO_OPENFILE

日志内容	Failed to open the password file.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_OPENFILE: Failed to open the password file.
日志说明	因文件系统异常导致创建或打开*.dat文件失败
处理建议	无

107.5 PWDCTL_NOENOUGHSPACE

日志内容	Not enough free space on the storage media where the file is located.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_NOENOUGHSPACE: Not enough free space on the storage media where the file is located.
日志说明	配置失败，因为*.dat文件所在介质（Flash或CF卡等）存储空间不足
处理建议	请检查设备文件系统存储空间是否充足

108 QOS

本节介绍 QoS 模块输出的日志信息。

108.1 MIRROR_SYNC_CFG_FAIL

日志内容	Failed to restore configuration for monitoring group [UINT32] in [STRING], because [STRING]
参数解释	$1：监控组编号 $2：chassis编号+slot编号或slot编号 $3：数据恢复失败的详细原因
日志等级	4
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.
日志说明	业务板插入设备后，恢复该业务板监控组数据失败。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	删除或者修改不支持配置

108.2 QOS_CAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to the user. Reason: [STRING].
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
日志等级	4
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.
日志说明	1.用户上线，下发配置的CAR信息失败 2.用户已经上线，修改CAR信息或者增加CAR应用失败
处理建议	取消CAR在profile下的应用或者修改CAR的相关参数信息

108.3 QOS_CBWFQ_REMOVED

日志内容	CBWFQ is removed from [STRING].
参数解释	$1：接口名称
日志等级	3
举例	QOS/3/QOS_CBWFQ_REMOVED: CBWFQ is removed from GigabitEthernet4/0/1.
日志说明	因接口最大带宽或接口速率更改后低于接口上原来配置的CBWFQ要求的带宽或速率，系统从接口上删除CBWFQ
处理建议	增大接口最大带宽或接口速率后重新应用被删除的CBWFQ

108.4 QOS_GTS_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply GTS in user profile [STRING] to the user. Reason: [STRING].
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
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.
日志说明	1.用户上线，下发配置的GTS信息失败 2.用户已经上线，修改GTS信息或者增加GTS应用失败
处理建议	取消GTS在user profile下的应用或者修改GTS的相关参数信息

108.5 QOS_LR_APPLYIF_FAIL

日志内容	Failed to apply the rate limit on interface [STRING]. Reason: [STRING]
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
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.
日志说明	• 不支持在接口上配置限速 • 由于资源不足，导致在接口上配置限速失败
处理建议	请根据失败原因，取消接口上的限速配置或者修改接口限速的相关配置

108.6 QOS_NOT_ENOUGH_BANDWIDTH

日志内容	Policy [STRING] requested bandwidth [UINT32](kbps). Only [UINT32](kbps) is available on [STRING].
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
举例	QOS/3/QOS_NOT_ENOUGH_BANDWIDTH: Policy d requested bandwidth 10000(kbps). Only 80(kbps) is available on GigabitEthernet4/0/1.
日志说明	因CBWFQ要求的带宽大于接口最大带宽，CBWFQ配置失败
处理建议	增大接口最大带宽值或减小CBWFQ要求的带宽值

108.7 QOS_NOT_ENOUGH_NNIBANDWIDTH

日志内容	The total UNI bandwidth is greater than the NNI bandwidth. The total UNI bandwidth is greater than the NNI bandwidth.The bandwidth of [STRING] is changed. The total UNI bandwidth is greater than the NNI bandwidth.[STRING] is created based on [STRING] of the UNI interface.
参数解释	$1：接口名称
日志等级	4
举例	QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. The bandwidth of GigabitEthernet4/0/1 is changed. 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.
日志说明	• 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 • 接口带宽改变导致下行接口总带宽大于上行接口总带宽 • 新创建的动态子接口导致下行接口总带宽大于上行接口总带宽
处理建议	增加上行接口带宽或降低下行接口带宽限速

108.8 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].
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
日志等级	4
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.
日志说明	系统在控制平面的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

108.9 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].
参数解释	$1：QoS策略名称 $2：流量方向 $3：槽位号 $4：失败原因
日志等级	4
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.
日志说明	系统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	请根据失败原因，修改策略中的配置

108.10 QOS_POLICY_APPLYGLOBAL_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction globally. [STRING].
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
日志等级	4
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.
日志说明	系统在某个方向上全局应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

108.11 QOS_POLICY_APPLYGLOBAL_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction globally. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：失败原因
日志等级	4
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.
日志说明	系统在某个方向上全局应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

108.12 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].
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
日志等级	4
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.
日志说明	系统在接口的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

108.13 QOS_POLICY_APPLYIF_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
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
日志等级	4
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.
日志说明	系统在接口的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

108.14 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].
参数解释	$1：用户标识信息 $2：QoS policy应用方向 $3：QoS policy名称 $4：User profile名称 $5：失败原因
日志等级	4
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.
日志说明	1.用户上线，下发配置的QoS policy信息失败 2.用户已经上线，修改QoS Policy信息或者增加QoS Policy应用失败
处理建议	取消QoS policy在User profile下的应用或者修改QoS Profile的信息

108.15 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].
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
日志等级	4
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.
日志说明	系统在VLAN的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

108.16 QOS_POLICY_APPLYVLAN_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：VLAN ID $4：失败原因
日志等级	4
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.
日志说明	系统在VLAN的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

108.17 QOS_QMPROFILE_APPLYIF_FAIL

日志内容	Failed to apply queue management profile [STRING] on interface [STRING]. Reason: [STRING]
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
举例	QOS/4/QOS_QMPROFILE_APPLYIF_FAIL: Failed to apply queue management profile b on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
日志说明	• 不支持在接口上应用队列调度策略 • 由于资源不足，导致在接口上应用队列调度策略失败
处理建议	请根据失败原因，取消队列调度策略在接口上的应用或者修改队列调度策略的相关配置

108.18 QOS_QMPROFILE_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply queue management profile [STRING] in session group profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：Queue management Profile名称 $3：Session group Profile名称 $4：失败原因
日志等级	4
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 management profile b in session group profile a to the user. Reason: The QMProfile is not supported.
日志说明	1.用户上线，下发配置的QMProfile信息失败 2.用户已经上线，修改QMProfile信息或者增加QMProfile应用失败
处理建议	取消QMProfile在Session group profile下的应用或者修改QMProfile的相关信息

108.19 QOS_QMPROFILE_MODIFYQUEUE_FAIL

日志内容	Failed to configure queue [UINT32] in queue management profile [STRING]. [STRING].
参数解释	$1：队列编号 $2：Profile名称 $3：失败原因
日志等级	4
举例	QOS/4/QOS_QMPROFILE_MODIFYQUEUE_FAIL: Failed to configure queue 1 in queue management profile myqueue. The value is out of range.
日志说明	qmprofile成功应用到端口后，再对某队列进行修改，新的参数超出端口能力范围
处理建议	取消此profile在对应板的应用再修改队列参数

108.20 QOS_QUEUE_APPLYIF_FAIL

日志内容	Failed to apply queue scheduling on interface [STRING]. Reason: [STRING]
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
举例	QOS/4/QOS_QUEUE_APPLYIF_FAIL: Failed to apply queue scheduling on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
日志说明	• 不支持在接口上进行队列配置 • 由于资源不足，导致在接口上进行队列配置失败
处理建议	请根据失败原因，取消接口上的队列配置或者修改队列配置的相关配置

108.21 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.
参数解释	$1：接口名称
日志等级	4
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.
日志说明	恢复下行接口时，因下行接口上的CAR限速总和超过上行接口带宽，接口的下行接口功能恢复失败
处理建议	增加上行接口带宽或降低下行接口CAR限速总和后，重新使能下行口功能

108.22 WRED_TABLE_CFG_FAIL

日志内容	Failed to dynamically modify the configuration of WRED table [STRING], because [STRING].
参数解释	$1：WRED表的名称 $2：配置失败的详细原因
日志等级	4
举例	QOS/4/WRED_TABLE_CFG_FAIL: Failed to dynamically modify the configuration of WRED table a, because ECN is not supported.
日志说明	由于各业务板支持特性不同，某些配置在部分业务板上不支持
处理建议	无

109 RADIUS

本节介绍 RADIUS 模块输出的日志信息。

109.1 RADIUS_AUTH_FAILURE

日志内容	User [STRING] from [STRING] failed authentication.
参数解释	$1：用户名称 $2：IP地址
日志等级	5
举例	RADIUS/5/RADIUS_AUTH_FAILURE: User abc@system from 192.168.0.22 failed authentication.
日志说明	RADIUS服务器了拒绝用户的认证请求
处理建议	无

109.2 RADIUS_AUTH_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名称 $2：IP地址
日志等级	6
举例	RADIUS/6/RADIUS_AUTH_SUCCESS: User abc@system from 192.168.0.22 was authenticated successfully.
日志说明	RADIUS服务器接收了用户的认证请求
处理建议	无

109.3 RADIUS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	RADIUS/4/RADIUS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
日志说明	删除RADIUS方案中的服务器失败
处理建议	无

110 RDDC

本节介绍 RDDC（冗余备份）模块输出的日志信息。

110.1 RDDC_ACTIVENODE_CHANGE

日志内容	Redundancy group [STRING] active node changed to [STRING], because of [STRING].
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
举例	RDDC/5/RDDC_ACTIVENODE_CHANGE: Redundancy group 1 active node changed to node 1 (chassis 1), because of manual switchover.
日志说明	由于用户配置了手工倒换，配置变更或权重变换，冗余组激活节点发生切换
处理建议	无

111 RESMON

本节介绍 RESMON（RESOURCE MONITER，资源监控）模块输出的日志信息。

111.1 RESMON_MINOR

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource decreased to or below minor threshold [STRING]. [STRING].
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
举例	RESMON/4/RESMON_MINOR: -Resource=AA-Total=100%-Used=83%-Free=17%; Free resource decreased to or below minor threshold 20%.
日志说明	当资源剩余值小于或等于低级别告警门限时，资源进入低级别告警状态，并定期输出该日志
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

111.2 RESMON_MINOR_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource increased above minor threshold [STRING]. [STRING].
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
举例	RESMON/5/RESMON_MINOR_RECOVER: -Resource=AA-Total=100%-Used=77%-Free=23%; Free resource increased above minor threshold 20%.
日志说明	当资源处于低级别告警状态，且剩余值大于低级别告警门限，则资源解除低级别告警状态，并输出该日志。资源使用率进入正常范围
处理建议	无

111.3 RESMON_SEVERE

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource decreased to or below severe threshold [STRING]. [STRING].
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
举例	RESMON/3/RESMON_SEVERE: -Resource=AA-Total=100%-Used=93%-Free=7%; Free resource decreased to or below severe threshold 10%.
日志说明	当资源剩余值小于或等于高级别告警门限，且资源没有被使用完，则资源进入高级别告警状态，并定期输出该日志
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

111.4 RESMON_SEVERE_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource increased above severe threshold [STRING]. [STRING].
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
举例	RESMON/5/RESMON_SEVERE_RECOVER: -Resource=AA-Total=100%-Used=83%-Free=17%; Free resource increased above severe threshold 10%.
日志说明	当资源处于高级别告警状态，并且剩余值大于高级别告警门限时，解除高级别告警状态，并输出该日志
处理建议	无

111.5 RESMON_USEDUP

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Resources used up. [STRING].
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
举例	RESMON/2/RESMON_USEDUP: -Resource=vlaninterface-Total=2048-Used=2048-Free=0; Resources used up.
日志说明	当资源被使用完时，资源进入用完状态，并定期输出该日志
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

111.6 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].
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
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.
日志说明	当资源处于用完状态，且资源被释放，则解除用完状态，并输出该日志
处理建议	无

112 RIP

本节介绍 RIP 模块输出的日志信息。

112.1 RIP_MEM_ALERT

日志内容	RIP Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	RIP/5/RIP_MEM_ALERT: RIP Process received system memory alert start event.
日志说明	RIP模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

112.2 RIP_RT_LMT

日志内容	RIP [UINT32] Route limit reached
参数解释	$1：RIP进程ID
日志等级	6
举例	RIP/6/RIP_RT_LMT: RIP 1 Route limit reached.
日志说明	RIP进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

113 RIPNG

本节介绍 RIPng 模块输出的日志信息。

113.1 RIPNG_MEM_ALERT

日志内容	RIPng Process receivedsystem memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	RIPNG/5/RIPNG_MEM_ALERT: RIPNG Process received system memory alert start event.
日志说明	RIPng模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

113.2 RIPNG_RT_LMT

日志内容	RIPng [UINT32] Route limit reached
参数解释	$1：RIPng进程ID
日志等级	6
举例	RIPNG/6/RIPNG_RT_LMT: RIPng 1 Route limit reached.
日志说明	RIPng进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

114 RM

本节介绍 RM 模块输出的日志信息。

114.1 RM_ACRT_REACH_LIMIT

日志内容	Max active [STRING] routes [UINT32] reached in URT of [STRING]
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
举例	RM/4/RM_ACRT_REACH_LIMIT: Max active IPv4 routes 100000 reached in URT of VPN1
日志说明	VPN实例单播路由表中的激活路由数达到了上限值
处理建议	检查所有的路由并删除不需要的路由

114.2 RM_ACRT_REACH_THRESVALUE

日志内容	Threshold value [UINT32] of max active [STRING] routes reached in URT of [STRING]
参数解释	$1：最大激活路由数告警百分比 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4
举例	RM/4/RM_ACRT_REACH_THRESVALUE: Threshold value 50% of max active IPv4 routes reached in URT of vpn1
日志说明	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百分比
处理建议	修改最大路由数告警百分比或路由数上限值

114.3 RM_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] of active [STRING] routes reached in URT of [STRING]
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
举例	RM/4/RM_THRESHLD_VALUE_REACH: Threshold value 10000 of active IPv4 routes reached in URT of vpn1
日志说明	VPN实例单播路由表中的激活路由数达到了上限值
处理建议	修改路由数上限值

114.4 RM_TOTAL_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] reached for active [STRING] routes in all URTs
参数解释	$1：最大激活路由数 $2：IPv4或IPv6
日志等级	4
举例	RM/4/ RM_TOTAL_THRESHLD_VALUE_REACH:Threshold value 1000 reached for active IPv4 routes in all URTs
日志说明	公网和所有VPN实例的激活路由总数达到了告警值
处理建议	检查路由表确认是否需要进行相关处理

115 RPR

本节介绍 RPR 模块输出的日志信息。

115.1 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].
参数解释	$1：接口名称
日志等级	4
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.
日志说明	RPR环上次级MAC地址的数量超过了最大数量
处理建议	关闭RPR环上配有VRRP功能站点的VRRP功能

115.2 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].
参数解释	$1：接口名称
日志等级	5
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.
日志说明	RPR环上次级MAC地址的数量不再超过最大数量
处理建议	无

115.3 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].
参数解释	$1：接口名称
日志等级	4
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.
日志说明	RPR环上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

115.4 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].
参数解释	$1：接口名称
日志等级	5
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.
日志说明	RPR环上站点的数量不再超过最大数量
处理建议	无

115.5 RPR_EXCEED_RESERVED_RATE

日志内容	An excess reserved rate defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_EXCEED_RESERVED_RATE: An excess reserved rate defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点配置的预留带宽总和超过了环路带宽
处理建议	减少站点的预留带宽，使其总和不大于环路带宽

115.6 RPR_EXCEED_RESERVED_RATE_OVER

日志内容	An excess reserved rate defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
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.
日志说明	RPR环上站点配置的预留带宽总和不再超过环路带宽
处理建议	无

115.7 RPR_IP_DUPLICATE

日志内容	A duplicate IP address defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_IP_DUPLICATE: A duplicate IP address defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	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

115.8 RPR_IP_DUPLICATE_OVER

日志内容	A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
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.
日志说明	RPR环上站点的IP地址不再相同
处理建议	无

115.9 RPR_JUMBO_INCONSISTENT

日志内容	A jumbo configuration defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	6
举例	RPR/6/RPR_JUMBO_INCONSISTENT: A jumbo configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	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

115.10 RPR_JUMBO_INCONSISTENT_OVER

日志内容	A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	6
举例	RPR/6/RPR_JUMBO_INCONSISTENT_OVER: A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的Jumbo帧配置一致
处理建议	无

115.11 RPR_LAGGCONFIG_INCONSISTENT

日志内容	An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：RPR逻辑接口名称
日志等级	4
举例	RPR/4/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	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
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

115.12 RPR_LAGGCONFIG_INCONSISTENT_OVER

日志内容	An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：RPR逻辑接口名称
日志等级	5
举例	RPR/5/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	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
处理建议	无

115.13 RPR_MISCABLING

日志内容	A miscabling defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_MISCABLING: A miscabling defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	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

115.14 RPR_MISCABLING_OVER

日志内容	A miscabling defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_MISCABLING_OVER: A miscabling defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	站点与其它站点间的RPR物理端口连接正确
处理建议	无

115.15 RPR_PROTECTION_INCONSISTENT

日志内容	A protection configuration defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_PROTECTION_INCONSISTENT: A protection configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	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

115.16 RPR_PROTECTION_INCONSISTENT_OVER

日志内容	A protection configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_PROTECTION_INCONSISTENT_OVER: A protection configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的保护模式配置一致
处理建议	无

115.17 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].
参数解释	$1：接口名称
日志等级	3
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.
日志说明	RPR环上至少两个站点间的次级MAC地址重复
处理建议	找到次级MAC地址相同的站点，并修改其次级MAC地址

115.18 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].
参数解释	$1：接口名称
日志等级	5
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.
日志说明	RPR环上站点的次级MAC地址不再相同
处理建议	无

115.19 RPR_TOPOLOGY_INCONSISTENT

日志内容	An inconsistent topology defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_TOPOLOGY_INCONSISTENT: An inconsistent topology defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点上不同端口收集的拓扑信息不一致
处理建议	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

115.20 RPR_TOPOLOGY_INCONSISTENT_OVER

日志内容	An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INCONSISTENT_OVER: An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点上不同端口收集的拓扑信息已一致
处理建议	无

115.21 RPR_TOPOLOGY_INSTABILITY

日志内容	A topology instability defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	RPR/4/RPR_TOPOLOGY_INSTABILITY: A topology instability defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环的拓扑不稳定
处理建议	无

115.22 RPR_TOPOLOGY_INSTABILITY_OVER

日志内容	A topology instability defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INSTABILITY_OVER: A topology instability defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环的拓扑已稳定
处理建议	无

115.23 RPR_TOPOLOGY_INVALID

日志内容	A topology invalid defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	RPR/4/RPR_TOPOLOGY_INVALID: A topology invalid defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点收集的拓扑信息无效
处理建议	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

115.24 RPR_TOPOLOGY_INVALID_OVER

日志内容	A topology invalid defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INVALID_OVER: A topology invalid defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点收集的拓扑信息有效
处理建议	无

116 RRPP

本节介绍 RRPP 模块输出的日志信息。

116.1 RRPP_RING_FAIL

日志内容	Ring [UINT32] in Domain [UINT32] failed.
参数解释	$1：环ID $2：域ID
日志等级	4
举例	RRPP/4/RRPP_RING_FAIL: Ring 1 in Domain 1 failed.
日志说明	RRPP域下的环链路故障
处理建议	检测RRPP环的各个节点，清除网络故障

116.2 RRPP_RING_RESTORE

日志内容	Ring [UINT32] in Domain [UINT32] recovered.
参数解释	$1：环ID $2：域ID
日志等级	4
举例	RRPP/4/RRPP_RING_RESTORE: Ring 1 in Domain 1 recovered.
日志说明	RRPP域下的环故障恢复
处理建议	无

117 RTM

本节介绍 EAA 的 RTM（Real-Time Management）模块输出的日志信息。

117.1 RTM_ENVIRONMENT

日志内容	Can't find environment variable [STRING].
参数解释	$1：EAA环境变量的名称
日志等级	4
举例	RTM/4/RTM_ENVIRONMENT: Can't find environment variable ifwk.
日志说明	EAA策略中引用了环境变量，但是策略执行时，找不到环境变量
处理建议	使用**display rtm environment**命令查询用户自定义的EAA环境变量配置，如果环境变量被误操作删除了，请重新创建

117.2 RTM_TCL_LOAD_FAILED

日志内容	Failed to load the Tcl script file of policy [STRING].
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_LOAD_FAILED: Failed to load the Tcl script file of policy [STRING].
日志说明	Tcl监控策略对应的文件加载到内存失败
处理建议	无

117.3 RTM_TCL_MODIFY

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file had been modified.
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_MODIFY: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file had been modified.
日志说明	Tcl监控策略触发执行时，对应的文件被修改
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

117.4 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.
参数解释	$1：Tcl监控策略的名称
日志等级	4
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.
日志说明	Tcl监控策略触发执行时对应的文件不存在
处理建议	确保Tcl监控策略对应的文件存在或者重新创建Tcl监控策略

118 SAVI

本节介绍 SAVI 模块输出的日志信息。

118.1 SAVI_FILTER_ENTRY_ADD

日志内容	Filter entry add with IP address [STRING], MAC [STRING] on interface [STRING] and VLAN [UINT32].
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
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.
日志说明	新增SAVI过滤表项
处理建议	无

118.2 SAVI_FILTER_ENTRY_DEL

日志内容	Filter entry delete with IP address [STRING], MAC [STRING] on interface [STRING] and VLAN [UINT32].
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
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.
日志说明	删除SAVI过滤表项
处理建议	无

118.3 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].
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
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.
日志说明	设备检测到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

119 SCMD

本节介绍 SCMD（服务控制管理）模块输出的日志信息。

119.1 PROCESS_ABNORMAL

日志内容	The process [STRING] exited abnormally.
参数解释	$1：进程名
日志等级	5
举例	SCMD/5/PROCESS_ABNORMAL: The process devd exited abnormally.
日志说明	服务异常退出
处理建议	**133.** 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 **134.** 如果进程未恢复，请搜集以下信息： ○ 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 ○ **display process log** 命令查看进程信息，如果 core 字段显示为 Y，则表示进程退出时产生 core 文件 ○ 如果产生 core 文件，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；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 ○ 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 **135.** 如果进程已恢复，但仍需要定位进程异常退出的原因，请执行第二步 当使用FTP功能将文件上传到服务器时，请使用binary传输模式

119.2 PROCESS_ACTIVEFAILED

日志内容	The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
参数解释	$1：进程名
日志等级	4
举例	SCMD/4/PROCESS_ACTIVEFAILED: The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
日志说明	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。进程重启
处理建议	无

119.3 SCM_ABNORMAL_REBOOT

日志内容	Failed to restore process [STRING]. Rebooting [STRING].
参数解释	$1：进程名 $2：chassis编号+slot编号或slot编号或the system
日志等级	3
举例	SCMD/3/SCM_ABNORMAL_REBOOT: Failed to restore process ipbased. Rebooting slot 1.
日志说明	进程在设备/slot启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则自动重启设备/slot
处理建议	**136.** 等单板重启后，使用 **`display process`** 命令查看进程是否恢复 **137.** 若多次重启后仍不能恢复，联系工程师解决

119.4 SCM_ABNORMAL_REBOOTMDC

日志内容	Failed to restore process [STRING] on [STRING] [UINT16]. Rebooting [STRING] [UINT16].
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
举例	SCMD/3/SCM_ABNORMAL_REBOOTMDC: Failed to restore process ipbased on MDC 2. Rebooting MDC 2.
日志说明	在主用主控板上的用户MDC的在启动过程中，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	**138.** 等单板重启后，使用 **`display process`** 命令查看进程是否恢复 **139.** 若多次重启后仍不能恢复，联系工程师解决

119.5 SCM_ABORT_RESTORE

日志内容	Failed to restore process [STRING]. Restoration aborted.
参数解释	$1：进程名
日志等级	3
举例	SCMD/3/SCM_ABORT_RESTORE: Failed to restore process ipbased. Restoration aborted.
日志说明	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
处理建议	**140.** 任意视图下执行 **display process log** 命令查看进程退出详细信息 **141.** 重启异常进程所在单板或 MDC，尝试恢复 **142.** 提供 **display process log** 命令的显示信息，联系工程师解决

119.6 SCM_INSMOD_ADDON_TOOLONG

日志内容	Failed to finish loading [STRING] in [UINT32] minutes.
参数解释	$1：内核文件的名称 $2：已加载时间
日志等级	4
举例	SCMD/4/SCM_INSMOD_ADDON_TOOLONG: Failed to finish loading addon.ko in 30 minutes.
日志说明	设备启动过程中加载内核文件超时
处理建议	**143.** 重启单板，尝试恢复 **144.** 联系工程师解决

119.7 SCM_KERNEL_INIT_TOOLONG

日志内容	Kernel init in sequence [STRING] function [STRING] is still starting for [UINT32] minutes.
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
举例	SCMD/4/SCM_KERNEL_INIT_TOOLONG: Kernel init in sequence 0x25e7 function 0x6645ffe2 is still starting for 15 minutes.
日志说明	内核初始化时，某个阶段某函数运行时间过长
处理建议	**145.** 重启单板，尝试恢复 **146.** 联系工程师解决

119.8 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].
参数解释	形式一： $1：进程名 $2：进程收到停止信号到输出该日志的时间 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输出该日志的时间
日志等级	6
举例	SCMD/6/SCM_KILL_PROCESS: The process stamgrd was killed because it failed to stop within 30 minutes..
日志说明	某进程超过一定时间没按照指令正常停止，则系统会强制杀掉该进程
处理建议	**147.** 系统/MDC/Context 稳定后，使用 **`display process`** 命令查看进程是否恢复 **148.** 联系工程师解决

119.9 SCM_PROCESS_STARTING_TOOLONG

日志内容	形式一： The process [STRING] has not finished starting in [UINT32] hours. 形式二： The process [STRING] on [STRING] [UINT16] has not finished starting in [STRING] hours.
参数解释	形式一： $1：进程名 $2：所用时间 形式二： $1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号 $4：所用时间
日志等级	4
举例	SCMD/4/SCM_PROCESS_STARTING_TOOLONG: The process ipbased has not finished starting in 1 hours.
日志说明	进程长时间未启动完成。可能是因为配置太多导致进程启动慢，也可能是进程异常
处理建议	**149.** 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 **150.** 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 **151.** 联系工程师解决

119.10 SCM_PROCESS_STILL_STARTING

日志内容	形式一： The process [STRING] is still starting for [UINT32] minutes. 形式二： The process [STRING] on [STRING] [UINT16] is still starting for [STRING] minutes.
参数解释	形式一： $1：进程的名称 $2：所用时间 形式二： $1：进程的名称 $2：取值为MDC或Context $3：MDC或Context编号 $4：所用时间
日志等级	6
举例	SCMD/6/SCM_PROCESS_STILL_STARTING: The process ipbased is still starting for 20 minutes.
日志说明	某进程一直处于启动状态
处理建议	无

119.11 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.
参数解释	形式一： $1：进程名 形式二： $1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号
日志等级	3
举例	SCMD/3/SCM_SKIP_PROCESS: The process ipbased was skipped because it failed to start within 6 hours.
日志说明	某进程超过6小时未启动完成，系统跳过该进程，继续启动
处理建议	**152.** 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 **153.** 联系工程师解决

120 SCRLSP

本节介绍静态 CRLSP 模块输出的日志信息。

120.1 SCRLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static CRLSP [STRING] is duplicate.
参数解释	$1：入标签值 $2：静态CRLSP名称
日志等级	4
举例	SCRLSP/4/SCRLSP_LABEL_DUPLICATE: Incoming label 1024 for static CRLSP aaa is duplicate.
日志说明	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： **154.** 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 **155.** 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

121 SESSION

本节介绍 SESSION 模块输出的日志信息。

121.1 SESSION_IPV4_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];
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 $21：日志类型描述信息，包括： • Session created：会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	SESSION/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;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;

日志说明	创建、删除IPv4会话时会发送该日志 IPv4会话过程中会定时发送该日志 IPv4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

121.2 SESSION_IPV6_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $3：目的IPv6地址 $4：目的端口号 $5：入方向的报文总数 $6：入方向的字节总数 $7：出方向的报文总数 $8：出方向的字节总数 $9：源VPN名称 $10：目的VPN名称 $11：创建会话的时间 $12：会话删除时间 $13：日志类型 $14：日志类型描述信息，包括： • Session created：会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	SESSION/6/SESSION_IPV6_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8)Session created;
日志说明	创建、删除IPv6会话时会发送该日志 IPv6会话过程中会定时发送该日志 IPv6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

122 SFLOW

本节介绍 sFlow 模块输出的日志信息。

122.1 SFLOW_HARDWARE_ERROR

日志内容	Failed to [STRING] on interface [STRING] due to [STRING].
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
举例	SFLOW/4/SFLOW_HARDWARE_ERROR: Failed to update sampling mode on interface GigabitEthernet1/0/1 due to not supported operation.
日志说明	用户执行的配置不会生效。触发该日志的原因可能有：设备不支持的流采样模式
处理建议	改用其它采样模式

123 SHELL

本节介绍 SHELL 模块输出的日志信息。

123.1 SHELL_CMD

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command is [STRING].
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
举例	SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User=**; Command is quit.
日志说明	记录设备执行过的命令
处理建议	无

123.2 SHELL_CMD_CONFIRM

日志内容	Confirm option of command [STRING] is [STRING].
参数解释	$1：命令字符串 $2：确认选项
日志等级	6
举例	SHELL/6/SHELL_CMD_CONFIRM: Confirm option of command save is no.
日志说明	记录需要用户确认命令的用户选项操作结果
处理建议	无

123.3 SHELL_CMD_EXECUTEFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be executed.
参数解释	$1：用户名 $2：IP地址 $3：命令字符串 $4：当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_EXECUTEFAIL: -User=**-IPAddr=192.168.62.138; Command save in view system failed to be executed.
日志说明	设备后台程序下发的命令执行失败
处理建议	定位命令执行失败的具体原因

123.4 SHELL_CMD_INPUT

日志内容	Input string for the [STRING] command is [STRING].
参数解释	$1：命令字符串 $2：输入字符串
日志等级	6
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.
日志说明	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

123.5 SHELL_CMD_INPUT_TIMEOUT

日志内容	Operation timed out: Getting input for the [STRING] command.
参数解释	$1：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMD_INPUT_TIMEOUT: Operation timed out: Getting input for the fdisk command.
日志说明	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	无

123.6 SHELL_CMD_INVALID_CHARACTER

日志内容	Execution failed for the [STRING] command. Reason: The command contains invalid characters (? or \t).
参数解释	$1：要执行的命令行
日志等级	6
举例	SHELL/6/SHELL_CMD_INVALID_CHARACTER: Execution failed for the sysname abc?? command. Reason: The command contains invalid characters (? or \t).
日志说明	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

123.7 SHELL_CMD_MATCHFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be matched.
参数解释	$1：用户名 $2：IP地址 $3：命令字符串 $4：当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=192.168.62.138; Command description 10 in view system failed to be matched.
日志说明	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	定位命令匹配失败的具体原因

123.8 SHELL_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command=[STRING] is denied.
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
举例	SHELL/5/SHELL_CMDDENY: -Line=vty0-IPAddr=192.168.62.138-User=**; Command vlan 10 is permission denied.
日志说明	命令执行失败。用户权限不够
处理建议	无

123.9 SHELL_CMDFAIL

日志内容	The [STRING] command failed to restore the configuration.
参数解释	$1：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMDFAIL: The “vlan 1024” command failed to restore the configuration.
日志说明	文本配置恢复操作失败
处理建议	无

123.10 SHELL_COMMIT

日志内容	The configuration has been committed.
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT: The configuration has been committed.
日志说明	配置提交成功
处理建议	无

123.11 SHELL_COMMIT_DELAY

日志内容	A configuration rollback will be performed in [INT32] minutes.
参数解释	$1：用户指定的配置提交超时时间
日志等级	5
举例	SHELL/5/SHELL_COMMIT_DELAY: A configuration rollback will be performed in 3 minutes.
日志说明	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

123.12 SHELL_COMMIT_REDELAY

日志内容	The commit delay has been reset, a configuration rollback will be performed in [INT32] minutes.
参数解释	$1：用户重新设置的超时时间
日志等级	5
举例	SHELL/5/SHELL_COMMIT_REDELAY: The commit delay has been reset, a configuration rollback will be performed in 3 minutes.
日志说明	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	无

123.13 SHELL_COMMIT_ROLLBACK

日志内容	The configuration commit delay is overtime, a configuration rollback will be performed.
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT_ROLLBACK: The configuration commit delay is overtime, a configuration rollback will be performed.
日志说明	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	请停止任何配置操作，即将进行配置回滚

123.14 SHELL_COMMIT_ROLLBACKDONE

日志内容	The configuration rollback has been performed.
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT_ROLLBACKDONE: The configuration rollback has been performed.
日志说明	配置回滚完成
处理建议	配置回滚完成，请继续操作

123.15 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.
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.
日志说明	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

123.16 SHELL_CRITICAL_CMDFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command=[STRING] .
参数解释	$1：用户名 $2：IP地址 $3：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CRITICAL_CMDFAIL: -User=admin-IPAddr=169.254.0.7; Command is save.
日志说明	命令执行失败
处理建议	无

123.17 SHELL_LOGIN

日志内容	[STRING] logged in from [STRING].
参数解释	$1：用户名 $2：用户线名
日志等级	5
举例	SHELL/5/SHELL_LOGIN: Console logged in from console0.
日志说明	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	无

123.18 SHELL_LOGOUT

日志内容	[STRING] logged out from [STRING].
参数解释	$1：用户名 $2：用户线名
日志等级	5
举例	SHELL/5/SHELL_LOGOUT: Console logged out from console0.
日志说明	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
处理建议	无

124 SLSP

本节介绍静态 LSP 模块输出的日志信息。

124.1 SLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static LSP [STRING] is duplicate.
参数解释	$1：入标签值 $2：静态LSP名称
日志等级	4
举例	SLSP/4/SLSP_LABEL_DUPLICATE: Incoming label 1024 for static LSP aaa is duplicate.
日志说明	静态LSP的入标签被静态PW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 PW 或静态 CRLSP 占用的静态 LSP • 在入标签被静态 PW 或静态 CRLSP 占用的静态 LSP 存在的情况下，使能 MPLS
处理建议	删除该LSP，重新配置一条静态LSP，并指定一个新的入标签

125 SMLK

本节介绍 Smart Link 模块输出的日志信息。

125.1 SMLK_LINK_SWITCH

日志内容	Status of port [STRING] in smart link group [UINT16] changes to active.
参数解释	$1：端口名称 $2：Smart Link组ID
日志等级	4
举例	SMLK/4/SMLK_LINK_SWITCH: Status of port GigabitEthernet0/1/4 in smart link group 1 changes to active.
日志说明	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

126 SNMP

本节介绍 SNMP 模块输出的日志信息。

126.1 SNMP_ACL_RESTRICTION

日志内容	SNMP [STRING] from [STRING] is rejected due to ACL restriction.
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
举例	SNMP/3/SNMP_ACL_RESTRICTION: SNMP community public from 192.168.1.100 is rejected due to ACL restrictions.
日志说明	当SNMP报文因ACL限制被拒绝通过时，打印系统日志
处理建议	检查SNMP agent上的ACL配置，及agent是否被攻击

126.2 SNMP_AUTHENTICATION_FAILURE

日志内容	Failed to authenticate SNMP message.
参数解释	无
日志等级	4
举例	SNMP/4/SNMP_AUTHENTICATION_FAILURE: Failed to authenticate SNMP message.
日志说明	NMS向Agent发起SNMP请求，当认证失败时，Agent记录此日志信息
处理建议	无

126.3 SNMP_GET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=GET-node=[STRING]-value=[STRING]; The agent received a message.
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
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.
日志说明	NMS向Agent发送Get请求报文。如果SNMP日志功能开启，SNMP模块将记录Get请求相关信息
处理建议	无

126.4 SNMP_INFORM_LOST

日志内容	Inform failed to reach NMS [STRING]: Inform [STRING][STRING].
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
举例	SNMP/3/SNMP_INFORM_LOST: Inform failed to reach NMS 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
日志说明	设备给NMS发送Inform报文后，未收到NMS的响应报文，则认为NMS不可达。设备会打印该日志方便用户定位 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
处理建议	检查设备到NMS是否路由可达

126.5 SNMP_NOTIFY

日志内容	Notification [STRING][STRING].
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
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)=**.
日志说明	Agent发送告警给NMS。如果SNMP告警日志功能开启，Agent将记录SNMP告警信息 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
处理建议	无

126.6 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.
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
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.
日志说明	NMS向Agent发送Set请求。如果SNMP日志功能开启，SNMP模块将记录Set操作
处理建议	无

126.7 SNMP_USM_NOTINTIMEWINDOW

日志内容	-User=[STRING]-IPAddr=[STRING]; SNMPv3 message is not in the time window.
参数解释	$1：用户名 $2：NMS的IP地址
日志等级	4
举例	SNMP/4/SNMP_USM_NOTINTIMEWINDOW: -User=admin-IPAddr=169.254.0.7; SNMPv3 message is not in the time window.
日志说明	SNMPv3消息不在时间窗
处理建议	无

127 SSHC

本节介绍 SSHC（SSH Client，SSH 客户端）模块输出的日志信息。

127.1 SSHC_ALGORITHM_MISMATCH

日志内容	The SSH client failed to log in because of [STRING] algorithm mismatch.
参数解释	$1：算法类型，取值包括： • 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
举例	SSHC/5/SSHC_ALGORITHM_MISMATCH: The SSH client failed to log in because of encryption algorithm mismatch.
日志说明	算法不匹配，SSH客户端登录失败
处理建议	修改算法，使SSH客户端和服务器使用相同算法

127.2 SSHC_AUTH_PASSWORD_FAIL

日志内容	SSH user [STRING] failed to pass password authentication because of invalid username or wrong password.
参数解释	$1：用户名
日志等级	5
举例	SSHC/5/SSHC_AUTH_PASSWORD_FAIL: SSH user aaa failed to pass password authentication because of invalid username or wrong password.
日志说明	由于用户名无效或者密码错误导致认证失败
处理建议	检查用户是否存在和密码是否正确

127.3 SSHC_AUTH_PUBLICKEY_FAIL

日志内容	SSH user [STRING] failed to pass publickey authentication.
参数解释	$1：用户名
日志等级	5
举例	SSHC/5/SSHC_AUTH_PUBLICKEY_FAIL: SSH user abc failed to pass publickey authentication.
日志说明	SSH用户没有通过公钥认证
处理建议	检查服务器上保存的用户公钥与客户端上的公钥是否一致

127.4 SSHC_CERT_VERIFY_FAIL

日志内容	Failed to verify the certificate because [STRING].
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
举例	SSHC/5/SSHC_CERT_VERIFY_FAIL: Failed to verify the certificate because null certificate.
日志说明	证书验证失败
处理建议	检查证书有效性

127.5 SSHC_CONNECT_FAIL

日志内容	The SSH client failed to connect to SSH server [IPADDR] port [UINT32].
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
举例	SSHC/5/SSHC_CONNECT_FAIL: The SSH client failed to connect to SSH server 1.1.1.1 port 2000.
日志说明	和SSH服务器建立连接失败
处理建议	检查IP地址端口是否正确，SSH服务器端是否开启服务

127.6 SSHC_DECRYPT_FAIL

日志内容	The SSH client failed to use [STRING] to decrypt the packet received from the SSH server.
参数解释	$1：加密算法（比如aes256-cbc）
日志等级	5
举例	SSHC/5/SSHC_DECRYPT_FAIL: The SSH client failed to use aes256-cbc to decrypt the packet received from the SSH server.
日志说明	来自SSH服务器端的报文解密失败
处理建议	请联系技术支持

127.7 SSHC_DISCONNECT

日志内容	The SSH client was disconnected from the SSH server because the network was not available.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_DISCONNECT: The SSH client was disconnected from the SSH server because the network was not available.
日志说明	SSH客户端与服务器由于网络问题断开连接
处理建议	检查网络

127.8 SSHC_ENCRYPT_FAIL

日志内容	The SSH client failed to use [STRING] to encrypt the packet sent to the SSH server.
参数解释	$1：加密算法（比如aes256-cbc）
日志等级	5
举例	SSHC/5/SSHC_ENCRYPT_FAIL: The SSH client failed to use aes256-cbc to encrypt the packet sent to the SSH server.
日志说明	发往SSH服务器的报文加密失败
处理建议	请联系技术支持

127.9 SSHC_HOST_NAME_ERROR

日志内容	The SSH server host name [STRING] is incorrect.
参数解释	$1：主机名
日志等级	5
举例	SSHC/5/SSHC_HOST_NAME_ERROR: The SSH server host name AAA is incorrect.
日志说明	服务器主机名错误
处理建议	检查指定的主机名

127.10 SSHC_KEY_EXCHANGE_FAIL

日志内容	The SSH client failed to exchange keys with the SSH server.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_KEY_EXCHANGE_FAIL: The SSH client failed to exchange keys with the SSH server.
日志说明	在密钥交换过程中出现错误
处理建议	检查SSH客户端和服务器端的支持的算法类型是否匹配，如不匹配更改SSH客户端支持的算法

127.11 SSHC_MAC_ERROR

日志内容	The SSH client received from the SSH server a packet with incorrect message authentication code.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_MAC_ERROR: The SSH client received from the SSH server a packet with incorrect message authentication code.
日志说明	SSH客户端从服务器收到一个MAC错误的报文
处理建议	无

127.12 SSHC_PUBLICKEY_NOT_EXIST

日志内容	The public key of the SSH server does not exist.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_PUBLICKEY_NOT_EXIST: The public key of the SSH server does not exist.
日志说明	用户登录过程中指定的服务器端公钥不存在
处理建议	通过**display public-key peer**命令检查服务器端指定公钥是否存在

127.13 SSHC_VERSION_MISMATCH

日志内容	The SSH client failed to log in because of version mismatch.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_VERSION_MISMATCH: The SSH client failed to log in because of version mismatch.
日志说明	版本不匹配，导致SSH客户端登录失败
处理建议	更改SSH客户端的版本号

128 SSHS

本节介绍 SSHS（SSH server，SSH 服务器）模块输出的日志信息。

128.1 SSHS_ACL_DENY

日志内容	The SSH Connection [IPADDR]([STRING]) request was denied according to ACL rules.
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
举例	SSHS/5/SSH_ACL_DENY: The SSH Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	SSH ACL规则限制登录IP地址。该日志在SSH服务端检测到非法客户端尝试登录时输出
处理建议	无

128.2 SSHS_ALGORITHM_MISMATCH

日志内容	SSH client [STRING] failed to log in because of [STRING] algorithm mismatch.
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（Message Authentication code）或者public key（公钥）
日志等级	6
举例	SSHS/6/SSHS_ALGORITHM_MISMATCH: SSH client 192.168.30.117 failed to log in because of encryption algorithm mismatch.
日志说明	算法不匹配，SSH客户端登录失败
处理建议	修改算法，使SSH客户端和服务器使用相同算法

128.3 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.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
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.
日志说明	SSH用户登录失败，认证尝试次数达到了最大值
处理建议	请SSH用户确认登录信息，并尝试重新登录

128.4 SSHS_AUTH_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass public key authentication for [STRING].
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	6
举例	SSHS/6/SSHS_AUTH_FAIL: SSH user David (IP: 192.168.30.117) didn't pass public key authentication for wrong public key algorithm.
日志说明	SSH用户没有通过公钥认证
处理建议	请SSH用户重新登录

128.5 SSHS_AUTH_KBDINT_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass keyboard-interactive authentication.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_AUTH_KBDINT_FAIL: SSH user David (IP: 192.168.30.117) didn't pass keyboard-interactive authentication.
日志说明	SSH用户没有通过keyboard-interactive认证
处理建议	请SSH用户重新登录

128.6 SSHS_AUTH_PWD_FAIL

日志内容	Authentication failed for user [STRING] from [STRING] port [INT32] because of invalid username or wrong password.
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
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.
日志说明	由于用户名无效或者密码错误导致认证失败
处理建议	检查用户名密码

128.7 SSHS_AUTH_SUCCESS

日志内容	SSH user [STRING] from [IPADDR] port [INTEGER] passed [STRING] authentication.
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
举例	SSHS/6/SSHS_AUTH_SUCCESS: SSH user ABC from 1.1.1.1 port 55361 passed keyboard-interactive authentication.
日志说明	SSH用户认证通过
处理建议	无

128.8 SSHS_AUTH_TIMEOUT

日志内容	Authentication timed out for [IPADDR].
参数解释	$1：用户IP地址
日志等级	6
举例	SSHS/6/SSHS_AUTH_TIMEOUT: Authentication timed out for 1.1.1.1.
日志说明	SSH用户认证超时。该日志在SSH服务端检测到用户认证超时时输出
处理建议	建议用户检查是否没有及时输入认证信息

128.9 SSHS_AUTHOR_FAIL

日志内容	Authorization failed for user [STRING] from [STRING] port [INT32].
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
举例	SSHS/6/SSHS_AUTHOR_FAIL: Authorization failed for user David from 140.1.2.46 port 15000.
日志说明	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

128.10 SSHS_CERT_VERIFY_FAIL

日志内容	Failed to verify the certificate because [STRING].
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
举例	SSHS/5/SSHS_CERT_VERIFY_FAIL: Failed to verify the certificate because null certificate.
日志说明	证书验证失败
处理建议	检查证书有效性

128.11 SSHS_CONNECT

日志内容	SSH user [STRING] (IP: [STRING]) connected to the server successfully.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_CONNECT: SSH user David (IP: 192.168.30.117) connected to the server successfully.
日志说明	SSH用户成功登录服务器
处理建议	无

128.12 SSHS_DECRYPT_FAIL

日志内容	The packet from [STRING] failed to be decrypted with [STRING].
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
举例	SSHS/5/SSHS_DECRYPT_FAIL: The packet from 192.168.30.117 failed to be decrypted with aes256-cbc.
日志说明	来自SSH客户端的报文解密失败
处理建议	无

128.13 SSHS_DISCONNECT

日志内容	SSH user [STRING] (IP: [STRING]) disconnected from the server.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_DISCONNECT: SSH user David (IP: 192.168.30.117) disconnected from the server.
日志说明	SSH用户退出登录
处理建议	无

128.14 SSHS_ENCRYPT_FAIL

日志内容	The packet to [STRING] failed to be encrypted with [STRING].
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
举例	SSHS/5/SSHS_ENCRYPT_FAIL: The packet to 192.168.30.117 failed to be encrypted with aes256-cbc.
日志说明	发往SSH客户端的报文加密失败
处理建议	无

128.15 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].
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
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.
日志说明	由于用户名无效或者密码错误导致认证失败 SSH用户授权失败
处理建议	无

128.16 SSHS_MAC_ERROR

日志内容	SSH server received a packet with wrong message authentication code (MAC) from [STRING].
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_MAC_ERROR: SSH server received a packet with wrong message authentication code (MAC) from 192.168.30.117.
日志说明	SSH服务器从客户端收到一个MAC错误的报文
处理建议	无

128.17 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].
参数解释	$1：SSH客户端IP地址 $2：当前的SSH会话数 $3：设备允许建立的SSH会话数
日志等级	6
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.
日志说明	SSH客户端登录失败，SSH会话数达到了最大值
处理建议	无

128.18 SSHS_REACH_USER_LIMIT

日志内容	SSH client [STRING] failed to log in, because the number of users reached the upper limit.
参数解释	$1：SSH客户端IP地址
日志等级	6
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.
日志说明	SSH客户端登录失败，SSH用户数达到了最大值
处理建议	无

128.19 SSHS_SCP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
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
举例	SSHS/6/SSHS_SCP_OPER: -MDC=1; User user1 at 1.1.1.1 requested operation: put file "aa".
日志说明	SCP服务器收到SCP用户请求执行相关操作
处理建议	无

128.20 SSHS_SFTP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
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
举例	SSHS/6/SSHS_SFTP_OPER: User user1 at 1.1.1.1 requested operation: open dir "flash:/".
日志说明	SFTP用户请求相关操作信息。该日志在SFTP服务端收到用户请求执行相关命令时输出
处理建议	无

128.21 SSHS_SRV_UNAVAILABLE

日志内容	The [STRING] server is disabled or the [STRING] service type is not supported.
参数解释	$1：服务类型，包括Stelnet、SCP、SFTP、NETCONF
日志等级	6
举例	SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type is not supported.
日志说明	Stelnet/SCP/SFTP/NETCONF over SSH服务不可用，服务器正在断开连接
处理建议	检查服务状态或用户配置

128.22 SSHS_VERSION_MISMATCH

日志内容	SSH client [STRING] failed to log in because of version mismatch.
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_VERSION_MISMATCH: SSH client 192.168.30.117 failed to log in because of version mismatch.
日志说明	SSH客户端和服务器的SSH版本号不匹配
处理建议	修改版本，使SSH客户端和服务器使用相同SSH版本

129 STAMGR

本节介绍 STAMGR 模块输出的日志信息。

129.1 STAMGR_ADD_FAILVLAN

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Added a user to the Fail VLAN [STRING].
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
举例	STAMGR/5/STAMGR_ADD_FAILVLAN:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Added a user to the Fail VLAN 5.
日志说明	用户认证失败加入Fail-VLAN
处理建议	无

129.2 STAMGR_ADDBAC_INFO

日志内容	Add BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_ADDBAC_INFO: Add BAS AC 3ce5-a616-28cd.
日志说明	Master AC与BAS AC建立连接
处理建议	无

129.3 STAMGR_ADDSTA_INFO

日志内容	Add client [STRING].
参数解释	$1：客户端的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_ADDSTA_INFO: Add client 3ce5-a616-28cd.
日志说明	客户端成功连接到BAS AC
处理建议	无

129.4 STAMGR_AUTHORACL_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign an ACL. Reason: [STRING].
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
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.
日志说明	下发ACL失败
处理建议	无

129.5 STAMGR_AUTHORUSERPROFILE_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign a user profile
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
举例	STAMGR/5/STAMGR_AUTHORUSERPROFILE_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Failed to assign a user profile
日志说明	下发user profile失败
处理建议	无

129.6 STAMGR_CLIENT_OFFLINE

日志内容	Client [STRING] went offline from BSS [STRING] with [STRING]. State changed to Unauth.
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
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.
日志说明	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

129.7 STAMGR_CLIENT_ONLINE

日志内容	Client [STRING] went online from BSS [STRING] with SSID [STRING]. State changed to Run.
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
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.
日志说明	客户端在BSS上线，状态变为运行状态
处理建议	无

129.8 STAMGR_DELBAC_INFO

日志内容	Delete BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_DELBAC_INFO: Delete BAS AC 3ce5-a616-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

129.9 STAMGR_DELSTA_INFO

日志内容	Delete client [STRING].
参数解释	$1：客户端的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_DELSTA_INFO: Delete client 3ce5-a616-28cd.
日志说明	客户端断开与BAS AC的连接
处理建议	无

129.10 STAMGR_DOT1X_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication.
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
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.
日志说明	用户802.1X认证失败。触发该日志的原因可能有：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

129.11 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.
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
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.
日志说明	用户通过802.1X认证
处理建议	无

129.12 STAMGR_DOT1X_LOGOFF

日志内容	Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; Session for an 802.1X user was terminated.
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
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.
日志说明	802.1X用户下线
处理建议	无

129.13 STAMGR_MACA_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user failed MAC authentication.
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
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.
日志说明	用户MAC地址认证失败。触发该日志的原因可能有：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

129.14 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.
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
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.
日志说明	用户通过MAC地址认证
处理建议	无

129.15 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.
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
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.
日志说明	用户下线
处理建议	无

129.16 STAMGR_STAIPCHANGE_INFO

日志内容	IP address of client [STRING] changed to [STRING].
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
举例	STAMGR/6/STAMGR_STAIPCHANGE_INFO: IP address of client 3ce5-a616-28cd changed to 4.4.4.4.
日志说明	客户端更新IP地址
处理建议	无

129.17 STAMGR_TRIGGER_IP

日志内容	-SSID=[STRING]-UserMAC=[STRING]-VLANID=[STRING]; Intrusion protection triggered. Action: [STRING].
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
举例	STAMGR/5/STAMGR_TRIGGER_IP:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-VLANID=11; Intrusion protection triggered, the intrusion protection action: added a user to the list of Block-MAC.
日志说明	触发入侵检测，并显示入侵检测模式
处理建议	无

130 STM

本节介绍 STM（IRF）模块输出的日志信息。

130.1 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].
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：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
举例	STM/4/STM_AUTO_UPDATE_FAILED: Slot 5 auto-update failed. Reason: Timeout when loading.
日志说明	形式一： 在加入IRF时，从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	**156.** 如果失败原因为 Timeout when loading，请检查 IRF 链路是否畅通 **157.** 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 **158.** 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 **159.** 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

130.2 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].
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
举例	STM/5/STM_AUTO_UPDATED_FINISHED: File loading finished on slot 3.
日志说明	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

130.3 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.
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
举例	STM/5/STM_AUTO_UPDATING: Don't reboot the slot 2. It is loading files.
日志说明	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

130.4 STM_LINK_DOWN

日志内容	IRF port [UINT32] went down.
参数解释	$1：IRF端口名
日志等级	3
举例	STM/3/STM_LINK_DOWN: IRF port 2 went down.
日志说明	IRF端口关闭。当绑定的所有物理端口都关闭时，IRF端口关闭
处理建议	检查绑定到IRF端口的物理端口，确保至少有一个物理端口处于UP状态，可以正常工作

130.5 STM_LINK_TIMEOUT

日志内容	IRF port [UINT32] went down because the heartbeat timed out.
参数解释	$1：IRF端口名
日志等级	2
举例	STM/2/STM_LINK_TIMEOUT: IRF port 1 went down because the heartbeat timed out.
日志说明	由于心跳检测超时，IRF端口关闭
处理建议	检查IRF链路是否故障

130.6 STM_LINK_UP

日志内容	IRF port [UINT32] came up.
参数解释	$1：IRF端口名
日志等级	6
举例	STM/6/STM_LINK_UP: IRF port 1 came up.
日志说明	IRF链路可以正常工作
处理建议	无

130.7 STM_MERGE

日志内容	IRF merge occurred.
参数解释	无
日志等级	4
举例	STM/4/STM_MERGE: IRF merge occurred.
日志说明	IRF合并事件发生
处理建议	无

130.8 STM_MERGE_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system needs a reboot.
参数解释	无
日志等级	4
举例	STM/4/STM_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
日志说明	由于本IRF系统在主设备选举中失败，请重启本IRF系统来完成IRF合并
处理建议	登录到本IRF，使用**reboot**命令重启本IRF

130.9 STM_MERGE_NOT_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system does not need to reboot.
参数解释	无
日志等级	5
举例	STM/5/STM_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
日志说明	由于本IRF系统在主设备选举中取胜，无须重启本IRF系统即可完成IRF合并
处理建议	重启对端IRF完成合并

130.10 STM_SAMEMAC

日志内容	Failed to stack because of the same bridge MAC addresses.
参数解释	无
日志等级	4
举例	STM/4/STM_SAMEMAC: Failed to stack because of the same bridge MAC addresses.
日志说明	因为桥MAC地址相同，无法形成IRF
处理建议	检查设备桥MAC地址是否相同

130.11 STM_SOMER_CHECK

日志内容	Neighbor of IRF port [UINT32] cannot be stacked.
参数解释	$1：IRF端口名
日志等级	3
举例	STM/3/STM_SOMER_CHECK: Neighbor of IRF port 1 cannot be stacked.
日志说明	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

131 STP

本节介绍生成树模块输出的日志信息。

131.1 STP_BPDU_PROTECTION

日志内容	BPDU-Protection port [STRING] received BPDUs.
参数解释	$1：接口名
日志等级	4
举例	STP/4/STP_BPDU_PROTECTION: BPDU-Protection port GigabitEthernet1/0/1 received BPDUs.
日志说明	使能了BPDU保护功能的接口收到BPDU报文
处理建议	检查下行设备是否是用户终端，是否存在恶意攻击

131.2 STP_BPDU_RECEIVE_EXPIRY

日志内容	Instance [UINT32]'s port [STRING] received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	5
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.
日志说明	非指定端口因在BPDU超时之前没有收到任何BPDU报文，端口状态发生改变
处理建议	检查上行设备的STP状态及是否存在恶意攻击

131.3 STP_CONSISTENCY_CHECK

日志内容	DR role assignment finished. Please verify that the local device and the peer device have consistent global and DR-interface-specific STP settings.
参数解释	N/A
日志等级	5
举例	STP/5/STP_CONSISTENCY_CHECK: DR role assignment finished. Please verify that the local device and the peer device have consistent global and DR-interface-specific STP settings.
日志说明	确保分布式聚合系统中两台DR设备上生成树全局和DR口上的配置一致
处理建议	无

131.4 STP_CONSISTENCY_RESTORATION

日志内容	Consistency restored on VLAN [UINT32]'s port [STRING].
参数解释	$1：VLAN ID $2：接口名
日志等级	6
举例	STP/6/STP_CONSISTENCY_RESTORATION: Consistency restored on VLAN 10's port GigabitEthernet1/0/1.
日志说明	接口类型不一致或者PVID不一致的保护状态解除
处理建议	无

131.5 STP_DETECTED_TC

日志内容	[STRING] [UINT32]'s port [STRING] detected a topology change.
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
举例	STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.
日志说明	接口所在生成树实例或VLAN拓扑发生变化，本端设备检测到拓扑变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

131.6 STP_DISABLE

日志内容	STP is now disabled on the device.
参数解释	无
日志等级	6
举例	STP/6/STP_DISABLE: STP is now disabled on the device.
日志说明	设备全局去使能了生成树特性
处理建议	无

131.7 STP_DISCARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to discarding state.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	6
举例	STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/0/1 has been set to discarding state.
日志说明	MSTP在计算实例内端口状态，该接口被置为discarding状态
处理建议	无

131.8 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.
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
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.
日志说明	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	通过**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

131.9 STP_ENABLE

日志内容	STP is now enabled on the device.
参数解释	无
日志等级	6
举例	STP/6/STP_ENABLE: STP is now enabled on the device.
日志说明	设备全局使能了生成树特性
处理建议	无

131.10 STP_FORWARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to forwarding state.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	6
举例	STP/6/STP_FORWARDING: Instance 0's port GigabitEthernet1/0/1 has been set to forwarding state.
日志说明	STP在计算实例内端口状态，该接口被置为forwarding状态
处理建议	无

131.11 STP_LOOP_PROTECTION

日志内容	Instance [UINT32]'s LOOP-Protection port [STRING] failed to receive configuration BPDUs.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	4
举例	STP/4/STP_LOOP_PROTECTION: Instance 0's LOOP-Protection port GigabitEthernet1/0/1 failed to receive configuration BPDUs.
日志说明	使能了环路保护功能的接口不能接受BPDU配置报文
处理建议	检查上行设备的STP状态及是否存在恶意攻击

131.12 STP_LOOPBACK_PROTECTION

日志内容	[STRING] [UINT32]'s port [STRING] received its own 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
举例	STP/4/STP_LOOPBACK_PROTECTION: Instance 0's port GigabitEthernet1/0/2 received its own BPDU.
日志说明	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	检查是否有恶意用户伪造BPDU攻击网络或者网络中是否存在环路

131.13 STP_NOT_ROOT

日志内容	The current switch is no longer the root of instance [UINT32].
参数解释	$1：生成树实例编号
日志等级	5
举例	STP/5/STP_NOT_ROOT: The current switch is no longer the root of instance 0.
日志说明	本设备某生成树实例配置为根桥，但它收到比自身更优的BPDU报文后，就不再是此实例的根桥
处理建议	检查桥优先级配置及是否存在恶意攻击

131.14 STP_NOTIFIED_TC

日志内容	[STRING] [UINT32]'s port [STRING] was notified a topology change.
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
举例	STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/0/1 was notified a topology change.
日志说明	远端相连设备通知本设备某接口所在生成树实例或VLAN的拓扑发生变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

131.15 STP_PORT_TYPE_INCONSISTENCY

日志内容	Access port [STRING] in VLAN [UINT32] received PVST BPDUs from a trunk or hybrid port.
参数解释	$1：接口名 $2：VLAN ID
日志等级	4
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.
日志说明	Access接口收到了对端Trunk或Hybrid接口发出的PVST报文
处理建议	检查两端的接口类型配置是否一致

131.16 STP_PVID_INCONSISTENCY

日志内容	Port [STRING] with PVID [UINT32] received PVST BPDUs from a port with PVID [UINT32].
参数解释	$1：接口名 $2：VLAN ID $3：VLAN ID
日志等级	4
举例	STP/4/STP_PVID_INCONSISTENCY: Port GigabitEthernet1/0/1 with PVID 10 received PVST BPDUs from a port with PVID 20.
日志说明	接口收到了PVID不一致的报文
处理建议	检查两端的接口PVID配置是否一致

131.17 STP_PVST_BPDU_PROTECTION

日志内容	PVST BPDUs were received on port [STRING], which is enabled with PVST BPDU protection.
参数解释	$1：接口名
日志等级	4
举例	STP/4/STP_PVST_BPDU_PROTECTION: PVST BPDUs were received on port GigabitEthernet1/0/1, which is enabled with PVST BPDU protection.
日志说明	在MSTP模式下，设备上使能了PVST报文保护功能的端口收到了PVST报文
处理建议	检查其他设备是否发出了PVST BPDU

131.18 STP_ROOT_PROTECTION

日志内容	Instance [UINT32]'s ROOT-Protection port [STRING] received superior BPDUs.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	4
举例	STP/4/STP_ROOT_PROTECTION: Instance 0's ROOT-Protection port GigabitEthernet1/0/1 received superior BPDUs.
日志说明	使能了根保护功能的接口收到了比自身BPDU报文更优的BPDU报文
处理建议	检查桥优先级配置及是否存在恶意攻击

132 SWITCH

本节介绍拨码开关相关的日志信息。

132.1 SWITCH_FLOW_CONTROL

日志内容	The flow-control-switch(switch 1) is turned $1.
参数解释	$1：拨码开关状态 • on：开启 • off：关闭
日志等级	5
举例	SWITCH/5/SWITCH_FLOW_CONTROL: The flow-control-switch(switch 1) is turned on.
日志说明	拨码开关1(流量控制开关)打开
处理建议	无

132.2 SWITCH_BROADCAST_SUPPRESSION

日志内容	The broadcast-suppression-switch(switch 2) is turned $1.
参数解释	$1：拨码开关状态 • on：开启 • off：关闭
日志等级	5
举例	SWITCH/5/SWITCH_BROADCAST_SUPPRESSION: The broadcast-suppression-switch(switch 2) is turned on.
日志说明	拨码开关2（广播抑制开挂）打开
处理建议	无

132.3 SWITCH_LINK_AGGREGATION

日志内容	The link-aggregation-switch(switch 3) is turned $1.
参数解释	$1：拨码开关状态 • on：开启 • off：关闭
日志等级	5
举例	SWITCH/5/SWITCH_LINK_AGGREGATION: The link-aggregation-switch(switch 3) is turned off.
日志说明	拨码开关3（链路聚合开关）关闭
处理建议	无

132.4 SWITCH_RRPP

日志内容	The RRPP-switch(switch 4) is turned $1.
参数解释	$1：拨码开关状态 • on：开启 • off：关闭
日志等级	5
举例	SWITCH/5/SWITCH_RRPP: The RRPP-switch(switch 4) is turned off.
日志说明	拨码开关4（RRPP协议开关）关闭
处理建议	无

133 SYSEVENT

本节介绍系统事件模块输出的日志信息。

133.1 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.
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
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.
日志说明	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	无

134 SYSLOG

本节包含 syslog（信息中心）模块输出的日志消息。

134.1 SYSLOG_LOGFILE_FULL

日志内容	Log file space is full.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_LOGFILE_FULL: Log file space is full.
日志说明	日志空间已满
处理建议	备份日志文件后将其删除，然后根据需要使能端口

134.2 SYSLOG_NO_SPACE

日志内容	Failed to save log file due to lack of space resources.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_NO_SPACE: -MDC=1; Failed to save log file due to lack of space resources.
日志说明	存储介质空间不足，将日志保存到日志文件失败
处理建议	请定期清理存储介质的存储空间，以免影响日志文件功能

134.3 SYSLOG_RESTART

日志内容	System restarted -- [STRING] [STRING] Software.
参数解释	$1：公司名 $2：软件名
日志等级	6
举例	SYSLOG/6/SYSLOG_RESTART: System restarted -- H3C Comware Software
日志说明	系统重启日志
处理建议	无

134.4 SYSLOG_RTM_EVENT_BUFFER_FULL

日志内容	In the last minute, [STRING] syslog logs were not monitored because the buffer was full.
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
举例	SYSLOG/5/SYSLOG_RTM_EVENT_BUFFER_FULL: In the last minute, 100 syslog logs were not monitored because the buffer was full.
日志说明	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	• 找到日志的来源，减少日志的生成 • 使用 **rtm event syslog buffer-size** 命令增大 EAA 监控的日志缓冲区的大小

135 TACACS

本节介绍 TACACS 模块输出的日志信息。

135.1 TACACS_AUTH_FAILURE

日志内容	User [STRING] from [STRING] failed authentication.
参数解释	$1：用户名称 $2：IP地址
日志等级	5
举例	TACACS/5/TACACS_AUTH_FAILURE: User cwf@system from 192.168.0.22 failed authentication.
日志说明	TACACS 服务器了拒绝用户的认证请求
处理建议	无

135.2 TACACS_AUTH_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名称 $2：IP地址
日志等级	6
举例	TACACS/6/TACACS_AUTH_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
日志说明	TACACS 服务器接收了用户的认证请求
处理建议	无

135.3 TACACS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	TACACS/4/TACACS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
日志说明	删除TACACS方案中的服务器失败
处理建议	无

136 TELNETD

本节介绍 TELNETD（Telnet Daemon）模块输出的日志信息。

136.1 TELNETD_ACL_DENY

日志内容	The Telnet Connection [IPADDR]([STRING]) request was denied according to ACL rules.
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
举例	TELNETD/5/TELNETD_ACL_DENY: The Telnet Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	Telnet ACL规则限制登录IP地址。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	无

136.2 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]).
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
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).
日志说明	Telnet登录用户达到上限。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	请根据需要使用命令**aaa session-limit**配置允许的Telnet最大登录用户数

137 TRILL

本节介绍 TRILL 模块输出的日志信息。

137.1 TRILL_DUP_SYSTEMID

日志内容	Duplicate System ID [STRING] in [STRING] PDU sourced from RBridge 0x[HEX].
参数解释	$1：System ID $2：PDU类型 $3：源RBridge的Nickname
日志等级	5
举例	TRILL/5/TRILL_DUP_SYSTEMID: Duplicate System ID 0011.2200.1501 in LSP PDU sourced from RBridge 0xc758.
日志说明	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

137.2 TRILL_INTF_CAPABILITY

日志内容	The interface [STRING] does not support TRILL.
参数解释	$1：接口名称
日志等级	4
举例	TRILL/4/TRILL_INTF_CAPABILITY: The interface GigabitEthernet0/1/3 does not support TRILL.
日志说明	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

137.3 TRILL_LICENSE_EXPIRED

日志内容	The TRILL feature is being disabled, because its license has expired.
参数解释	无
日志等级	3
举例	TRILL/3/TRILL_LICENSE_EXPIRED: The TRILL feature is being disabled, because its license has expired.
日志说明	TRILL的License已经过期
处理建议	请更换有效的License

137.4 TRILL_LICENSE_EXPIRED_TIME

日志内容	The TRILL feature will be disabled in [ULONG] days.
参数解释	$1：功能还可使用的天数
日志等级	5
举例	TRILL/5/TRILL_LICENSE_EXPIRED_TIME: The TRILL feature will be disabled in 2 days.
日志说明	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

137.5 TRILL_LICENSE_UNAVAILABLE

日志内容	The TRILL feature has no available license.
参数解释	无
日志等级	3
举例	TRILL/3/TRILL_LICENSE_UNAVAILABLE: The TRILL feature has no available license.
日志说明	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

137.6 TRILL_MEM_ALERT

日志内容	TRILL process receive system memory alert [STRING] event.
参数解释	$1：内存告警事件的类型
日志等级	5
举例	TRILL/5/TRILL_MEM_ALERT: TRILL process receive system memory alert start event.
日志说明	TRILL从系统收到一个内存告警事件
处理建议	检查系统内存

137.7 TRILL_NBR_CHG

日志内容	TRILL [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
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
举例	TRILL/5/TRILL_NBR_CHG: TRILL 1, Level-1 adjacency 0011.2200.1501 (GigabitEthernet0/1/3), state changed to down.
日志说明	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

138 VCF

本节介绍 VCF Fabric 模块输出的日志信息。

138.1 VCF_AGGR_CREAT

日志内容	Phase [STRING], Device [STRING] created Layer 2 aggregation group [INT32]: member ports=[STRING].
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
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.
日志说明	创建二层聚合组，并将端口加入对应的聚合组
处理建议	无

138.2 VCF_AGGR_DELETE

日志内容	Phase [STRING], Device [STRING] deleted Layer 2 aggregation group [INT32].
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
举例	VCF/6/VCF_AGGR_DELETE: Phase 2.0.6, Device 0000-0000-0000 deleted Layer 2 aggregation group 10.
日志说明	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

138.3 VCF_AGGR_FAILED

日志内容	Phase [STRING], Device [STRING] failed to create Layer 2 aggregation group [INT32].
参数解释	$1：阶段 $2：设备MAC地址 $3：聚合组ID
日志等级	3
举例	VCF/3/ VCF_AGGR_FAILED: Phase 2.0.7, Device 0000-0000-0000 failed to create Layer 2 aggregation group 10.
日志说明	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

138.4 VCF_AUTO_ANALYZE_USERDEF

日志内容	Phase [STRING], Device [STRING] started to parse template file.
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	6
举例	VCF/6/VCF_AUTO_ANALYZE_USERDEF: Phase 1.2.2, Device 0000-0000-0000 started to parse template file.
日志说明	开始解析模板文件中的用户自定义配置
处理建议	无

138.5 VCF_AUTO_NO_USERDEF

日志内容	Phase [STRING], Device [STRING] found undefined variable [STRING] in command [STRING] on line [INTEGER].
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
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.
日志说明	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

138.6 VCF_AUTO_START

日志内容	Phase [STRING], Device [STRING] (Role [STRING]) started VCF automated deployment.
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
举例	VCF/5/VCF_AUTO_START: Phase 1.0.1, Device 0000-0000-0000 (Role leaf) started VCF automated deployment.
日志说明	自动化部署开始
处理建议	无

138.7 VCF_AUTO_STATIC_CMD

日志内容	Phase [STRING], Device [STRING] automatically executed static commands.
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	6
举例	VCF/6/VCF_AUTO_STATIC_CMD: Phase 1.2.4, Device 0000-0000-0000 automatically executed static commands.
日志说明	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

138.8 VCF_BGP

日志内容	Phase [STRING], Device [STRING] established a BGP session with peer [STRING] in AS [INT32].
参数解释	$1：阶段 $2：设备的MAC地址 $3：peer地址 $4：BGP的AS号
日志等级	6
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.
日志说明	VCF成功与对等体建立BGP会话
处理建议	无

138.9 VCF_DOWN_LINK

日志内容	Phase [STRING], Device [STRING] discovered downlink interface [STRING].
参数解释	$1：阶段 $2：设备MAC地址 $3：下行接口名
日志等级	6
举例	VCF/6/VCF_DOWN_LINK: Phase 2.0.8, Device 0000-0000-0000 discovered downlink interface Ten-GigabitEthernet1/0/1.
日志说明	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

138.10 VCF_FAILED_ADD_IRFPORT

日志内容	In phase [STRING], device with MAC address [STRING] add IRF port [STRING] has failed three times.
参数解释	$1：阶段 $2：设备的MAC地址 $3：IRF物理端口
日志等级	4
举例	VCF/4/VCF_FAILED_ADD_IRFPORT: In phase 2.0.10, device with MAC address 4c85-5206-0100 add IRF port GigabitEthernet 1/0/1 has failed three times.
日志说明	设备自动化上线时，设备将IRF物理端口与IRF端口绑定失败三次
处理建议	检查同一IRF端口绑定的IRF物理端口的工作模式是否相同

138.11 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].
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
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.
日志说明	通过模板文件获取新版本的文件名和版本号
处理建议	无

138.12 VCF_GET_TEMPLATE

日志内容	Phase [STRING], Device [STRING] downloaded template file [STRING].
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
举例	VCF/6/VCF_GET_TEMPLATE: Phase 1.2.1, Device 0000-0000-0000 downloaded template file /mnt/flash:/vxlan_spine.template.
日志说明	将自动部署的模板文件下载到本地设备
处理建议	无

138.13 VCF_INSTALL_IMAGE

日志内容	Phase [STRING], Device [STRING] started to install the [STRING] version of startup image.
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
举例	VCF/6/VCF_INSTALL_IMAGE: Phase 1.3.3, Device 0000-0000-0000 started to install the V700R001B70D001 version of startup image.
日志说明	设备开始安装新版本
处理建议	无

138.14 VCF_IRF_FINISH

日志内容	Phase [STRING], Device [STRING] finished IRF configuration: result=[INT32].
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
举例	VCF/5/VCF_IRF_FINISH: Phase 2.0.3, Device 0000-0000-0000 finished IRF configuration: result=0.
日志说明	完成IRF配置下发
处理建议	如果配置下发失败，请联系用服工程师解决

138.15 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].
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
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.
日志说明	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

138.16 VCF_IRF_REBOOT

日志内容	Phase [STRING], Device [STRING] will reboot immediately to activate IRF settings.
参数解释	$1：阶段 $2：本设备的MAC地址
日志等级	5
举例	VCF/5/VCF_IRF_REBOOT: Phase 2.0.4, Device 0000-0000-0000 will reboot immediately to activate IRF settings.
日志说明	VCF完成IRF配置下发后，角色为leaf或access的设备若IRF成员设备编号变化则重启；角色为spine的设备全都要重启
处理建议	无

138.17 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].
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
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.
日志说明	开始下发IRF配置
处理建议	无

138.18 VCF_LOOPBACK_START

日志内容	Phase [STRING], IP address assignment started for [STRING] on other nodes.
参数解释	$1：阶段 $2：接口名称
日志等级	5
举例	VCF/5/VCF_LOOPBACK_START: Phase 3.0.1, IP address assignment started for Loopback0 on other nodes.
日志说明	VCF主节点开始为其他节点的接口分配IP地址
处理建议	无

138.19 VCF_LOOPBACK_START_FAILED

日志内容	Phase [STRING], failed to assign IP addresses to [STRING] on other nodes: reason=[STRING].
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
举例	VCF/5/VCF_LOOPBACK_START_FAILED: Phase 3.0.1, failed to assign IP addresses to Loopback0 on other nodes: reason=-1.
日志说明	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

138.20 VCF_LOOPBACK_ALLOC

日志内容	Phase [STRING], assigned IP [STRING] to [STRING] on Device [STRING]: result=[INT32].
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
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.
日志说明	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

138.21 VCF_LOOPBACK_NO_FREE_IP

日志内容	Phase [STRING], no IP addresses available for Device [STRING].
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	4
举例	VCF/4/VCF_LOOPBACK_NO_FREE_IP: Phase 3.0.4, no IP addresses available for Device 0000-0000-0000.
日志说明	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

138.22 VCF_LOOPBACK_RECLAIM

日志内容	Phase [STRING], reclaimed IP [STRING] from [STRING] on Device [STRING]: reason=[INT32].
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 ○ 1：表示设备 DOWN
日志等级	5
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.
日志说明	VCF收回已经分配出去的接口的IP地址
处理建议	无

138.23 VCF_REBOOT

日志内容	Phase [STRING], Device [STRING] completed startup image update. The device will reboot immediately. Phase [STRING], Device [STRING] will reboot because [STRING].
参数解释	$1：阶段 $2：设备的MAC地址 $3：重启原因，当前仅支持： the IRF member ID changed from [INT] to 1: IRF 成员编号从其他值变为1。
日志等级	5
举例	VCF/5/VCF_REBOOT: Phase 1.3.4, Device 00e0-fc20-6304 completed startup image update. The device will reboot immediately. VCF/5/VCF_REBOOT: Phase 1.2.3, Device 00e0-fc20-6304 will reboot because the IRF member ID changed from 5 to 1.
日志说明	由于完成新版本升级或修改IRF成员编号等原因，VCF模块重启设备
处理建议	无

138.24 VCF_SKIP_INSTALL

日志内容	Phase [STRING], Device [STRING] skipped automatic version update.
参数解释	$1：阶段 $2：设备的MAC地址
日志等级	5
举例	VCF/5/VCF_SKIP_INSTALL: Phase 1.3.2, Device 0000-0000-0000 skipped automatic version update.
日志说明	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

138.25 VCF_STATIC_CMD_ERROR

日志内容	Phase [STRING], Device [STRING] failed to automatically execute static command '[STRING]' in context '[STRING]'.
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
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'.
日志说明	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

138.26 VCF_UP_LINK

日志内容	Phase [STRING], Device [STRING] discovered uplink interface [STRING].
参数解释	$1：阶段 $2：设备MAC地址 $3：上行接口名
日志等级	6
举例	VCF/6/VCF_UP_LINK: Phase 2.0.9, Device 0000-0000-0000 discovered uplink interface Ten-GigabitEthernet1/0/1.
日志说明	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

139 VLAN

本节介绍接口 VLAN 模块输出的日志信息。

139.1 VLAN_CREATEFAIL

日志内容	Failed to create VLAN [STRING]. The maximum number of VLANs has been reached.
参数解释	$1：VLAN ID
日志等级	4
举例	VLAN/4/ VLAN_CREATEFAIL: Failed to create VLAN 1025-4094. The maximum number of VLANs has been reached.
日志说明	因为VLAN硬件资源不足，导致创建VLAN失败
处理建议	无

139.2 VLAN_FAILED

日志内容	Failed to add interface [STRING] to the default VLAN.
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_FAILED: Failed to add interface S-Channel4/2/0/19:100 to the default VLAN.
日志说明	在硬件资源不足的时候创建一个S-Channel接口，此S-Channel接口不能加入到缺省VLAN
处理建议	无

139.3 VLAN_QINQETHTYPE_FAILED

日志内容	Failed to set the TPID value in CVLAN tags to [UINT32] (hexadecimal). The operation is not supported.
参数解释	$1：内层VLAN Tag的TPID值
日志等级	4
举例	VLAN/5/VLAN_QINQETHTYPE_FAILED: Failed to set the TPID value in CVLAN tags to 8200 (hexadecimal). The operation is not supported.
日志说明	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，提示配置未成功
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

139.4 VLAN_VLANMAPPING_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANMAPPING_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组，所以部分或全部VLAN映射配置丢失
处理建议	无

139.5 VLAN_VLANTRANSPARENT_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANTRANSPARENT_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组，所以部分或全部VLAN透传配置丢失
处理建议	无

140 VRRP

本节介绍 VRRP 模块输出的日志信息。

140.1 VRRP_STATUS_CHANGE

日志内容	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
参数解释	$1：VRRP协议版本 $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：虚地址删除 • 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 • Master group drove：管理备份组驱动
日志等级	6
举例	VRRP/6/VRRP_STATUS_CHANGE: The status of IPv4 virtual router 10 (configured on Ethernet0/0) changed (from Backup to Master): Master-down-timer expired.
日志说明	VRRP备份组中的Master或Backup路由器状态发生变化。可能的原因包括：收到接口事件、虚地址删除、Track对象状态变化、收到VRRP报文、当前设备成为地址拥有者、Master down定时器超时、收到0优先级的报文、发生了抢占或者管理备份组驱动
处理建议	检查VRRP备份组中的Master或Backup路由器状态，确保备份组工作正常

140.2 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].
参数解释	$1：VRRP协议版本 $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 $6：VF当前状态 $7：状态变化原因
日志等级	6
举例	VRRP/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.
日志说明	虚拟转发器状态发生改变。可能的原因包括权重变化、定时器超时、VRRP备份组Down
处理建议	检查Track项的状态

140.3 VRRP_VMAC_INEFFECTIVE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
参数解释	$1：VRRP协议版本 $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
日志等级	3
举例	VRRP/3/VRRP_VMAC_INEFFECTIVE: The IPv4 virtual router 10 (configured on Ethernet0/0) failed to add virtual MAC: Insufficient hardware resources.
日志说明	添加虚拟MAC地址失败
处理建议	确定操作失败的根因并解决

141 VSRP

本节介绍 VSRP 模块输出的日志信息。

141.1 VSRP_BIND_FAILED

日志内容	Failed to bind the IP addresses and the port on VSRP peer [STRING].
参数解释	$1：VSRP peer name.
日志等级	6
举例	VSRP/6/VSRP_BIND_FAILED: Failed to bind the IP addresses and the port on VSRP peer aaa.
日志说明	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
处理建议	无

142 VXLAN

本节介绍 VXLAN 模块输出的日志信息。

142.1 VXLAN_LICENSE_UNAVAILABLE

日志内容	The VXLAN feature is disabled, because no licenses are valid.
参数解释	无
日志等级	3
举例	VXLAN/3/VXLAN_LICENSE_UNAVAILABLE: The VXLAN feature is disabled, because no licenses are valid.
日志说明	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

143 WEB

本节介绍 WEB 模块输出的普通日志信息。

143.1 LOGIN

日志内容	[STRING] logged in from [STRING].
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGIN: admin logged in from 127.0.0.1.
日志说明	用户登录成功
处理建议	无

143.2 LOGIN_FAILED

日志内容	[STRING] failed to log in from [STRING].
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGIN_FAILED: admin failed to log in from 127.0.0.1.
日志说明	用户登录失败
处理建议	无

143.3 LOGOUT

日志内容	[STRING] logged out from [STRING].
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGOUT: admin logged out from 127.0.0.1.
日志说明	用户退出登录
处理建议	无

144 WEBAUTH

本节介绍 Web 认证模块输出的日志信息。

144.1 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.
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
举例	WEBAUTH/6/WEBAUTH_USER_LOGON_SUCCESS: -Username=admin-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-AccessVLAN ID=444-AuthorizationVLANID=444; User passed Web authentication and came online successfully.
日志说明	用户通过Web认证，上线成功
处理建议	无

145 WIPS

本节介绍 WIPS 模块输出的日志信息。

145.1 APFLOOD

日志内容	-VSD=[STRING]; AP flood detected.
参数解释	$1：VSD名字
日志等级	5
举例	WIPS/5/APFLOOD: -VSD=home; AP flood detected.
日志说明	指定VSD内检测到AP设备数量过多时触发日志
处理建议	检查是否存在攻击

145.2 AP_CHANNEL_CHANGE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Channel change detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/AP_CHANNEL_CHANGE: -VSD=home-SrcMAC=1122-3344-5566; Channel change detected.
日志说明	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

145.3 ASSOCIATEOVERFLOW

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Association/Reassociation DoS attack detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/ASSOCIATEOVERFLOW: -VSD=home-SrcMAC=1122-3344-5566; Association/Reassociation DoS attack detected.
日志说明	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	检查AP是否受到攻击

145.4 HONEYPOT

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Honeypot AP detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/HONEYPOT: -VSD=home-SrcMAC=1122-3344-5566; Honeypot AP detected.
日志说明	指定VSD内检测到指定AP为蜜罐时触发日志
处理建议	检查是否存在攻击

145.5 HTGREENMODE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; HT-Greenfield AP detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/HTGREENMODE: -VSD=home-SrcMAC=1122-3344-5566; HT-Greenfield AP detected.
日志说明	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	检查是否受到攻击

145.6 MAN_IN_MIDDLE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Man-in-the-middle attack detected.
参数解释	$1：VSD名字 $2：client的地址
日志等级	5
举例	WIPS/5/MAN_IN_MIDDLE: -VSD=home-SrcMAC=1122-3344-5566; Man-in-the-middle attack detected.
日志说明	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	检查client是否受到中间人攻击

145.7 WIPS_DOS

日志内容	-VSD=[STRING]; [STRING] rate attack detected.
参数解释	$1：VSD名字 $2：设备类型 • AP：AP • Client：客户端
日志等级	5
举例	WIPS/5/WIPS_DOS: -VSD=home; AP rate attack detected.
日志说明	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	检查设备是否受到攻击

145.8 WIPS_FLOOD

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] flood detected.
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
举例	WIPS/5/WIPS_FLOOD: -VSD=home-SrcMAC=1122-3344-5566; Association request flood detected.
日志说明	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	检查报文发送者的合法性

145.9 WIPS_MALF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Error detected: [STRING].
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
举例	WIPS/5/WIPS_MALF: -VSD=home-SrcMAC=1122-3344-5566; Error detected: fata jack.
日志说明	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	检查报文发送者的合法性

145.10 WIPS_SPOOF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] detected.
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
举例	WIPS/5/WIPS_SPOOF: -VSD=home-SrcMAC=1122-3344-5566; AP spoofing AP detected.
日志说明	指定VSD内检测到设备仿冒时触发日志
处理建议	检查报文发送者的合法性

145.11 WIPS_WEAKIV

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Weak IV detected.
参数解释	$1：VSD名字 $2：发送者的MAC地址
日志等级	5
举例	WIPS/5/WIPS_WEAKIV: -VSD=home-SrcMAC=1122-3344-5566; Weak IV detected.
日志说明	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

145.12 WIRELESSBRIDGE

日志内容	-VSD=[STRING]-AP1=[MAC]-AP2=[MAC]]; Wireless bridge detected.
参数解释	$1：VSD名字 $2：AP的地址 $3：AP的地址
日志等级	5
举例	WIPS/5/WIRELESSBRIDGE: -VSD=home-AP1=1122-3344-5566-AP2=7788-9966-5544; Wireless bridge detected.
日志说明	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