ACL 资源不足怎么办

文档版本 01

发布日期 2021-09-18

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 简介

很多业务都会使用ACL资源，而CloudEngine 系列交换机的ACL资源是有限的，所以当ACL资源不足时，使用ACL资源的业务就会下发失败。

因为ACL资源不足是现网中很常见的问题，与此同时，ACL资源的原理很难理解，解决ACL资源不足的问题也很困难。因此本文档将对ACL资源不足的原因、使用ACL资源的业务、以及如何预判业务是否会下发成功进行简单的介绍。

本文档可以使用户对ACL资源有初步的了解，如果希望有更加深入的研究可以查看**ACL技术专题**。

2 ACL 资源不足的原因

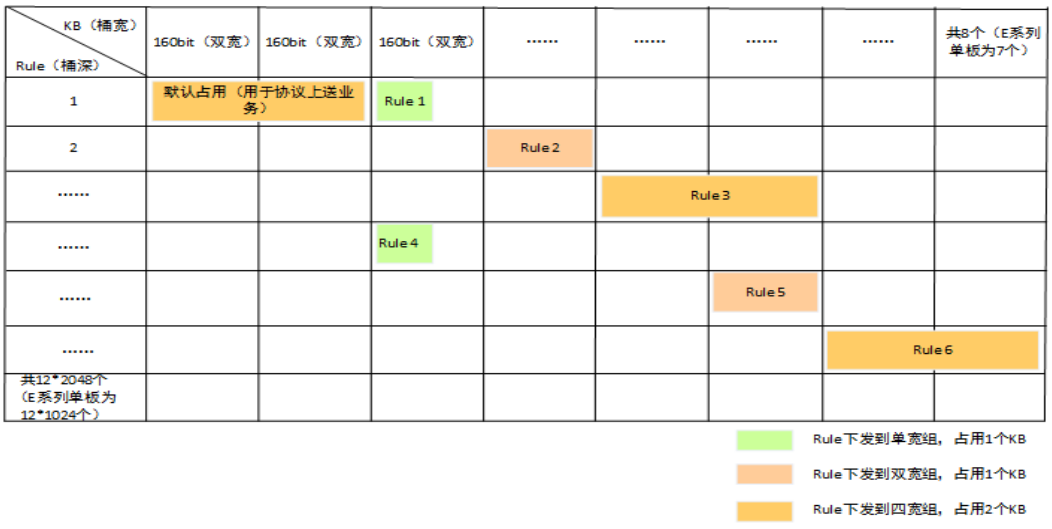
在现网中，用户往往仅配置了少量规则Rule，远没有达到Rule的规格，但是设备就会报ACL资源不足。这是为什么呢？因为Rule资源仅仅是ACL资源的一种，而ACL资源的瓶颈在于KB资源。

使用ACL资源的业务要想正常运行必须首先成功下发到Group中。设备会预定义很多Group，但Group一开始是未被创建的，可以理解为Group为空，不能用以下发业务。只有在配置ACL业务时才会开始创建Group，Group创建时需要申请KB资源，如果KB资源充足，Group就会创建成功后，才能用以下发业务。Group可以分为单宽组、双宽组和四宽组。其中单宽组和双宽组需要占用一个KB，四宽组需要占用两个KB。

另外多种业务可以下发到同一个Group中，当配置新业务时，如果已经创建的Group满足要求，业务可以直接下发到已创建的Group中，此时便无需占用额外的KB资源。如果已创建的Group无法满足要求，则需要再申请KB资源创建新的Group。

因此在实际配置过程中，虽然规则Rule是用户接触最多也最直观的资源，但是业务能否下发成功的关键还在于用以创建Group的KB资源是否充足。为了更好的理解，我们以CE12800设备为例，并通过如下表格来简单地介绍下ACL原理。

图 2-1 ACL 资源原理



表格的行数为桶深，表示Rule的规格，表格的列数为桶宽，表示KB的规格，其中桶宽为业务能否下发成功的瓶颈。

如果一条Rule匹配字段的总和不超过80bit（例如匹配源IP地址和目的IP地址，因为IP地址为32bit，那么匹配字段总和就是64bit，其他字段的长度，即在报文中占用的位数请参考相关产品文档），则会选择单宽组并占用一个KB；如果一条Rule匹配字段的总和为80到160bit之间，则会选择双宽组并占用一个KB；如果一条Rule匹配字段的总和超过160bit，则会选择四宽组并占用两个连续的KB。

例如用户配置如下规则Rule：

Rule 1：rule permit tcp source 1.1.1.1 24 destination 1.1.2.2 24

Rule 2：rule permit tcp source 1.1.1.1 24 destination 1.1.2.2 24 source-port eq 1 destination-port eq 10

Rule 3：rule permit tcp source 1.1.1.1 24 destination 1.1.2.2 24 source-port eq 1 destination-port eq 10 tcp-flag ack ttl-expired tos 2 precedence 5 logging

如**图2-1**所示，协议报文的上送会默认占用两个KB。Rule 1下发到单宽组中占用一个KB，Rule 2下发到双宽组中占用一个KB，Rule 3下发到四宽组中占用两个连续的KB。此外，多条Rule也可以占用相同的KB，如Rule 4和Rule 1所示。

假设后续再配置Rule 5、Rule 6，8个KB资源全部被占用，如果继续配置新业务，而且已创建的Group又无法满足条件时，因为已经没有KB资源去创建新的Group，此时即便Rule的条数远远没有达到规格，设备也会提示ACL资源不足导致业务下发失败。

这里有一个关键问题就是Group中到底有哪些内容，怎么判断已经创建的Group是否满足配置的新业务，下一个章节将继续介绍。

3 使用 ACL 资源的业务

通过上面的章节我们已经简单的了解了ACL的基本原理和ACL资源不足的原因。但是在现网中，用户在没有直接配置ACL规则Rule的情况下也会出现ACL资源不足的情况。这又是为何呢？通过本节使用ACL资源的业务的介绍，可以为您解答这个疑惑。

ACL功能非常强大，一方面用户可以直接配置基于ACL规则的MQC实现针对不同业务的差分服务，另一方面很多业务的功能实现也是依赖内部下发ACL完成的。比如VLAN流量统计业务，需要下发ACL针对相应VLAN的流量进行统计。IPv4、IPv6、MPLS、TRILL、VXLAN等相关特性的业务，基本都与ACL有着不可分割的联系。

根据用户对使用ACL的感知情况，当前业务分为显式使用ACL的业务和隐式使用ACL的业务。例如当用户配置MQC时，会配置ACL规则，所以属于显式使用ACL的业务；当用户使能VLAN流量统计业务时，虽然会下发用于处理VLAN流量统计的ACL，但是用户没有直观的感知，所以就属于隐式使用ACL的业务。

上章节我们说过，使用ACL资源的业务正常运行需要先下发到Group中，设备预定义的Group有很多，并不是所有的Group都满足业务要求，满足业务要求的Group占用的ACL资源也不一样，那么怎么选择合适的Group呢？选择Group的过程，我们称之为选组。

选组方式有两种：一种是静态选组，即业务使用的ACL规则使用哪个分组是固定的，选组时直接选择对应分组，隐式使用ACL的业务都属于此方式；另一种是动态选组，即需要根据用户配置的字段、执行的动作以及应用的视图信息去遍历预定义好的分组模板，找到一个合适的分组，该选组方式则主要用于MQC业务。

下面分别以一个简单的例子对两种选组方式进行说明。

隐式业务静态选组：

流量统计功能是常用的维护功能，是使用ACL实现的。例如需要统计从VLAN进来的流量可以执行如下命令：

```
#
vlan 10
 statistics enable
#
```

使能VLAN流量统计后会下发ACL规则：匹配VLAN 10，动作为统计。

可以通过命令**display system tcam service brief** [**slot** *slot-id*] 查看到VLAN统计业务已经成功下发到编号为11的Group中。

```
[~HUAWEI] display system tcam service brief slot 1
Slot: 1
```



```
-------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage         ServiceName                Count
       (FEI/FE)
-------------------------------------------------------------------------------
   0     2/2     Quadruple  Ingress       BPDU Deny                    21
         2/2     Quadruple  Ingress       CPCAR                         5
         2/2     Quadruple  Ingress       L2 Protocol Tunnel            1
         3/3     Quadruple  Ingress       App-Session                   3
         3/3     Quadruple  Ingress       CPCAR                        23
        11/1      Single     Ingress      VLAN Statistics               1
-------------------------------------------------------------------------------
```

MQC业务动态选组：

以配置MQC允许从VLANIF 10进来的特定TCP报文通过为例：

配置acl 3000

```
#
acl number 3000
 rule 5 permit tcp source 1.1.1.1 0 source-port eq 2048 destination 1.1.1.2 0 destination-port eq 1024
 rule 10 deny tcp
#
```

配置流分类，匹配acl 3000

```
#
traffic classifier c_example type or
 if-match acl 3000
#
```

配置流行为，动作为统计

```
#
traffic behavior b_example
 statistics enable
#
```

配置流策略

```
#
traffic policy p_example
 classifier c_example behavior b_example precedence 5
#
```

在VLANIF 10视图下应用流策略

```
#
interface vlanif10
 traffic-policy p_example inbound
#
```

在流策略p_example中，流分类c_example匹配的acl 3000里配置的字段为IP五元组，流行为b_example里配置的动作为统计，应用视图为VLANIF，在选择Group时，会根据这些匹配字段、动作和应用视图遍历所有预定义的MQC Group模板，选择能够包含上述条件且占用资源最少的Group模板。例如遍历如下预定义MQC Group模板，最终选择Group 216。

表 3-1 MQC 业务动态选组

Group ID	KB个数	报文格式	匹配条件	动作	应用视图	备注
213	1	IPv4	IP五元组	丢弃 | 重定向 | 镜像 | remark (local-precedence | dscp)	接口/VLAN	由于不包含统计动作和VLANIF视图，不选择该分组
214	1	IPv4	IP五元组	丢弃 | 重定向 | 限速	接口 / VLAN	由于不包含统计动作和VLANIF视图，不选择该分组
216	1	IPv4	**IP五元组**，TCP Flag	丢弃 | 重定向 | **统计**	接口 / VLAN/ **VLANIF**	匹配条件、动作和视图均满足要求，且仅占用一个KB资源，选择该分组
233	2	IPv4	IP五元组，TOS，TTL，TCP-Flag	丢弃 | 重定向 | 统计 | remark (local-precedence | dscp)	接口 / VLAN/ VLANIF/ 全局	消耗2个KB资源，不是最佳选项，不选择该分组

执行命令**display traffic-policy applied-record**查询流策略p_example应用成功：

```
[~HUAWEI] display traffic-policy applied-record
Total records : 1
-------------------------------------------------------------------------------
Policy Type/Name          Apply Parameter          Slot   State
p_example                 Vlanif10 inbound         1   success
                                                   2   success
                                                   3   success
                                                   4   success
-------------------------------------------------------------------------------
```

执行命令**display system tcam service brief** [**slot** *slot-id*]查看到MQC业务Traffic Policy VLANIF下发到Group 216中：

```
[~HUAWEI] display system tcam service brief slot 1
Slot: 1
-------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                Count
```



```
     (FEI/FE)
-------------------------------------------------------------------------------
  0     2/2     Quadruple  Ingress      BPDU Deny                    21
        2/2     Quadruple  Ingress      CPCAR                     5
        2/2     Quadruple  Ingress      L2 Protocol Tunnel           1
        3/3     Quadruple  Ingress      App-Session                1
        3/3     Quadruple  Ingress      CPCAR                    23
       216/1     Double     Ingress      Traffic Policy VLANIF        2
-------------------------------------------------------------------------------
```

至此可以看到，一个基于五元组、动作为统计、在VLANIF接口下应用的MQC业务，下发到Group 216 中。

根据**表3-1**，如果后续继续配置其他MQC业务，例如基于五元组、动作为**重定向**、在VLANIF接口下应用的MQC1业务，因为已经创建的Group 216中同样支持重定向动作，所以MQC1业务也会下发到Group 216中，不需要往外占用KB资源；如果配置基于五元组、动作为**限速**、在VLANIF接口下应用的MQC2业务，因为已经创建的Group 216中不支持限速，所以MQC2业务无法下发到Group 216中，此时需要创建新的Group，并占用更多的KB资源。假设此时KB资源已经耗尽，MQC2业务便会应为资源不足而下发失败。

4 ACL 资源不足的解决方法

如果显示业务可以下发成功，则可以正常配置业务。如果显示业务下发失败，则可以调整业务部署方式继续采用预判工具进行查询。

如果通过预判工具，业务始终无法下发成功，此时需要对ACL资源有更加深入的研究，请参考**ACL技术专题**，或直接联系华为技术支持人员。

5 相关信息

CloudEngine 12800, 12800E, 8800, 7800, 6800, 5800系列交换机 ACL技术专题

CloudEngine 12800, 12800E V200R005C10 ACL配置指南

