某局点S7506E 接口下配置包过滤报错的经验案例

ACL packet-filter 张腾 2019-03-24 发表

组网及说明

无

问题描述

接口下配置包过滤调用ACL时报错如下：

[S7506-Ten-GigabitEthernet1/3/0/8]packet-filter 3888 outbound

Failed to apply or refresh IPv4 ACL 3888 rule 0 to the outbound direction of interface Ten-GigabitEthernet1/3/0/8. The resources are insufficient.

过程分析

1、从报错看是ACL资源不足导致配置失败

2、包过滤是在1框3槽的物理接口下发的，通过命令dis qos-acl resource查看对应槽位ACL资源

Interfaces: XGE1/3/0/1 to XGE1/3/0/48 (chassis 1 slot 3)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	768	0	256	75%
IFP ACL	16384	9216	317	6851	58%
IFP Meter	8192	5120	1	3071	62%
IFP Counter	8192	4608	0	3584	56%
EFP ACL	1024	0	556	468	54%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	2	510	0%

具体含义如下：

VFP ACL表示二层转发前的，用于重标记QoS本地ID值功能的ACL资源

IFP ACL表示入方向的ACL资源

IFP Meter表示入方向的流量监管资源

IFP Counter表示入方向的流量统计资源

EFP ACL表示出方向的ACL资源

EFP Meter表示出方向的流量监管资源

EFP Counter表示出方向的流量统计资源

现场在物理接口配置出方向的包过滤，对应EFP ACL资源；

EFP ACL 1024 0 556 468 54%

看到出方向acl资源总共1K，已经使用了556条，还剩下468条；

3、通过 debug qacl show acl-resc chassis 1 slot 3查看1框3槽详细的出方向acl资源占用情况

Acl Hw Resource: **EFP**, Pipe:0

Pri 2, Group 11,usedEntries 2 ,mode Single, physlice 3/

==========

acl type usedEntries[2]

==========

[2]MQC Port 2 //**Ten-GigabitEthernet1/3/0/6口 qos apply policy LT outbound流量统计占了2条出方向资源**

==========

Pri 3, Group 12,usedEntries 554,mode Single, physlice 0/1/2/

==========

acl type usedEntries[554]

==========

[99]PktFilter IP on PORT 554 //**Ten-GigabitEthernet1/3/0/7口 packet-filter 3888 outbound包过滤占了554条出方向资源**

==========

现场想在 Ten-GigabitEthernet1/3/0/8口配置 packet-filter 3888 outbound，与 Ten-GigabitEthernet1/3/0/7配置相同；从1/3/0/7口详细的出方向ACL资源占用情况可以看到，想在1/3/0/8口下发acl 3888同样还需要554条出方向ACL资源；但3槽目前只剩下468条出方向acl资源，所以下发失败；

4、ACL 3888占用的出方向资源是如何计算的：

现场设备版本，结合用的是Packet-Filter outbound方式，具体Packet-Filter outbound 计算方式如下：

配置里ACL 3888 一共354 条rule 规则，其中range rule规则48个，非range数量306个

对于range rule 规则，实际占用Slice资源= 每一条 range rule规则 端口范围，拆分为N步长后，逐条加

入Slice中，比如
rule 1690 permit tcp destination 10.6.2.0 0.0.0.127 destination-port range 5060 5080，就被拆成4条规则存储在Slice中

========
Acl-Type PktFilter IP on PORT, Stage EFP, SinglePort, Installed, Active
Prio Mjr/Sub 264/33, Group 4 [4], Slice/Idx 3/0, Entry 276, Single: 768
ACL GroupNo : 3344, RuleID : 1690 [1]
Rule Match --------
    Out Port: 6
    Dest IP: 10.6.2.0, 255.255.255.128
    IP protocol: tcp
    IP Type: Any IPv4 packet
  L4 Dst Port: 5060, 0xfffc
Actions --------
    Permit
========
Acl-Type PktFilter IP on PORT, Stage EFP, SinglePort, Installed, Active
Prio Mjr/Sub 264/33, Group 4 [4], Slice/Idx 3/1, Entry 277, Single: 769
ACL GroupNo : 3344, RuleID : 1690 [1]
Rule Match --------
    Out Port: 6
    Dest IP: 10.6.2.0, 255.255.255.128
    IP protocol: tcp
    IP Type: Any IPv4 packet
    L4 Dst Port: 5064, 0xfff8
Actions --------
    Permit
========
Acl-Type PktFilter IP on PORT, Stage EFP, SinglePort, Installed, Active
Prio Mjr/Sub 264/33, Group 4 [4], Slice/Idx 3/2, Entry 278, Single: 770
ACL GroupNo : 3344, RuleID : 1690 [1]
Rule Match --------
    Out Port: 6
    Dest IP: 10.6.2.0, 255.255.255.128
    IP protocol: tcp
    IP Type: Any IPv4 packet
    L4 Dst Port: 5072, 0xfff8
Actions --------
    Permit
========
Acl-Type PktFilter IP on PORT, Stage EFP, SinglePort, Installed, Active
Prio Mjr/Sub 264/33, Group 4 [4], Slice/Idx 3/3, Entry 279, Single: 771
ACL GroupNo : 3344, RuleID : 1690 [1]
Rule Match --------
    Out Port: 6
    Dest IP: 10.6.2.0, 255.255.255.128
    IP protocol: tcp
    IP Type: Any IPv4 packet
  L4 Dst Port: 5080, 0xffff
Actions --------
    Permit

因此Packet-Filter outbound ACL 3888资源应该= （非range数量306）+（48条range 规则分别拆分存储占用Slice数量）=554条；

解决方法

1、从ACL资源分布情况可以看到，设备或单板的**入方向ACL**资源是远大于**出方向ACL资源**的，可以在1框3槽的入接口调用入方向包过滤；

Type Total Reserved Configured Remaining Usage

VFP ACL 1024 768 0 256 75%

IFP ACL	**16384**	9216	317	6851	58%
IFP Meter	8192	5120	1	3071	62%
IFP Counter	8192	4608	0	3584	56%
EFP ACL	**1024**	0	556	468	54%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	2	510	0%

2、根据情况优化ACL rule规则，减小条目数，工程量较大；

3、现场其它槽位单板剩余的出方向ACL资源和接口满足条件，在其它槽位配置；