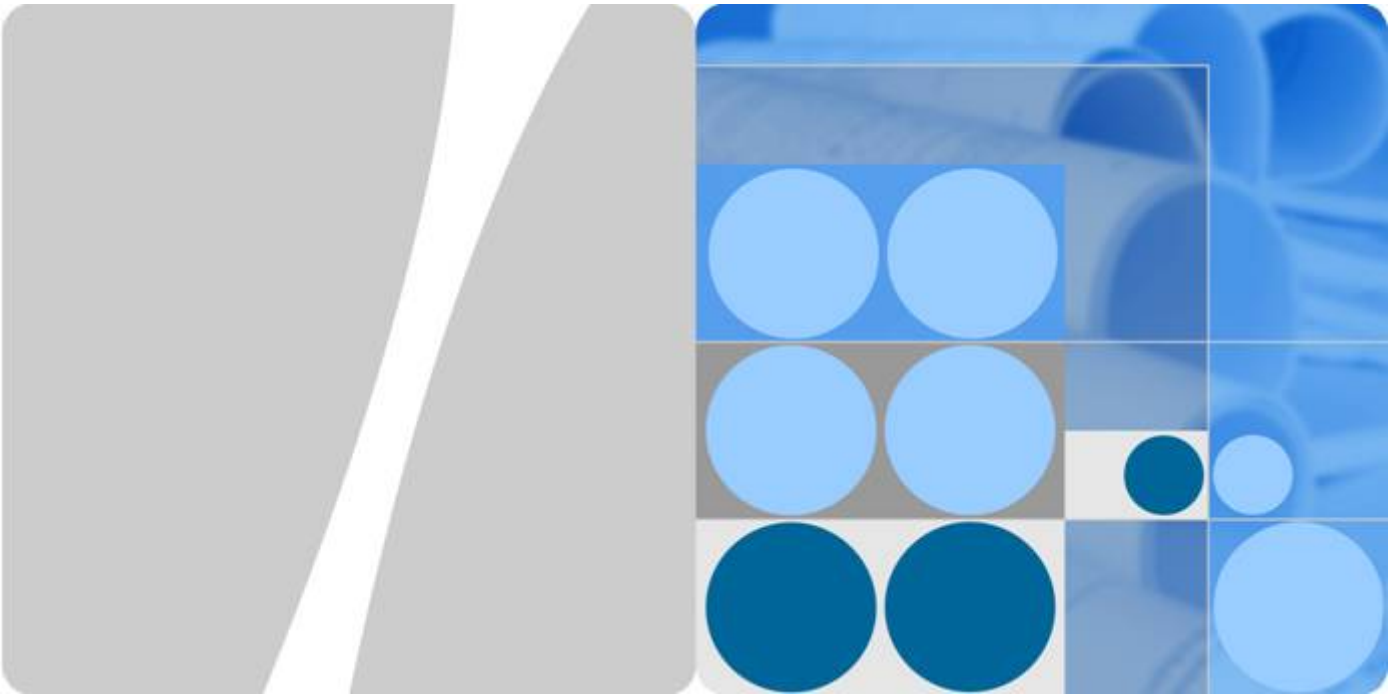


CloudEngine 12800, 12800E, 8800, 7800, 6800, 5800 系列交换机

ACL 技术专题

文档版本　07

发布日期　2018-10-18

华为技术有限公司

HUAWEI

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默示的声明或保证。

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： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 ACL 资源原理

该文档不适用于安装ED-E/EG-E/EGA-E系列单板的CE12800E、CE5880EI和CE6880EI。文档中命令的回显如果没有特别说明都以V200R002C50版本为例。

1.1 简介

在现网中，用户往往仅配置了少量规则Rule，还远没有达到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。

当业务下发时，业务会首先选择一个Group，然后再申请所需要的KB资源。只有KB资源充足，Group创建成功后，业务才可以正常运行。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。

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，而无需占用额外的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。

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。

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），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，且要求KB的起始编号必须为偶数。

例如：

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

如上表格所示，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KB，另外设备默认占用两个KB用于协议报文的上送。

假设后续再配置Rule 4 、Rule 5、Rule 6、Rul4 7、Rul4 8后，8个KB资源全部被占用。如果继续配置新业务，而已创建的Group又无法满足条件时，因为已经没有KB资源去创建新的Grp，所以设备就会提示ACL资源不足导致业务下发失败。

1.2 ACL 资源原理（CE12800 和 CE6870）

说明

章节中描述的Block也称为Bank或slice。

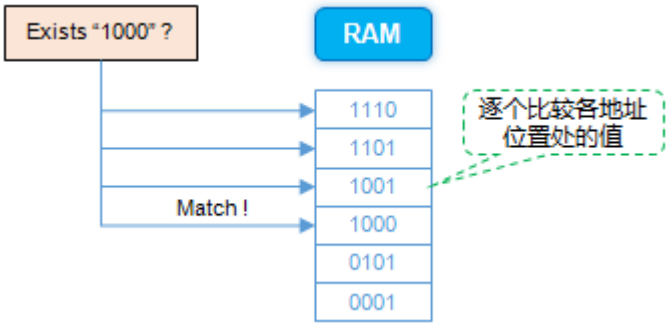
仅CE12800支持外扩TCAM单板。

1.2.1 ACL 基本概念

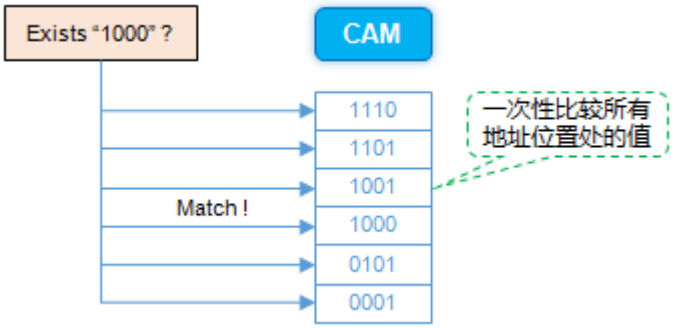
在开始CE系列交换机的ACL业务特性及编程能力描述之前，先了解ACL实现相关的几个关键概念：TCAM、ACL、MQC。

1.2.1.1 什么是 TCAM

在TCAM出现之前，用于存放ACL规则的存储器是RAM(Random Access Memory)，也就是随机访问存储器。对于查找而言，RAM是从某个地址开始依次比较，直到匹配到某个值或者查询完为止。整个查找过程是多次查找，速度较慢。



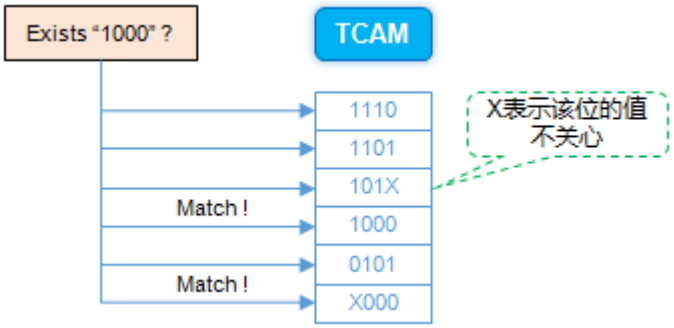
为了提高查找效率，就出现了CAM(Content Addressable Memory)，即内容可寻址存储器。顾名思义，CAM的查找是基于内容的，输入一个值，如果CAM中存在该值，就会输出该值所在的地址。CAM是一次性全部查找，速度非常快。



从上可以看出，RAM和CAM的本质区别在于，RAM是由地址得到数据，而CAM是由数据得到地址。上图中，对存放同样数据的RAM和CAM进行查找，RAM是依次比较，CAM是立即查找所有匹配项。

TCAM(Ternary Content Addressable Memory)，是CAM的升级版，采用掩码匹配。掩码，即用1来对应我们关心的数据，用0来对应不关心的数据。

如下图所示，TCAM中的值是由掩码和数据相与产生的，当掩码为0时，TCAM中的值为X，此时可以与1000中的相应位进行模糊匹配，即无论相应位是0还是1都可以匹配上；当掩码为1时，TCAM中的值为相应的数据，此时需要与1000中的相应位进行精确匹配。这样实际上数据就可以有三种值：0、1和X。

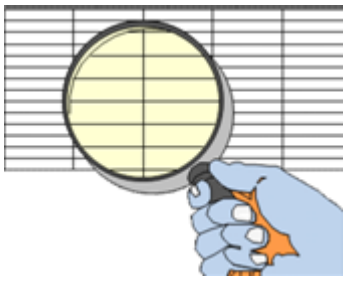


在上面的例子中，1000就是查找KEY，用来查找TCAM中的多条规则：entry 0 = {1110}，entry 1 = {1101}，entry 2 = {101X}，entry 3 = {1000}，entry 4 = {0101}，entry

5 = {X000}，可以匹配上的规则entry 3和entry 5。若有多个entry被命中，则TCAM采取最低索引的命中表项，即命中的entry 3生效。

1.2.1.2 什么是 ACL

ACL是Access Control List的简称，中文是访问控制列表。顾名思义，ACL就是一张表。



ACL表中包含了一系列的规则(rule)，如下列在设备上配置的ACL规则。

```
#
acl number 3000
 rule 5 permit ip source 1.1.1.1 0
 rule 10 permit ip source 1.1.1.2 0
 rule 15 deny ip destination 2.2.2.0 0.0.0.255
 rule 20 deny igmp
 rule 25 deny udp destination-port eq 255
 rule 30 permit tcp source-port eq 6550
#
```

简单来说，ACL其实是人为定义的一组或几组规则，以便设备判断是否执行用户指定的动作。抽象来说，通过ACL，可以对报文进行分类，将具有某类共同特征的报文划分为一类，来为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

按照ACL功能，ACL可以分为如下几类：

分类	适用的IP版本	功能介绍	说明
基本ACL	IPv4	可使用IPv4报文的源IP地址、分片标记和时间段信息来定义规则。	基本IPv4 ACL简称基本ACL。编号范围为2000～2999。
高级ACL	IPv4	既可使用IPv4报文的源IP地址，也可使用目的地址、IP优先级、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP（User Datagram Protocol）源端口/目的端口号等来定义规则。	高级IPv4 ACL简称高级ACL。编号范围为3000～3999。
二层ACL	IPv4&IPv6	可根据报文的以太网帧头信息来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、以太帧协议类型等。	编号范围为4000～4999。
用户自定义ACL	IPv4&IPv6	可根据偏移位置和偏移量从报文中提取出一段内容进行匹配。	编号范围为5000～5999。

分类	适用的IP版本	功能介绍	说明
基于ARP的ACL	IPv4	基于ARP的ACL根据ARP报文的源/目的IP地址、源/目的MAC地址定义规则，实现对ARP报文的匹配过滤。	编号范围为23000～23999。
基本ACL6	IPv6	可使用IPv6报文的源IP地址、分片标记和时间段信息来定义规则。	基本IPv6 ACL简称基本ACL6。编号范围为2000～2999。
高级ACL6	IPv6	可以使用IPv6报文的源地址、目的地址、IP承载的协议类型、针对协议的特性（例如TCP的源端口、目的端口、ICMPv6协议的类型、ICMPv6 Code）等内容定义规则。	高级IPv6 ACL简称高级ACL6。编号范围为3000～3999。

1.2.1.3 什么是 MQC

为了简化用户的ACL配置，并支持ACL配置的灵活性，CE系列交换机提供了模块化QoS命令行MQC(Modular QoS Command-Line Interface)。

下列显示了一个通过MQC命令行配置的流策略，该流策略规则对DstMac=0000-1111-2222和SrcIp=1.1.1.1的报文，进行流量统计和流量监管动作。

```
#
acl number 3000
 rule 5 permit ip source 1.1.1.1 0
#
traffic classifier demo type and
 if-match destination-mac 0000-1111-2222 ffff-ffff-ffff
 if-match acl 3000
#
traffic behavior demo
 statistics enable
 car cir 100 kbps
#
traffic policy demo
 classifier demo behavior demo precedence 5
#
```

从以上可以看出，MQC命令行形式有3个要素：流分类(traffic classifier)、流行为(traffic behavior)、流策略(traffic policy)。

具体配置可以参考CE系列交换机产品文档-QoS业务配置-MQC业务配置。

在配置好MQC流策略后，就可以将流策略应用到全局、slot、接口、子接口、VLAN、VPN实例、VSI实例、BD等视图上。

应用时，可以指定流策略需要应用的方向。其中inbound表示入方向、outbound表示出方向。如下列将流策略demo-PORT应用到接口40GE2/0/1的入方向上。

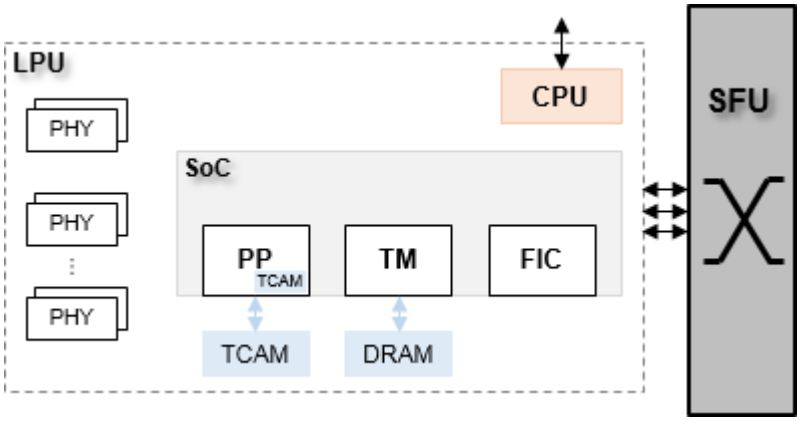
```
#
interface 40GE2/0/1
 traffic-policy demo-PORT inbound
#
```


1.2.2 报文转发原理

为便于更好地理解ACL的实现，这里先描述下单板的硬件逻辑，以及报文在转发芯片里的处理流程。熟悉报文转发流程的实现，有助于更好地掌握如何应用ACL、在哪个阶段应用ACL、应用ACL时所需的转发芯片资源。

1.2.2.1 单板硬件逻辑

LPU单板硬件框图如下所示。



几个关键的硬件处理单元为：

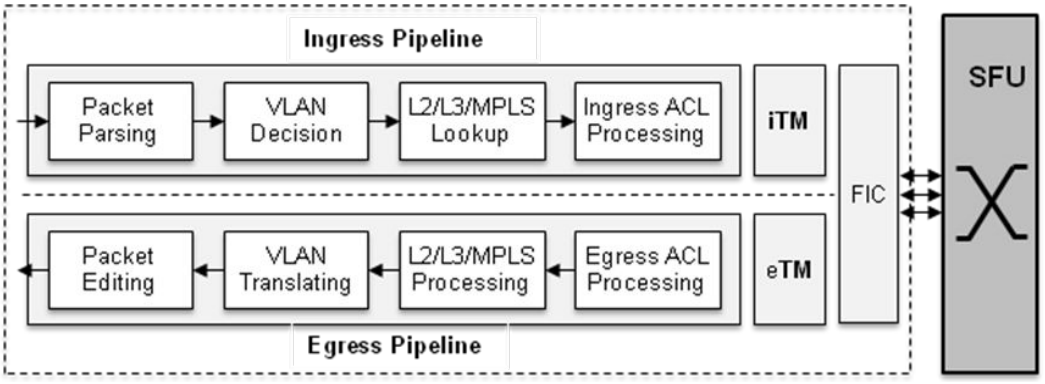
CPU	单板的CPU	负责本地管理和主控板通信。处理控制信令(如协议报文的上送和下发)、表项转换与下发到转发芯片。
PP	Packet Processor	报文处理器，负责数据报文的处理(包括选路、编辑和发送等)。
TM	Traffic Manager	流量管理单元，负责大缓存队列的管理及报文入队调度等工作。
FIC	Fabric Interface Card	交换网接口单元，负责报文到交换网的选路和调度，信元拆分/重组等工作。
PHY	Ethernet PHY	PHY芯片，负责数据的线路编码和数模转换，对应OSI 7层模型的物理层功能。
DRAM	单板外扩DRAM	用于存储报文内容。
TCAM	单板外扩TCAM	用于存储路由、ACL等表项。

单板使用的SoC转发芯片，内置了报文处理所需的各个处理单元：PP、TM、FIC。SoC芯片内置了TCAM存储单元，部分单板同时也外扩了TCAM器件，以支持大规格的路由、ACL的部署场景。

当然，部分单板采用了多个SoC芯片，以支持更大密度的端口数量和更大的端口带宽。上图中，只示意了一个SoC芯片以作说明。

1.2.2.2 芯片转发流程

报文的转发处理由SoC芯片内置的PP、TM、FIC等逻辑模块负责，其对报文基本的处理流程如下。

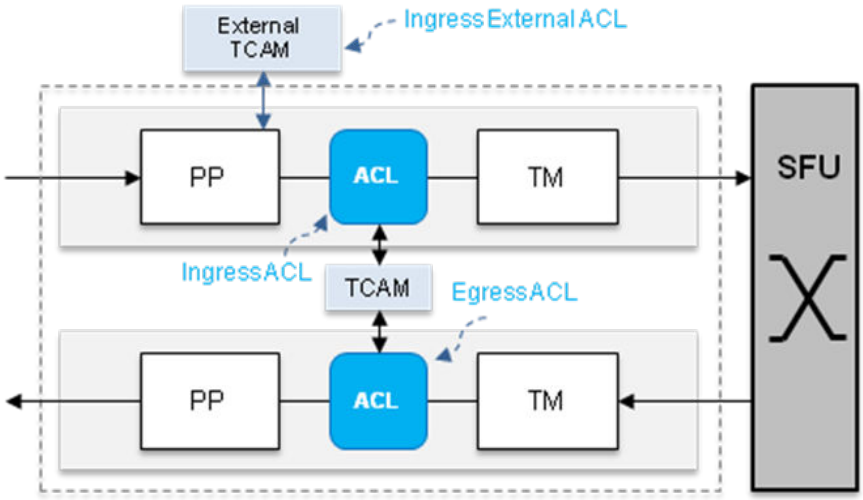


阶段流程	描述
Packet Parsing	解析报文的前128字节以获取各层次的报文头字段。
VLAN Decision	基于端口、VLAN、流等添加或修改VLAN Tag，并进行VLAN/STP检查。
L2/L3/MPLS Lookup	执行L2、L3、MPLS流程的转发表项查找。
Ingress ACL Processing	上行ACL查找，执行流过滤、QoS分类、策略路由等。
Ingress TM	负责上行队列管理和报文入队、流量调度等工作。
FIC & SFU	把报文切分成多个信元，通过SFU交换网板交换，并重组成报文。
Egress TM	负责下行方向的流量调度。
Egress ACL Processing	下行ACL查找，执行流过滤、报文重标记等。
L2/L3/MPLS Processing	下行隧道封装、L3头修改、L2头封装的信息处理。
VLAN Translating	下行VLAN映射变换、VLAN/STP检查等。

阶段流程	描述
Packet Editing	对报文执行所有的编辑、修改、封装动作。

1.2.2.3 ACL 处理阶段

根据上述的报文转发流程， ACL处理阶段如下图所示。



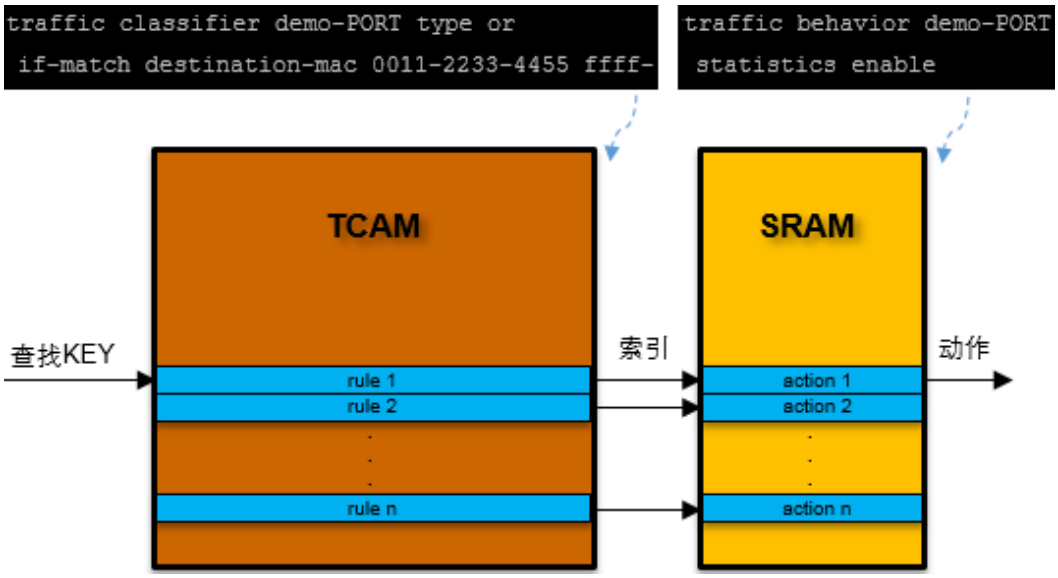
当用户通过MQC命令行配置流策略(traffic policy)时，根据流策略所绑定的出入方向(inbound/outbound)，来决定相应的ACL规则下发到哪个ACL阶段。

ACL阶段	描述
Ingress ACL	用户配置入方向的流策略时，规则下发到Ingress ACL阶段。
Ingress External ACL	对于外扩TCAM单板，若用户配置的外扩TCAM资源划分模板包含ACL表项，则配置入方向的流策略时，规则下发到Ingress External ACL阶段。
Egress ACL	用户配置出方向的流策略时，规则下发到Egress ACL阶段。

上图中可以看出，Ingress ACL阶段和Egress ACL阶段共享SoC芯片内置的TCAM存储单元。

1.2.2.4 ACL 规则存储

在用户配置MQC流策略并提交后，就将对应的各个ACL规则下发到转发芯片里。ACL规则在转发芯片TCAM里的存储形式如下所示。



从MQC配置命令行可以看出，一条ACL规则是由流分类classifier、以及流行为behavior构成。classifier为规则rule，存放在转发芯片内置的TCAM存储单元里，而behavior为规则执行的动作，存放在转发芯片内置的SRAM存储单元里。

转发芯片内置了一定容量的TCAM和SRAM存储单元，这些存储容量也就决定了用户能下发的总的ACL规则数量。

TCAM的特点是，在众多的ACL规则中，只能命中1条ACL规则。即使有多个ACL规则能被同时命中，TCAM器件也只选取命中索引最低的ACL规则，并执行其对应的动作。然而，在实际业务部署中，通常会出现一个报文需要同时命中多个视图的流策略规则的情形。

比如在40GE2/0/1接口配置了入方向的MQC流策略，对特定目的MAC地址的报文进行流量统计。

```
#
traffic classifier demo-PORT type or
 if-match destination-mac 0011-2233-4455 ffff-ffff-ffff
#
traffic behavior demo-PORT
 statistics enable
#
traffic policy demo-PORT
 classifier demo-PORT behavior demo-PORT precedence 5
#
interface 40GE2/0/1
 traffic-policy demo-PORT inbound
#
```

同时又在VLAN 100配置了入方向的MQC流策略，对特定802.1p的报文进行优先级重标记。

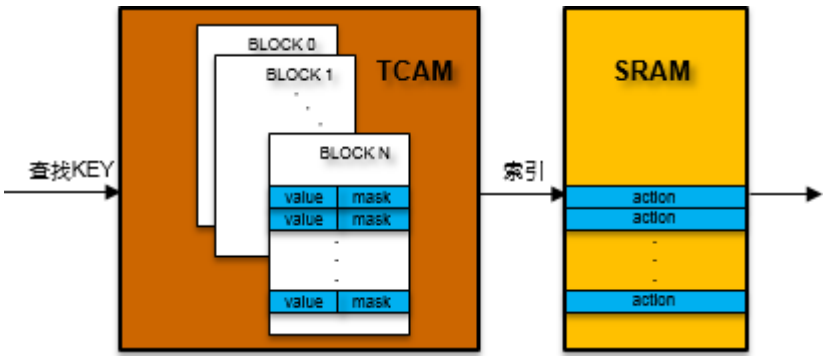
```
#
traffic classifier demo-VLAN type or
 if-match 8021p 6
#
traffic behavior demo-VLAN
 remark local-precedence af2
#
traffic policy demo-VLAN
 classifier demo-VLAN behavior demo-VLAN precedence 5
#
vlan 100
```



```
 traffic-policy demo-VLAN inbound
#
```

若一个目的MAC地址为0011-2233-4455、所属VLAN为100、802.1p为6的报文从40GE2/0/1接口进入，则会同时命中上述接口视图和VLAN视图下的MQC流策略。

为支持这样的应用场景，转发芯片把内置的TCAM划分成多个小的TCAM Block（Block又叫做bank或slice）。每个TCAM Block都可以命中1条ACL规则，一个报文可以同时并行查找多个TCAM Block，从而可以命中多个流策略，如下图所示。图中，rule以value/mask的形式存放在TCAM中。



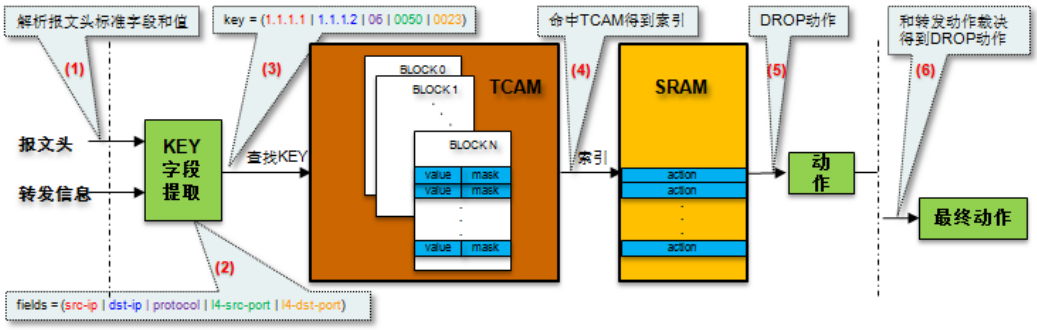
对于外扩TCAM单板类型，存放到外扩TCAM里的ACL规则存放形式和内置TCAM一样。

1.2.3 ACL 查找实现

上文描述了ACL的基本概念和报文转发处理流程。在清楚了ACL的功能和实现之后，下文重点描述ACL查找流程及相关的芯片资源。

1.2.3.1 ACL 查找流程

在ACL规则下发到转发芯片里的TCAM存储单元后，报文进入时，转发芯片根据报文的相关字段信息来查找用户配置下发的ACL规则。

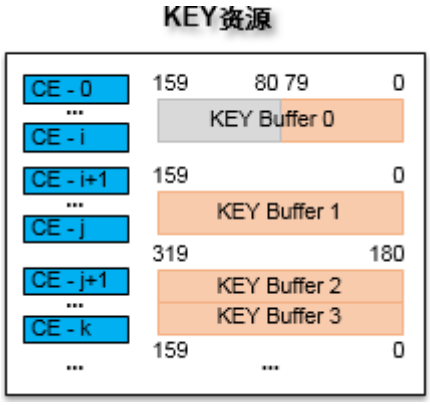


上图显示了转发芯片的ACL规则查找流程，具体如下表所示。

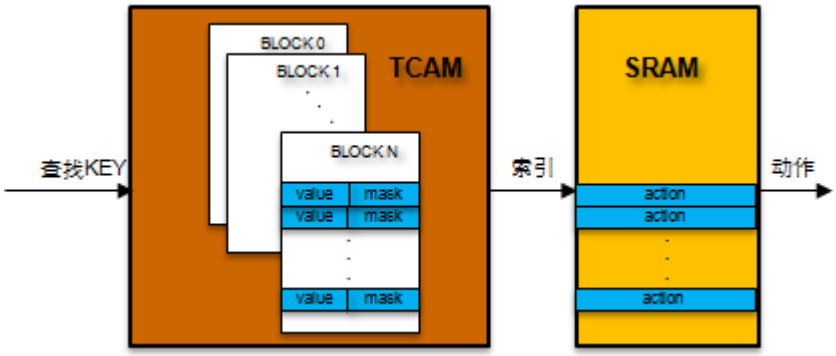
查找流程	步骤描述
字段解析	从报文头和转发信息里，解析所需的匹配字段对应的位段。
字段值提取	根据匹配字段解析的位段，提取对应位置的值。

查找流程	步骤描述
查找KEY构建	根据提取的各个匹配字段的值，来构建查找TCAM所需的KEY。
发起TCAM查找	将构建的查找KEY发给TCAM Block，命中时得到对应的ENTRY的索引。
获取动作	根据TCAM命中的索引，来访问对应命中ENTRY的各个动作。
动作冲突裁决	命中的ACL的动作可能会和之前的转发流程的动作冲突，需要进行一次裁决。

在查找TCAM里的ACL规则之前，需要构建查找KEY。查找KEY根据报文的各层头字段、以及报文在芯片里的转发信息(如转发类型、下一跳索引、出接口等)来构建。KEY构建是整个ACL查找流程的关键步骤，涉及转发芯片内部的ACL资源，包括提取报文字段的Copy Engine（CE）资源、构建查找KEY的KEY Buffer（KB）资源，如下图所示。



构建好查找KEY后，就发起TCAM查找命令到相应的各个TCAM Block。各个TCAM Block若有ACL规则命中，则根据命中的索引，进一步访问该命中规则在SRAM里的动作。



转发芯片在获取所有命中规则的动作后，综合查找ACL之前的报文转发动作，进行一次动作裁决，裁决后的动作为报文最终的转发动作。

当报文命中多条规则时，每条规则的动作可能不一样，此时最终执行的动作需要经过裁决，具体按照如下原则：

1、当多个规则在同一个分组时，无论规则对应的动作是否冲突，仅执行优先级最高的规则对应的动作。例如：接口下同一个traffic policy内，两个规则对应的动作分别为统计和镜像，虽然两个动作不冲突，但是最终也只有优先级较高的动作执行。

规则优先级的原则为：首先同一个流策略中，*precedence-value*越小，规则优先级越高；其次流分类中针对同一个ACL，rule-id越小，规则优先级越高。

2、当多个规则位于不同分组时，如果规则对应的动作不冲突，则全部动作都可以执行。例如：全局下执行重定向，接口下执行统计，两个规则位于不同的分组内，最终重定向和统计的动作都能执行。

3、当多个规则位于不同分组时，如果规则对应的动作冲突，则选择分组优先级较高的动作执行。

4、所有流策略的应用生效优先级，可通过在诊断视图下执行**display traffic-policy apply-information**命令进行查看。组的优先级越大的越先生效，业务的优先级越小的越先生效。

```
<HUAWEI> system-view
[~HUAWEI] diagnose
[~HUAWEI-diagnose] display traffic-policy apply-information slot 1:
slot 1:
-------------------------------------------------------------------------------
Chip Policy Type/Name         Apply Parameter         GroupId     Priority
                                                                Group / Service
-------------------------------------------------------------------------------
   0 traffic-filter           10GE1/0/1(In)               30      27 / 102
   0 w1                       10GE1/0/11(Out)             60       4 / 110
   0 w1                       VLAN 77(Out)                60       4 / 112
-------------------------------------------------------------------------------
```

1.2.3.2 ACL KEY 资源

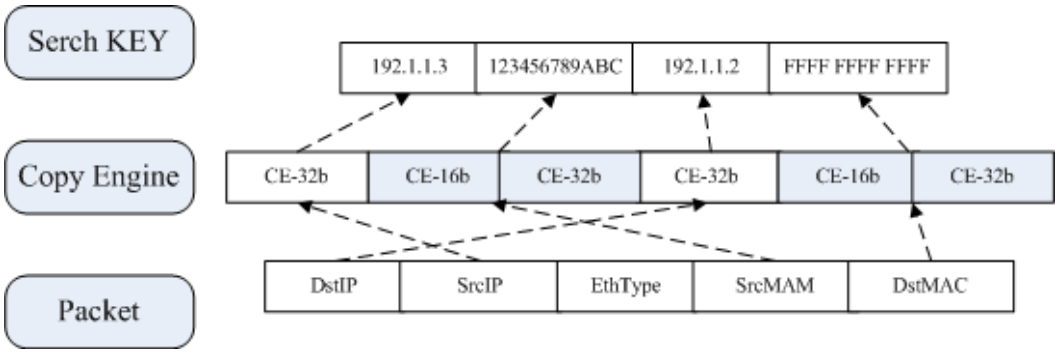
为让用户更好地部署ACL业务，下文着重描述构建查找KEY的芯片资源。

用户在理解了这些资源的内部使用和实现方式后，就能充分地利用设备提供的ACL功能来实现期望的业务。

1.2.3.2.1 ACL KEY 构建

转发芯片内置了硬件资源：CE(Copy Engine)。CE资源用来从报文头提取各个字段，比如ACL规则需要匹配目的MAC地址，那么转发芯片就使用一个CE资源来从报文头提取目的MAC地址字段。提取不同的报文字段需要使用不同的CE资源。

在转发芯片里，有2类CE资源：CE-32bit、CE-16bit，分别用于提取32bit和16bit的字段。若需要提取的字段宽度超过32bit，则需要多个CE来组合提取该字段，比如目的MAC地址宽度为48bit，所以提取该字段就需要1个CE-32bit和1个CE-16bit。如下图所示。

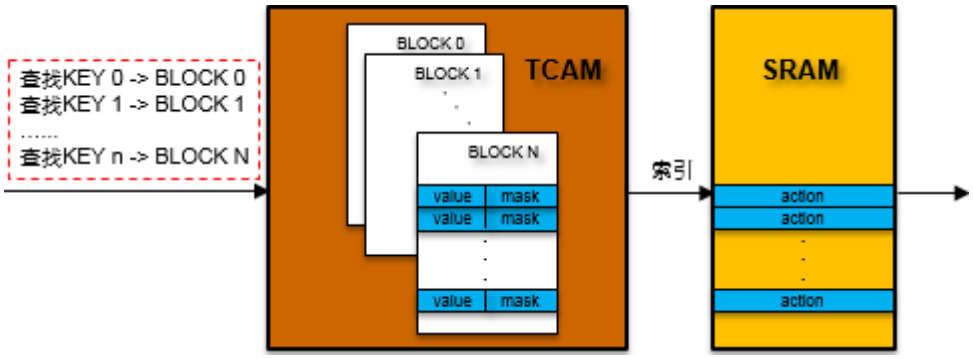


CE资源的硬件规格，决定了用户对同一个报文能匹配的最大字段数。

1.2.3.2.2 ACL 并行 KEY

上述ACL规则查找流程中，描述了TCAM划分成多个TCAM Block，并支持多个TCAM Block的并行查找。每个TCAM Block的查找KEY可以一样，也可以不一样。

若TCAM Block的查找KEY不一样，转发芯片就需要为同一个报文构建多个不同的查找KEY，并一次性地发给TCAM，以并行查找各个TCAM Block的ACL规则。



转发芯片内部使用Key Buffer来存放各个不同的查找KEY。因为不同类型的ACL业务使用的ACL查找KEY均不一样，所以转发芯片的Key Buffer硬件规格，决定了用户能配置多少个不同ACL业务（包括不同的MQC流策略）。

1.2.3.2.3 ACL 分组

上文提到，不同类型的ACL业务，其匹配的字段也即查找KEY都不一样。比如MQC流策略，在各个接口、VLAN等视图下可以灵活匹配不同的报文字段。

下面以两个例子进行说明：

1、在40GE2/0/1接口上配置入方向的MQC流策略，对特定目的MAC地址和VLAN的报文进行流量统计。

```
#
acl number 4000
 rule 5 permit destination-mac 0011-2233-4455
#
traffic classifier demo-MAC type and
 if-match acl 4000
 if-match vlan 100
#
traffic behavior demo-MAC
 statistics enable
#
traffic policy demo-MAC
```



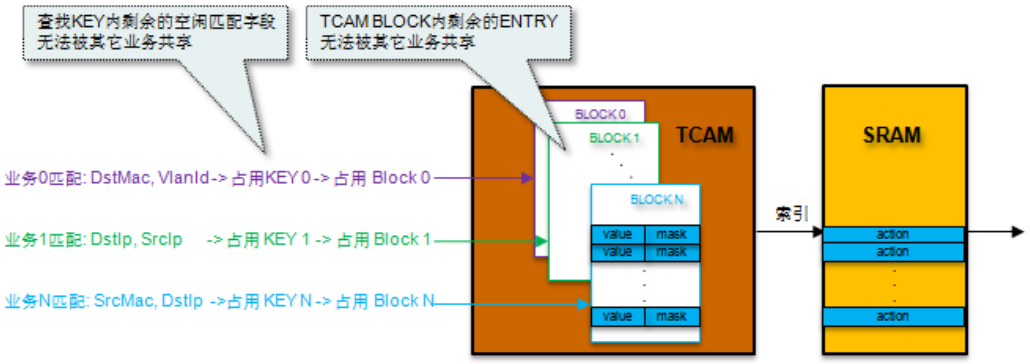
```
 classifier demo-MAC behavior demo-MAC precedence 5
#
interface 40GE2/0/1
 traffic-policy demo-MAC inbound
#
```

2、在40GE2/0/2接口配置入方向的MQC流策略，对特定源IP地址的报文进行优先级重标记。

```
#
acl number 2000
 rule 5 permit source 192.168.1.1 0.0.0.254
#
traffic classifier demo-IP type and
 if-match acl 2000
#
traffic behavior demo-IP
 remark local-precedence af2
#
traffic policy demo-IP
 classifier demo-IP behavior demo-IP precedence 5
#
interface 40GE2/0/2
 traffic-policy demo-IP inbound
#
```

若为不同的视图配置的匹配字段都构建不同的查找KEY，并占用独自的TCAM Block，则Copy Engine、Key Buffer、TCAM Block资源均无法共享，业务叠加不会超过KB资源的数目。

对于上面2个MQC流策略，就分别占用了1个Key Buffer和1个TCAM Block，总共占用2个Key Buffer和2个TCAM Block，如下图示意。

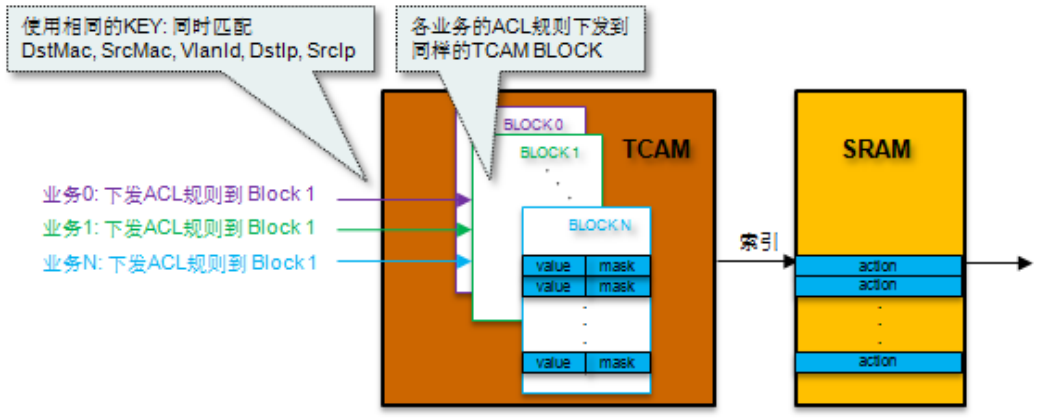


从上图可以看出，各个业务都只匹配了少量的报文字段，若都独自占用一个查找KEY，则会出现查找KEY里剩余的空闲字段无法被其它业务利用，而造成KB资源的浪费。

另一方面，芯片的TCAM Block资源也是有限的，各ACL业务若只需要下发少量的ACL规则，但也占用一个TCAM Block的话，则该TCAM Block内大量剩余的ENTRY也无法被其它ACL业务共享，使得TCAM存储资源浪费严重。

为了高效利用转发芯片的ACL资源，引入了ACL分组概念(ACL Group)。通俗的讲，为避免KEY Buffer和TCAM Block资源的“碎片”化，将常见的会同时部署的多个ACL业务的匹配字段归为一组，占用同样的查找KEY和TCAM Block。

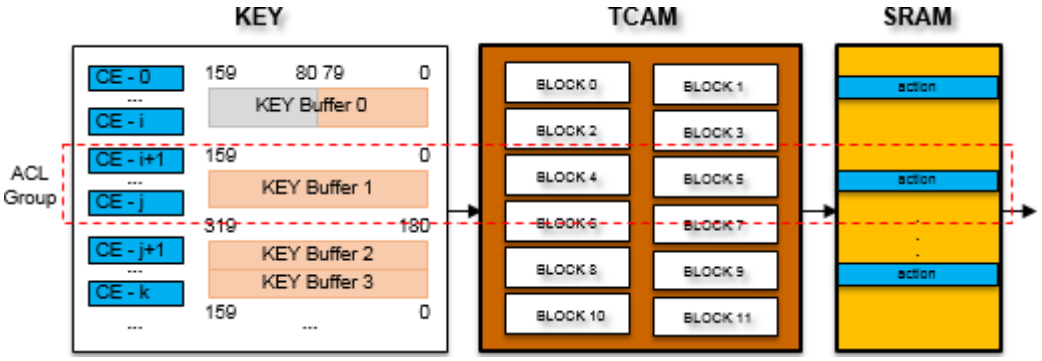
对于上面2个MQC流策略，只需要占用1个Key Buffer，同时包含目的MAC地址、VLAN、源IP地址三个匹配字段。同时2个流策略对应的规则都下发到同样的TCAM Block里，如下图示意。



从ACL业务角度来看，上述2个MQC流策略属于同一个ACL Group。

可以看出，若一个ACL业务下发“创建”了ACL分组(也即分配了KEY Buffer、TCAM Block)，后续属于同一个分组的ACL业务下发就无须再额外申请KEY Buffer、TCAM Block资源，而直接将所需的ACL规则下发到对应的TCAM Block里即可。

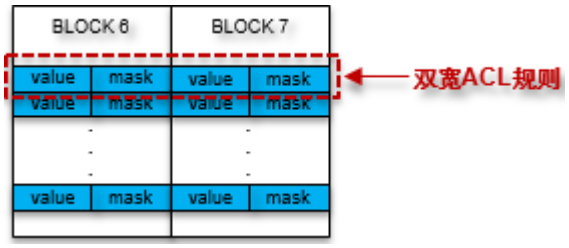
由此可以看出，ACL Group是设备为申请必须的ACL资源而进行的逻辑抽象，也即以ACL Group为单位，申请必须的Key Buffer、对应的Copy Engine、TCAM Block资源。



1.2.3.2.4 ACL 分组模式

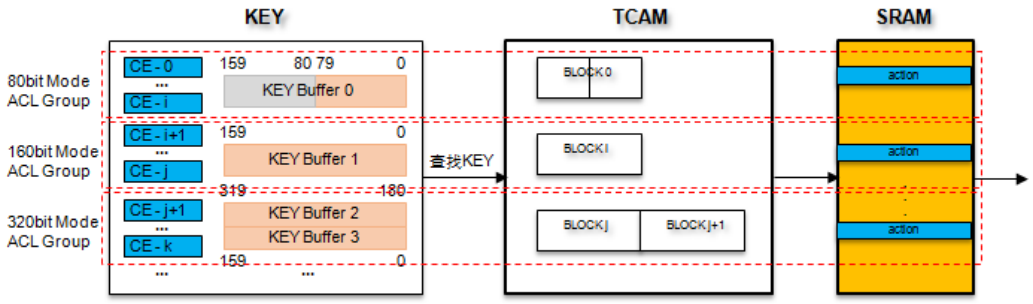
当ACL业务匹配字段较多时，相应的构建查找KEY的位宽就越大。为了满足这些ACL业务的需要，设备提供了几种位宽模式的ACL Group，即：80bit、160bit、320bit。

转发芯片内置的TCAM的物理ENTRY的位宽是160bit，1个Key Buffer也是160bit。当ACL业务需要320bit的查找KEY时，转发芯片就需占用2个Key Buffer，以构建出320bit的查找KEY。同时，转发芯片会将相邻的2个160bit的TCAM Block拼在一起，形成1个320bit的TCAM Block。如下图所示。



对只需要匹配少数几个报文字段的ACL业务，CE系列交换机提供了80bit的ACL分组，此时一个TCAM的物理ENTRY被分成2个80bit的ENTRY，这样可下发的ACL规则数量就会翻倍。

综合以上描述，CE系列交换机基于ACL Group及其模式来分配如下的ACL资源。



通过**display system tcam service brief**命令，可查询已经创建的ACL分组及其模式，包括对应的业务和已下发的ACL规则数。其中，Width列对应分组模式，Single代表单宽模式（80bit位宽），Double代表双宽模式（160bit位宽），Quadruple代表四宽模式（320bit位宽）。

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

------------------------------------------------------------------------------

 Chip  GroupID    Width      Stage          ServiceName
Count
       (FEI/
FE)

------------------------------------------------------------------------------

    0     2/2     Quadruple  Ingress        CPCAR
3
          3/3     Quadruple  Ingress        CPCAR
12
------------------------------------------------------------------------------

    1     2/2     Quadruple  Ingress        BPDU Deny
21
          2/2     Quadruple  Ingress        CPCAR
6
          2/2     Quadruple  Ingress        L2 Protocol Tunnel
1
          3/3     Quadruple  Ingress        App-Session
6
          3/3     Quadruple  Ingress        CPCAR
27
          8/1     Double     Ingress        MPLS PHP
12
------------------------------------------------------------------------------
```

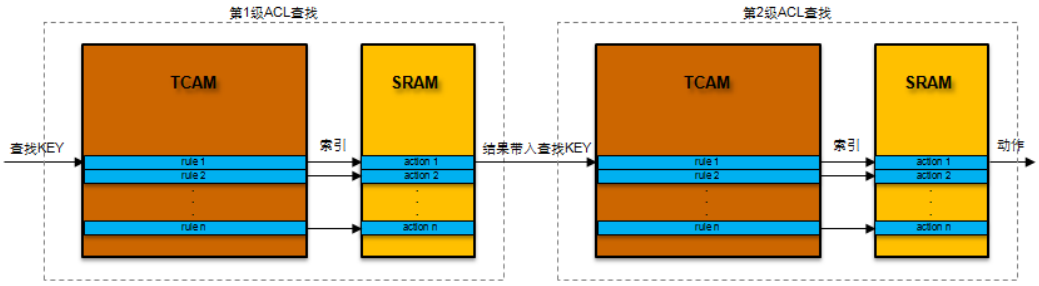
1.2.3.3 上下行 ACL

上文基于转发芯片上行ACL的实现，描述了ACL的转发原理和查找流程，涵盖了ACL规则的存储、查找KEY的构建、Copy Engine的使用、ACL逻辑分组的引入。

上行外扩ACL和下行ACL的转发原理和查找流程和上行ACL一致，仅在ACL芯片资源规格上有所差异。

为了充分利用转发芯片的ACL能力，设备还实现支持了两种“级联”ACL查找能力：上行外扩ACL和上行ACL的级联查找、上行ACL和下行ACL的级联查找。

级联查找的意思是，第1级ACL的查找结果，带入第2级ACL的查找KEY里，进行第2级ACL的查找。设备可以通过级联来实现具有竞争力的高级ACL业务特性。



比如，设备支持外扩TCAM存放组播路由，组播路由的查找结果带入内置TCAM里再进行ACL查找，以实现外扩TCAM里的组播路由的老化功能。

此外，设备对出方向匹配分片标记的MQC流策略，是在入方向先通过ACL规则来匹配IP报文的分片标记，将匹配的结果通过转发芯片内部转发头字段带入下行，再在下行ACL里匹配该结果，来进行相应的流策略动作。

1.2.4 ACL 资源规格

ACL资源是和单板密切相关的。CE12800系列交换机的单板可以简单的划分为两类：

E系列单板：CE-L48GT-EA、CE-L48GT-EC、CE-L48GS-EA、CE-L48GS-EC、CE-L24XS-BA、CE-L24XS-EA、CE-L48XS-BA、CE-L48XS-EA、CE-L24LQ-EA、CE-L48GT-ED、CE-L48GS-ED、CE-L12XS-ED、CE-L24XS-EC、CE-L24XS-ED、CE-L48XT-EC、CE-L48XS-EC、CE-L48XS-ED、CE-L48XS-EF、CE-L02LQ-EC、CE-L06LQ-EC、CE-L12LQ-EF、CE-L24LQ-EC、CE-L24LQ-EC1、CE-L36LQ-EG、CE-L04CF-EC、CE-L04CF-EF、CE-L08CC-EC和CE-L12CF-EG。

F系列单板：FD/FDA/FD1/FG/FG1/SD系列单板。

说明

CE-L24XS-BA、CE-L48XS-BA也属于E系列单板。

F系列单板和E系列单板的ACL实现流程和分配原则相同，二者的区别在于，F系列单板有8个KB资源，E系列单板有7个KB资源。其中F系列单板的规格指单板的互通模式为增强模式时的规格。

CE6870的ACL资源规格和F系列单板的ACL资源规格保持一致。

从前面的描述，可以看出，转发芯片的ACL模块实现，存在如下的芯片资源：Copy Engine、Key Buffer、TCAM Block。而上行外扩ACL、上行ACL、下行ACL各个阶段，均独自占用这些芯片资源。

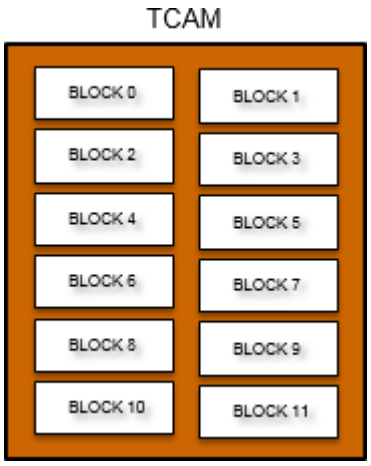
芯片资源	描述
Copy Engine（CE）	CE用于从报文头和转发信息提取ACL查找所需的各个字段。
Key Buffer（KB）	KB用于存放查找TCAM时构建的查找KEY。
TCAM Block	TCAM用于存放用户下发的各个ACL规则内容。

1.2.4.1 TCAM 规格

设备当前存在2种类别的单板，2类单板对应的转发芯片的内置TCAM Block规格如下，芯片总的ACL规格数为：Block数 * Rule数

TCAM规格	E系列单板	F系列单板
Block	12	12
Rule	1024*2	2048*2

内置的TCAM Block为上行ACL、下行ACL共享。



CE12800支持不同规格的外扩TCAM单板。各设备的具体ACL资源规格可以执行**display system tcam resource acl** [slot *slot-id*]查看。其中Bank或Slice即上述描述的Block。

1.2.4.2 KB 规格

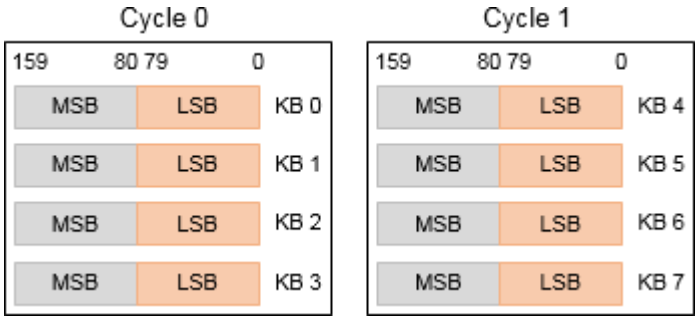
CE12800当前存在2种类别的单板，2类单板对应的转发芯片的Key Buffer规格如下。

KB规格	E系列单板	F系列单板
上行ACL	7	8
下行ACL	2	2
上行外扩TCAM的ACL	1	4

对于上行ACL，设备转发芯片的Key Buffer资源在芯片内部被划分在两个资源池Cycle中。对于E系列单板，KB1~3位于Cycle0中，KB4~7位于Cycle1中；对于F系列单板，KB0~3位于Cycle0中，KB4~7位于Cycle1中。

对于上行ACL，为支持80bit的查找KEY， 160bit的Key Buffer又被平均分成两部分，高低2个80bit分别称之为MSB、LSB。

以F系列单板为例：



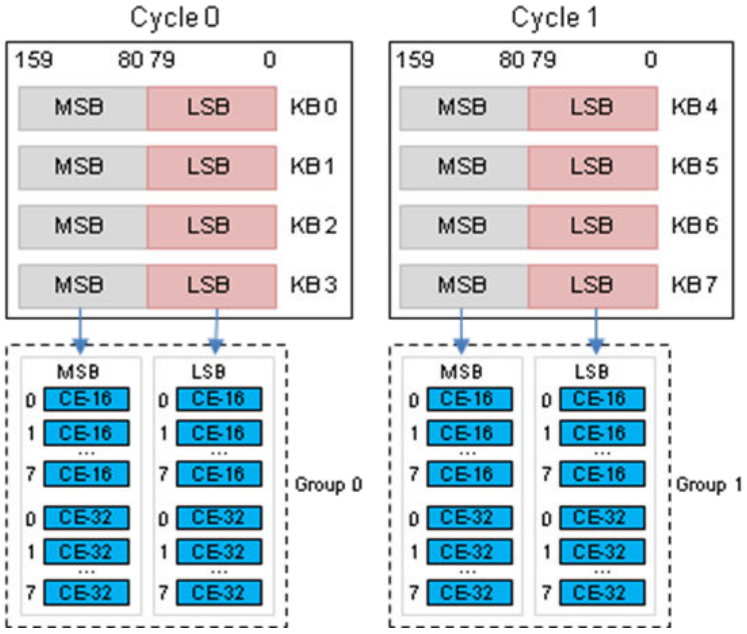
1.2.4.3 CE 规格

CE12800单板对应的转发芯片的Copy Engine规格如下。

CE规格		E系列单板	F系列单板
上行ACL	CE-16	16 * 2	16 * 2
	CE-32	16 * 2	16 * 2
下行ACL	CE-16	8	8
	CE-32	8	8
上行外扩TCAM的ACL	CE-16	6	16
	CE-32	6	16

同KB分成2组一样，对应的CE资源也分成2组，每组各16个CE-16bit、16个CE-32bit。一部分专门用于构建Key Buffer的MSB，一部分专门用于构建Key Buffer的LSB。

对于上行ACL，各Key Buffer及其构建所需的Copy Engine资源对应关系如下。

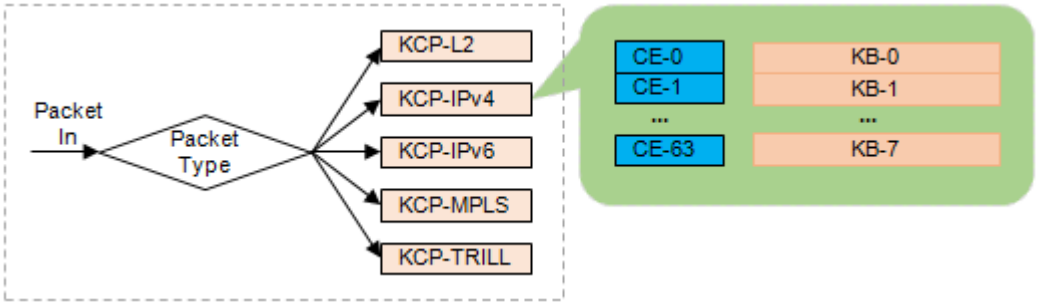


KB编号	CE-MSB排布		CE-LSB排布	
	CE-32	CE-16	CE-32	CE-16
KB-0	8	8	8	8
KB-1				
KB-2				
KB-3				
KB-4	8	8	8	8
KB-5				
KB-6				
KB-7				

1.2.4.4 资源关系

转发芯片增加了一个“内部”资源，该资源指明了哪些类型的报文可以查找指定的ACL Group。换句话说，设备下发的ACL Group都会告知转发芯片该ACL Group对哪些格式的报文有效。通过这种方式，就可以防止ACL Group误命中不期望的报文类型，因而不需要在其Key Buffer里增加相关报文类型的匹配字段。

转发芯片的这种内部资源称之为KCP(Key Construction Program)，当前设备支持的KCP资源基于报文格式类型进行分类：L2、IPv4、IPv6、MPLS、TRILL。



当报文进入时，根据报文的格式类型映射到对应的KCP，该KCP指明了该报文要查找哪些ACL Group，并用哪些CE资源提取对应的匹配字段，来构建对应的Key Buffer。那么对于该KCP下的ACL Group，也就意味着仅针对对应格式类型的报文才有效。

每种KCP都有64个CE、8个KB资源。若一个ACL Group想对多个报文类型有效，就意味着在多个KCP下均能查找到该ACL Group，因而该ACL Group就占用多个KCP下的CE、KB资源。

业务占用的KCP，ACL Group和KB资源可以通过执行如下命令查看。

```
[~HUAWEI] display system tcam acl group resource slot 1
STG : Stage                   KCP  : Key Construction Program
ING : Ingress                 EGR  : Egress
CYC : Cycle                   PTYPE: PortType
FRT : Front Ports             RCY  : Recycle Ports
16-L: 16bit-LSB Copy Engine   16-M : 16bit-MSB Copy Engine
32-L: 32bit-LSB Copy Engine   32-M : 32bit-MSB Copy Engine
```



```
F   : Free                    T    : Total
-------------------------------------------------------------------------------
Slot: 1    Chip : 0   UseRate:Normal
-------------------------------------------------------------------------------
STG KCP PacketType       PTYPE       CYC Group   UsedKey 16-L  32-L  16-M  32-M
                                                          F|T   F|T   F|T   F|T
-------------------------------------------------------------------------------
ING   1 L2               FRT           0 2       2,3     2|8   5|8   7|8   6|8
ING   2 IPV4             FRT           0 3       2,3     0|8   4|8   4|8   6|8
ING   3 TRILL            FRT           0 1       2,3     6|8   5|8   7|8   6|8
ING   4 IPV6             FRT           0 4       2,3     2|8   5|8   1|8   6|8
-------------------------------------------------------------------------------
```

若某个KCP下的CE、KB资源不足，则该报文类型下的新增ACL业务不能下发。

1.3 ACL 资源原理（CE12800 和 CE6870 除外）

说明

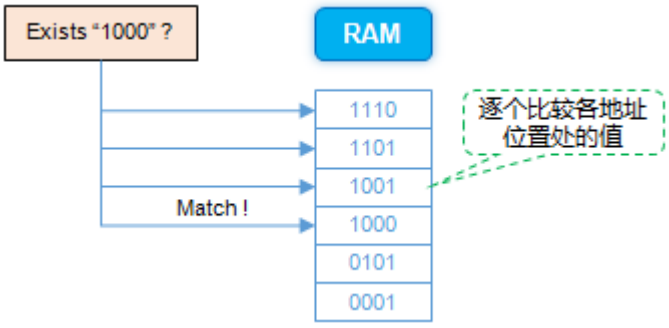
章节中描述的Block也称为Bank或slice。

1.3.1 ACL 基本概念

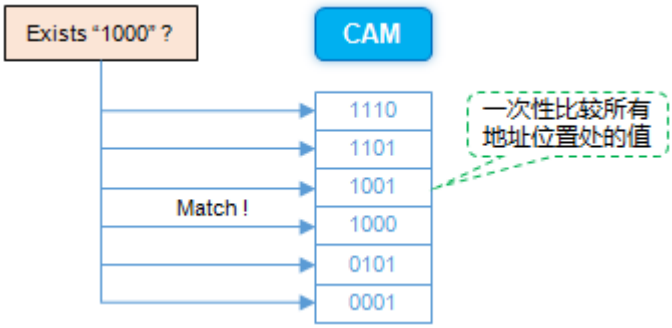
在开始CE系列交换机的ACL业务特性及编程能力描述之前，先了解ACL实现相关的几个关键概念：TCAM、ACL、MQC。

1.3.1.1 什么是 TCAM

在TCAM出现之前，用于存放ACL规则的存储器是RAM(Random Access Memory)，也就是随机访问存储器。对于查找而言，RAM是从某个地址开始依次比较，直到匹配到某个值或者查询完为止。整个查找过程是多次查找，速度较慢。



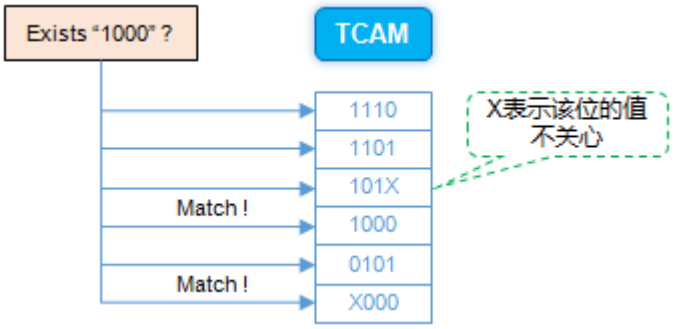
为了提高查找效率，就出现了CAM(Content Addressable Memory)，即内容可寻址存储器。顾名思义，CAM的查找是基于内容的，输入一个值，如果CAM中存在该值，就会输出该值所在的地址。CAM是一次性全部查找，速度非常快。



从上可以看出，RAM和CAM的本质区别在于，RAM是由地址得到数据，而CAM是由数据得到地址。上图中，对存放同样数据的RAM和CAM进行查找，RAM是依次比较，CAM是立即查找所有匹配项。

TCAM(Ternary Content Addressable Memory)，是CAM的升级版，采用掩码匹配。掩码，即用1来对应我们关心的数据，用0来对应不关心的数据。

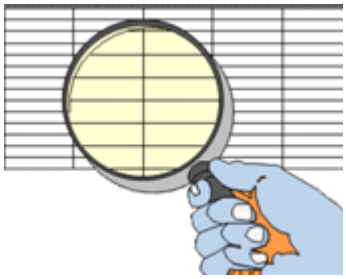
如下图所示，TCAM中的值是由掩码和数据相与产生的，当掩码为0时，TCAM中的值为X，此时可以与1000中的相应位进行模糊匹配，即无论相应位是0还是1都可以匹配上；当掩码为1时，TCAM中的值为相应的数据，此时需要与1000中的相应位进行精确匹配。这样实际上数据就可以有三种值：0、1和X。



在上面的例子中，1000就是查找KEY，用来查找TCAM中的多条规则：entry 0 = {1110}，entry 1 = {1101}，entry 2 = {101X}，entry 3 = {1000}，entry 4 = {0101}，entry 5 = {X000}，可以匹配上的规则entry 3和entry 5。若有多个entry被命中，则TCAM采取最低索引的命中表项，即命中的entry 3生效。

1.3.1.2 什么是 ACL

ACL是Access Control List的简称，中文是访问控制列表。顾名思义，ACL就是一张表。



ACL表中包含了一系列的规则(rule)，如下列在设备上配置的ACL规则。

```
#
acl number 3000
 rule 5 permit ip source 1.1.1.1 0
 rule 10 permit ip source 1.1.1.2 0
 rule 15 deny ip destination 2.2.2.0 0.0.0.255
 rule 20 deny igmp
 rule 25 deny udp destination-port eq 255
 rule 30 permit tcp source-port eq 6550
#
```

简单来说，ACL其实是人为定义的一组或几组规则，以便设备判断是否执行用户指定的动作。抽象来说，通过ACL，可以对报文进行分类，将具有某类共同特征的报文划分为一类，来为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

按照ACL功能，ACL可以分为如下几类：

分类	适用的IP版本	功能介绍	说明
基本ACL	IPv4	可使用IPv4报文的源IP地址、分片标记和时间段信息来定义规则。	基本IPv4 ACL简称基本ACL。编号范围为2000～2999。
高级ACL	IPv4	既可使用IPv4报文的源IP地址，也可使用目的地址、IP优先级、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP（User Datagram Protocol）源端口/目的端口号等来定义规则。	高级IPv4 ACL简称高级ACL。编号范围为3000～3999。
二层ACL	IPv4&IPv6	可根据报文的以太网帧头信息来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、以太帧协议类型等。	编号范围为4000～4999。
用户自定义ACL	IPv4&IPv6	可根据偏移位置和偏移量从报文中提取出一段内容进行匹配。	编号范围为5000～5999。
基于ARP的ACL	IPv4	基于ARP的ACL根据ARP报文的源/目的IP地址、源/目的MAC地址定义规则，实现对ARP报文的匹配过滤。	编号范围为23000～23999。
基本ACL6	IPv6	可使用IPv6报文的源IP地址、分片标记和时间段信息来定义规则。	基本IPv6 ACL简称基本ACL6。编号范围为2000～2999。
高级ACL6	IPv6	可以使用IPv6报文的源地址、目的地址、IP承载的协议类型、针对协议的特性（例如TCP的源端口、目的端口、ICMPv6协议的类型、ICMPv6 Code）等内容定义规则。	高级IPv6 ACL简称高级ACL6。编号范围为3000～3999。

1.3.1.3 什么是 MQC

为了简化用户的ACL配置，并支持ACL配置的灵活性，CE系列交换机提供了模块化QoS命令行MQC(Modular QoS Command-Line Interface)。

下列显示了一个通过MQC命令行配置的流策略，该流策略规则对DstMac=0000-1111-2222和SrcIp=1.1.1.1的报文，进行流量统计和流量监管动作。

```
#
acl number 3000
 rule 5 permit ip source 1.1.1.1 0
#
traffic classifier demo type and
 if-match destination-mac 0000-1111-2222 ffff-ffff-ffff
 if-match acl 3000
#
```



```
traffic behavior demo
 statistics enable
 car cir 100 kbps
#
traffic policy demo
 classifier demo behavior demo precedence 5
#
```

从以上可以看出，MQC命令行形式有3个要素：流分类(traffic classifier)、流行为(traffic behavior)、流策略(traffic policy)。

具体配置可以参考CE系列交换机产品文档-QoS业务配置-MQC业务配置。

在配置好MQC流策略后，就可以将流策略应用到全局、slot、接口、子接口、VLAN、VPN实例、VSI实例、BD等视图上。

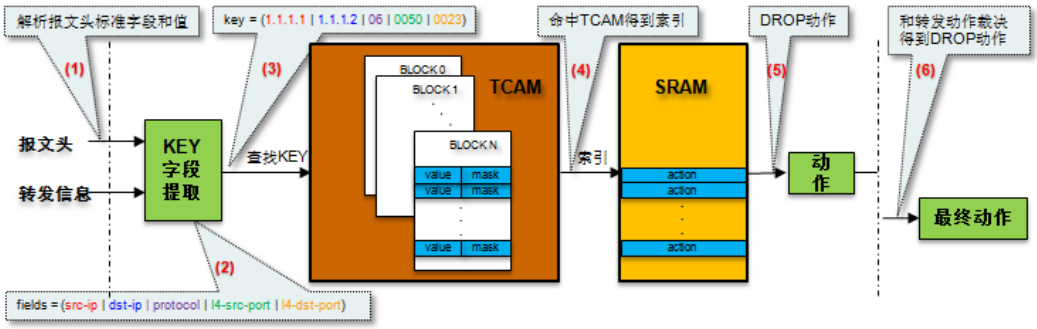
应用时，可以指定流策略需要应用的方向。其中inbound表示入方向、outbound表示出方向。如下列将流策略demo-PORT应用到接口40GE2/0/1的入方向上。

```
#
interface 40GE2/0/1
 traffic-policy demo-PORT inbound
#
```

1.3.2 ACL 查找实现

1.3.2.1 ACL 查找流程

在ACL规则下发到转发芯片里的TCAM存储单元后，转发芯片根据报文的相关字段信息来查找用户配置下发的ACL规则。



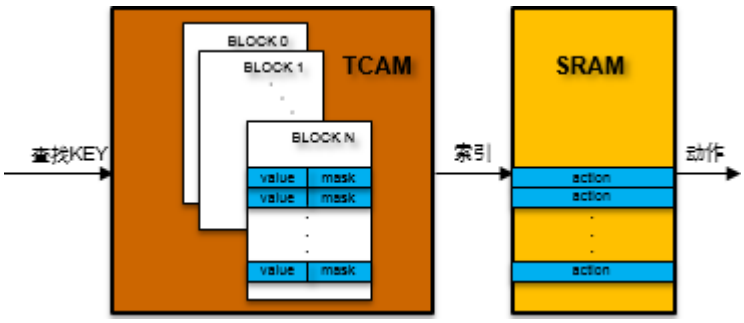
上图显示了CE转发芯片的ACL规则查找流程，具体步骤如下：

查找流程	步骤描述
字段解析	从报文头和转发信息里，解析所需的匹配字段对应的位段。
字段值提取	根据匹配字段解析的位段，提取对应位置的值。
查找KEY构建	根据提取的各个匹配字段的值，来构建查找TCAM所需的KEY。
发起TCAM查找	将构建的查找KEY发给TCAM Block，命中ENTRY时得到对应的ENTRY的索引。

查找流程	步骤描述
获取动作	根据TCAM的命中索引，来访问对应命中ENTRY的各个动作。
动作冲突裁决	命中的ACL的动作可能会和之前的转发流程的动作冲突，需要进行一次裁决。

在查找TCAM里的ACL规则之前，需要构建查找KEY。查找KEY根据报文的各层头字段、以及报文在芯片里的转发信息(如转发类型、下一跳索引、出接口等)来构建。

构建好查找KEY后，就发起TCAM查找命令到相应的各个TCAM Block。各个TCAM Block若有ACL规则命中，则根据命中的索引，进一步访问该命中规则在SRAM里的动作。



转发芯片在获取所有命中规则的动作后，综合查找ACL之前的报文转发动作，进行一次动作裁决，裁决后的动作为报文最终的转发动作。

比如，报文在PP的转发流程里，得到的动作是转发到一个物理出接口，之后命中的ACL规则的动作是丢弃，那么报文经过最终裁决会执行丢弃动作而非转发到物理出接口。

1.3.2.2 ACL 处理阶段

在CE系列交换机上，ACL的处理模块称为CAP（Content aware processer）。根据在转发流程处理阶段的不同，CAP又划分为以下三个模块：

VCAP（VFP）：处于VLAN分配阶段的CAP处理模块，在L2查找之前就需要生效的ACL在此模块处理，例如：MAC不学习动作。

ICAP（IFP）：处于上行报文处理流程结尾的CAP处理模块。大部分在入方向生效的ACL都在此模块处理。

ECAP（EFP）：处于下行报文处理流程结尾的CAP处理模块。所有在出方向生效的ACL都在此模块处理。

以上三个模块为都有独立的TCAM rule资源和SRAM action资源，不能共用。

1.3.2.3 ACL 分组

CE系列交接机将设备上的TCAM资源划分为包含若干条rule资源的Block。在TCAM资源分配时，TCAM必须以Block为单位进行资源分配，而且每个Block的格式必须是相同的，即每个Block中的rule必须匹配相同的报文字段。每个Block每条rule可以包含的匹配字段长度的上限为Block的位宽。

以CE6851HI为例，TCAM资源的规格如下所示：

TCAM阶段	Block数目	ENTRY数目	位宽
VCAP	4	256	234bit
ICAP	4	512	275bit
	8	256	275bit
ECAP	4	256	234bit

不同设备的规格可以通过执行**display system tcam resource acl** [**slot** *slot-id*]命令查看，其中Pre-Ingress对应VCAP，Ingress对应ICAP，Egress对应ECAP，Slice对应Block。

```
[~HUAWEI] display system tcam resource acl
Slot: 1, Chip: 0
-------------------------------------------------------------
Stage          Resource   Total     Used Limited     Free
-------------------------------------------------------------
Pre-Ingress    Slices         4        2       2        2
               Rules       1024        6     506      512
               Meters         0        0       0        0
               Counters       0        0       0        0
-------------------------------------------------------------
Ingress        Slices        12        4       4        8
               Rules       6144      212    1836     4096
               Meters      2048        0       0     2048
               Counters   38912       41       0    38871
-------------------------------------------------------------
Egress         Slices         4        0       0        4
               Rules       1024        0       0     1024
               Meters      1024        0       0     1024
               Counters    1024        0       0     1024
-------------------------------------------------------------
```

若为不同的规则都指定不同的Block格式，按Block为单位为rule分配资源则会造成TCAM资源的严重浪费。

为了解决上述问题，CE系列交换系统内部提供了多种TCAM Block资源的格式，即为ACL分组，每个ACL业务下发时，必须选取一个TCAM Block资源的格式，即选择一个分组。

例如，设备存在在如下预置分组：

分组ID	分组模式	字段集合
38	single	Source IP Destination IP Source Port, Outer VLAN ID Ethernet Type, IP Protocol, IP Type, IP Frag

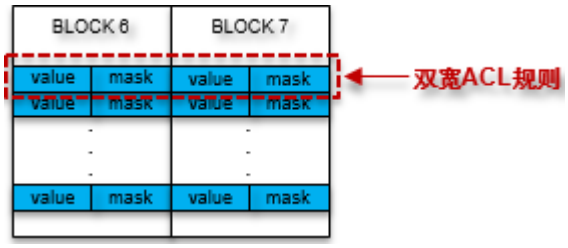
当两个traffic policy分别匹配源IP地址和目的IP地址时，虽然匹配的字段不一样，但是因为上述分组的字段集合中同时包含源IP地址和目的IP地址，所以两个traffic policy可以使用上述分组共享同一个TCAM的Block。

1.3.2.4 ACL 分组模式

当ACL业务匹配字段较多时，相应的构建查找KEY的位宽就越大。为了满足这些ACL业务的需要，CE系列交换机对ACL分组提供了几种位宽模式，例如单宽模式Single、双宽模式Double、三宽模式Triple、四宽模式Quadruple。

例如，当ACL业务下发时，如果ACL匹配的字段总长度不超过TCAM Block的位宽，一条rule仅下发在一个Block内，即创建Single模式的分组。

如果ACL业务匹配的字段总长度超过TCAM Block的位宽，小于两倍TCAM Block的位宽时，一条rule就需要下发到两个Block内，此时转发芯片会将相邻的2个TCAM Block拼在一起，即创建Double模式的分组。如下图所示：



当ACL的分组模式为Double时，每下发一条rule，同时要占用两个Block资源，相对于单宽的ACL分组，在TCAM资源总数相等的情况下，可以下发的ACL规则条数减半。

不同的设备，ACL分组模式不同，可以在诊断视图下执行**display system tcam service brief [slot** *slot-id* **]**命令进行查看。

```
[~HUAWEI-diagnose] display system tcam service brief slot 1
Slot: 1
--------------------------------------------------------------------------------
Chip  GroupID    Width      Stage          ServiceName                  Count
--------------------------------------------------------------------------------
   0        8   Double     Ingress        App-Session                      2
            8   Double     Ingress        CPCAR                           35
            8   Double     Ingress        L2 Protocol Tunnel               1
            8   Double     Ingress        UDP Helper                       6
            8   Double     Ingress        VxLAN DFS                        2
           64   Double     Ingress        CPCAR                            6
--------------------------------------------------------------------------------
```


1.3.2.5 SRAM 动作执行

当报文命中多条规则时，每条规则的动作可能不一样，此时最终执行的动作需要经过裁决，具体按照如下原则：

1、当多个规则在同一个分组时，无论规则对应的动作是否冲突，仅执行优先级最高的规则对应的动作。例如：接口下同一个traffic policy内，两个规则对应的动作分别为统计和镜像，虽然两个动作不冲突，但是最终也只有优先级较高的动作执行。

规则优先级的原则为：首先同一个流策略中，*precedence-value*越小，规则优先级越高；其次流分类中针对同一个ACL，rule-id越小，规则优先级越高。

2、当多个规则位于不同分组时，如果规则对应的动作不冲突，则全部动作都可以执行。例如：全局下执行重定向，接口下执行统计，两个规则位于不同的分组内，最终重定向和统计的动作都能执行。

3、当多个规则位于不同分组时，如果规则对应的动作冲突，则选择分组优先级较高的动作执行。

4、所有流策略的应用生效优先级，可通过在诊断视图下执行**display traffic-policy apply-information**命令进行查看。组的优先级越大的越先生效，业务的优先级越小的越先生效。

```
<HUAWEI> system-view
[~HUAWEI] diagnose
[~HUAWEI-diagnose] display traffic-policy apply-information slot 1:
slot 1:
-------------------------------------------------------------------------------
Chip Policy Type/Name         Apply Parameter         GroupId     Priority
                                                                Group / Service
-------------------------------------------------------------------------------
   0 traffic-filter           10GE1/0/1(In)               30     27 / 102
   0 w1                       10GE1/0/11(Out)             60      4 / 110
   0 w1                       VLAN 77(Out)                60      4 / 112
-------------------------------------------------------------------------------
```


2 业务与 ACL

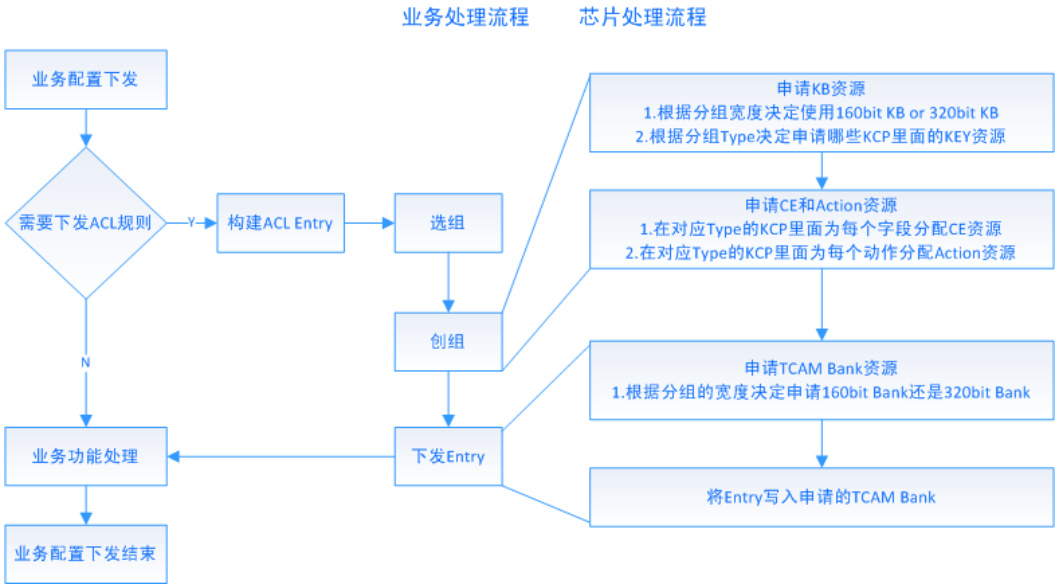
文档中命令的回显如果没有特别说明都以V200R002C50版本为例。

2.1 业务与 ACL（CE12800 和 CE6870）

2.1.1 概述

ACL功能非常强大，一方面用户可以直接配置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。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。比如Vlanif流量统计业务，需要下发ACL针对对应Vlanif的流量进行统计。

业务下发ACL规则流程和对应的芯片处理流程如下图所示。



分组的选择方式有两种：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；一种是动态选组，即需要根据用户配置字段和动作

信息去遍历预定义好的分组模板，找到一个合适的分组，该选组方式主要用于MQC业务。

如果业务下发ACL时，选到的分组已经创建，则此时不需要再创建该分组，即不需要再申请KB、CE、Action资源。只需要申请TCAM Bank资源下发ACL规则。

静态选组的分组模板定义与业务映射关系举例如下：

Group ID	Type	字段集合		动作集合			
14	ALL	Port	Vlan ID	DMAC Hit	DMAC	Statistics	CAR
业务	QoS CAR	Y	-	-	-	Y	Y
	Port BC Suppress	Y	-	-	Y	-	Y
	Port Unknown UC Supress	Y	-	Y	-	-	Y
	Vlan BC Suppress	-	Y	-	Y	-	Y

该表说明了编号为14的ACL Group对应所有的报文类型以及下发到该组的业务所匹配的字段和执行的动作，其中Y表示某业务中匹配相应的字段和执行相应的动作。

动态选组的分组模板定义举例如下，与业务不是静态映射的，根据用户配置进行动态选组：

Group ID	Type	字段集合		动作集合							
		Port	VS	SrcIP	DstIP	L4S Port	L4D Port	Protocol	Statistics	Deny	Redirect
290	IPv4	Y	-	Y	-	-	-	-	-	Y	Y
214	IPv4	-	Y	Y	Y	Y	Y	Y	Y	Y	Y

该表说明，某类型的报文匹配某些字段和执行某些动作时会下发到相应的分组，其中Y表示匹配该字段以及执行该动作。

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业务。当用户配置的MQC流策略时，会配置ACL规则，所以属于显式使用ACL的业务；当用户使能IPv6业务时，虽然会下发用于处理IPv6协议报文的ACL，但是用户没有直观的感知，所以就属于隐式的使用ACL的业务。

2.1.2 隐式使用 ACL 的业务

2.1.2.1 概述

由于业务应用场景需要，当使能一些配置时，如VXLAN、TRILL、MPLS、IPv6等业务，也会下发ACL规则进行某些处理，例如用于实现协议报文捕获等功能，但是不需要用户增加ACL的配置，ACL的作用不会被用户直接感知。又比如用于邻居设备发现的LLDP功能，用户能看到的是本设备的邻居设备信息，ACL负责捕获LLDP协议报文送给业务处理，作为整个LLDP功能的一个环节，也不为用户感知。

隐式使用ACL的业务，下发ACL规则时，选组的方式是静态选组。

2.1.2.2 默认下发的业务

为保证基础二三层业务默认可用，设备启动之后，会默认下发两个ACL分组2和3，用于捕获基础二三层协议报文到CPU处理的ACL业务下发，如ARP、ICMP等协议。

Group ID	分组模式	处理的报文格式	业务名称
2	320bit（Quadruple）	L2（指ARP、BPDU等二层报文）	ARP、BPDU、STP、LACP等二层业务
3	320bit（Quadruple）	IPv4	ICMP、VRRP、DHCP、IGMP、RIP、BGP、Telnet、SSH等三层业务

具体可以的通过诊断命令**display system tcam service brief [slot** *slot-id*]查看业务ACL规则下发情况：

```
[~HUAWEI-diagnose] 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
-------------------------------------------------------------------------------
```

设备初始时各类KB资源使用情况如下（以E系列单板为例）：

KCP	分组ID	使用的KB编号	剩余的KB编号
L2	2	KB-2，KB-3	KB-1，KB-4~KB-7
IPv4	3	KB-2，KB-3	KB-1，KB-4~KB-7
IPv6	NA	NA	KB-1 ~ KB-7
MPLS	NA	NA	KB-1 ~ KB-7
TRILL	NA	NA	KB-1 ~ KB-7

设备初始时TCAM Bank资源使用情况如下：

Bank ID	0	1	2	3	4	5	6	7	8	9	10	11
状态	Used	Used	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free

2.1.2.3 TCAM 单板业务

外扩TCAM单板通过在芯片额外增加一块大规格的TCAM器件，用来实现路由和ACL表项的扩容。当在外扩TCAM单板上使能外扩TCAM组播功能时，会下发组播流量统计的ACL，使用2个ACL分组67和68，如下所示。

```
[~HUAWEI-diagnose] 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                    4
          3/3     Quadruple  Ingress        CPCAR                         25
         67/1     Single     Ingress        MC Mapping Statistics          1
         68/4     Single     Ingress        Multicast Statistics           7
------------------------------------------------------------------------------
```

外扩TCAM单板注册后，会默认使能外扩TCAM组播功能，此时KB资源使用情况如下：

说明

V200R001C00版本开始不再默认使能外扩TCAM组播功能。

KCP	分组ID	使用的KB编号	剩余的KB编号
L2	2	KB-2，KB-3	KB-1，KB-4~KB-7
IPv4	3、67、68	KB-2，KB-3，KB-4，KB-5	KB-1，KB-6，KB-7
IPv6	67、68	KB-4，KB-5	KB-1～KB-3，KB-6，KB-7
MPLS	NA	NA	KB-1～KB-7
TRILL	NA	NA	KB-1～KB-7

2.1.2.4 其他配置类业务

除了默认下发的业务外，部分配置类业务也会隐式地使用ACL，例如：

Group ID	KEY个数	处理报文的格式	业务名称
4	2	IPv6	CPCARv6
7	2	TRILL	CPCAR TRILL
8	1	MPLS	DiffServ MPLS MPLS PHP
11	1	ALL	Vlan Statistics BD Statistics
12	1	IPv4	DHCP SNOOPING IPSG
14	1	ALL	QOS CAR Storm Control
19	2	ALL	Blacklist Filter Auto-Defend

2.1.2.5 配置举例

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统计后会下发ACL规则：匹配Vlan 10，动作为统计。

由前面原理可知，业务下发ACL规则时，需要为该ACL规则选择合适的Group。ACL规则下发到TCAM之前，需要先创建选择的Group，Group的创建实质上就是申请KB资源、CE资源和Action资源的过程。Group创建成功之后，ACL规则会申请TCAM Bank资源，将规则写入TCAM Bank。同时Group也会记录ACL规则所在的TCAM Bank ID，用于告知查找KEY需要查找哪些TCAM Bank。

可以通过诊断命令**display system tcam service brief** [**slot** *slot-id*] 查看Vlan统计业务ACL资源的下发情况：

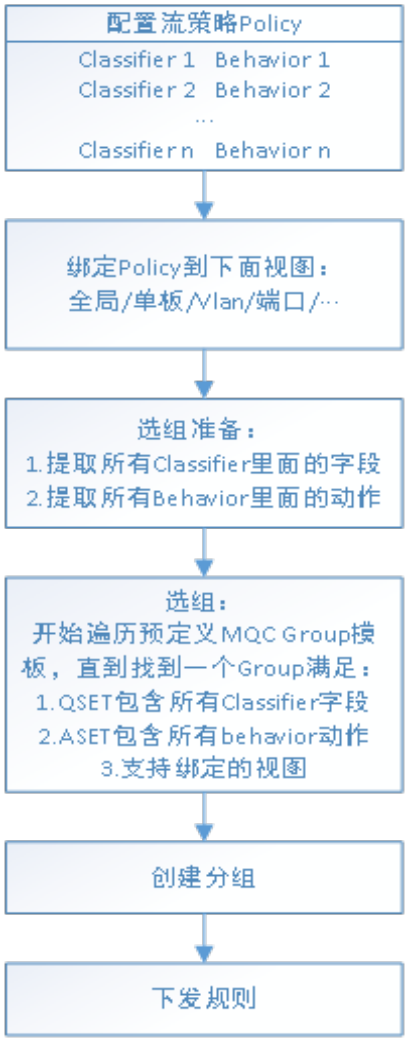
```
[~HUAWEI-diagnose] display system tcam service brief slot 1
Slot: 1
------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                 Count
       (FEI/FE)
------------------------------------------------------------------------------
    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
------------------------------------------------------------------------------
```

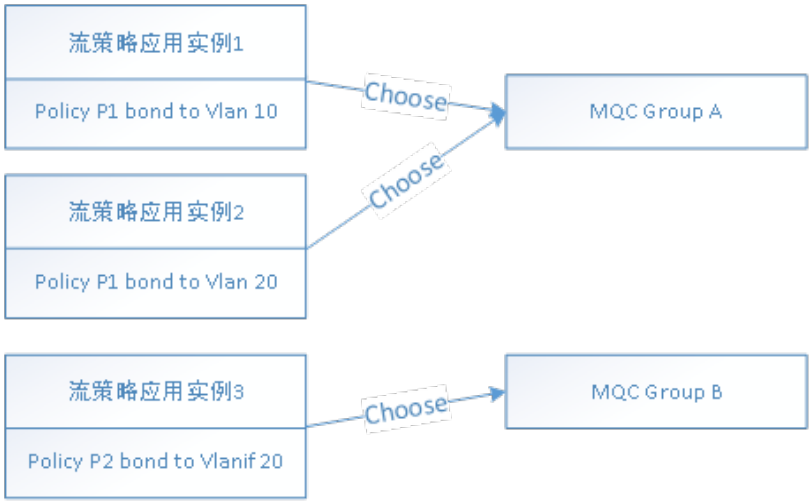
2.1.3 显式使用 ACL 的业务

MQC业务属于显示使用ACL的业务，因为MQC业务的ACL规则信息是用户配置的，用户可以感知到。用户可以指定匹配具备某些特征的报文，对其进行统计、限速、丢弃等处理。

MQC对用户赋予的配置灵活性是非常高的，理论上可以指定匹配任意内容和执行任意动作。MQC业务在下发ACL规则时，分组的选择是根据用户配置决定的，采用动态方式进行选组。当一个流策略Policy绑定到一个视图下，称之为一个流策略应用实例。每个流策略应用实例都会进行选组，选组逻辑如下图所示：



流策略应用实例与分组可能是一对一的关系，也可能是多对一的关系。



2.1.3.1 MQC 配置举例

以配置MQC允许从Vlanif10进来的特定端口号的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
#
```

流策略p_example里面，流分类c_example匹配的acl 3000里面涉及的字段有IP五元组，流行为b_example里面动作为统计，应用视图为Vlanif，在选择Group时，会根据匹配内容、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。

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	由于动作和视图不支持，不选择
214	1	IPv4	IP五元组	丢弃 | 重定向 | 限速	Interface / Vlan	由于动作和视图不支持，不选择
216	1	IPv4	IP五元组，TCP Flag	丢弃 | 重定向 | 统计	Interface / Vlan/ Vlanif	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)	Interface / Vlan/ Vlanif/全局	该分组消耗2个KEY资源，不是最佳选项，不选择

执行命令**display traffic-policy applied-record**查询流策略应用记录：

```
[~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
-------------------------------------------------------------------------------
```

执行诊断命令查询**display system tcam service brief [slot** *slot-id* **]**查看MQC业务下发情况：

```
[~HUAWEI-diagnose] 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
-------------------------------------------------------------------------------
```


2.1.3.2 MQC 分组模板

产品预先定义了很多MQC分组模板，用于不同配置时进行选择。以V200R001C00版本为例，MQC业务部分预定义分组模板信息如下：

GroupID	KB个数	报文格式	匹配条件	动作	应用视图
213	1	IPv4	IP五元组，分片	丢弃、重定向、镜像、remark(local-precedence、dscp)	Interface/ Vlan
214	1	IPv4	IP五元组，分片	丢弃、重定向、限速	Interface / Vlan
216	1	IPv4	IP五元组，分片，TCP Flag	丢弃、重定向、镜像、remark(local-precedence、dscp)	Interface / Vlan/Vlanif
233	2	IPv4	IP五元组，分片，TOS，TTL，TCP Flag	丢弃、重定向、统计、remark (local-precedence、dscp)	Interface / Vlan/Vlanif/ 全局
242	2	IPv6	IPv6五元组	丢弃、重定向、统计、remark(local-precedence、dscp)	Interface

2.1.4 ACL 业务叠加场景

当前现网中使用到硬件ACL资源的业务在相互叠加时，可能会出现ACL资源不足的问题。所以本章节对ACL 业务典型的叠加场景做一个总结，用来指导用户部署相关业务。

2.1.4.1 VXLAN/EVPN 业务叠加场景

1、入方向 VXLAN/EVPN 业务叠加场景

VXLAN/EVPN业务是占用ACL资源的大户。其中EVPN场景同样需要配置VXLAN业务，只是比VXLAN场景多下发一个EVPN MAC业务。

为了节省ACL资源，叠加尽可能多的业务，在入方向VXLAN/EVPN场景下有如下建议：

1. 不使用不推荐的单板类型，因为不推荐的单板在配置VXLAN时比其他单板默认多占用一个KB资源；
2. 执行**assign forward nvo3 service extend enable**命令，因为该命令可以在非不推荐的单板上生效并减少一个VXLAN业务所需要的KB资源；

   说明

   CE6870不支持此命令。
3. 执行**assign forward nvo3 acl extend enable**命令并重启单板生效，因为该命令生效后可以减少一个VXLAN业务所需要的KB资源；

按照如上建议，总共可以减少3个KB资源的占用，有利于叠加更多的业务。

在入方向VXLAN/EVPN场景中，需要首先配置VXLAN业务，之后再叠加其他业务。

入方向VXLAN/EVPN场景中不推荐使用的单板类型如下表所示：

接口板类型	不推荐的单板类型
GE	CE-L48GT-EA、CE-L48GT-EC、CE-L48GS-EA、CE-L48GS-EC、CE-L48GT-ED、CE-L48GS-ED
10GE	CE-L24XS-BA、CE-L24XS-EA、CE-L48XS-BA、CE-L48XS-EA
40GE	CE-L24LQ-EA
100GE	NA

现网中在入方向VXLAN/EVPN场景下经常使用的业务如下表所示：

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
协议报文上送	CPCARL3	系统默认下发	2	用户上送的IPv4协议类报文类型包括DHCP（Client、Server、Relay）、BFD、NTP、FTP、SSH、SNMP、Telnet、STP、VRRP、M-LAG等。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
VXLAN HASH	ECMPHASH	# ip tunnel mode vxlan # bridge-domain 10 l2 binding vlan 10 vxlan vni 5010 # interface Nve1 source 2.2.2.2 vni 5000 head-end peer-list 3.3.3.3 #	1	● 非增强模式下E系列单板配置VXLAN功能后，默认下发。 ● F系列单板只有在增强模式下通过执行命令**assign forward nvo3 ecmp hash enable**下发。 ● CE6870通过执行命令**assign forward nvo3 ecmp hash enable**下发。 ● 该分组不下发时，VXLAN报文只能基于内层IP地址Hash，不能基于内层的端口号Hash。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
	LAGHASH	# ip tunnel mode vxlan # bridge-domain 10 l2 binding vlan 10 vxlan vni 5010 # interface Nve1 source 2.2.2.2 vni 5000 head-end peer-list 3.3.3.3 #	1	● E系列单板配置VXLAN功能后，默认下发。执行**assign forward nvo3 eth-trunk hash disable**命令后，不下发该组。 ● F系列单板只有在增强模式下通过执行命令**assign forward nvo3 eth-trunk hash enable**才下发。 ● CE6870通过执行命令**assign forward nvo3 eth-trunk hash enable**下发。 ● 该分组不下时，VXLAN报文只能基于内层IP地址Hash，不能基于内层的端口号Hash。
EVPN MAC	EVN MAC Drif	# evpn-overlay enable # bridge-domain 666 vxlan vni 666 evpn #	1	EVPN场景下，用于支持静态MAC的虚拟机迁移功能（V200R001C00版本新增）

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
VXLAN DHCP Relay	VXLAN DHCP Relay	# dhcp enable # dhcp snooping enable # interface Vbdif20 dhcp select relay #	1	配置DHCP Relay。
VXLAN安全	VXLAN Security	# interface Nve1 source 1.1.1.1 vni 4096 head-end peer-list 1.1.1.12 ip source check user-bind peer-ip 1.1.1.12 enable #	1	配置VXLAN DHCP Snoop绑定表和NVE接口下的IPSG业务。
基于VBDIF接口的MQC报文过滤	MQC Vbdif	# traffic classifier n1 type or if-match vxlan tag-format none inner-protocol 6 inner-tcp-flag established # traffic behavior n1 deny # traffic policy n1 classifier n1 behavior n1 precedence 5 # interface Vbdif10 traffic-policy n1 inbound #	1	在VBDIF接口视图下配置流策略，可以匹配VXLAN报文内层源IP地址、目的IP地址、源端口号、目的端口号、协议类型、TCP Flag，可以执行的动作为permit、deny。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于VBDIF接口的MQC策略路由		# traffic classifier n2 type or if-match vxlan tag-format none inner-source-ip 10.10.1.3 mask 32 # traffic behavior n2 redirect nexthop 10.1.1.2 # traffic policy n2 classifier n2 behavior n2 precedence 5 #		在VBDIF接口视图下配置流策略，可以匹配VXLAN报文内层源IP地址、目的IP地址、源端口号、目的端口号、协议类型，动作为重定向。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于接口的MQC流量统计		# acl number 3000 rule 5 permit ip destination 10.1.0.0 0.0.255.255 # traffic classifier n3 type or **if-match vxlan acl 3000** # traffic behavior n3 statistics enable # traffic policy n3 classifier n3 behavior n3 precedence 5 #		在接口视图下配置流策略，匹配VXLAN报文内层源IP地址、目的IP地址、源端口号、目的端口号、协议类型，动作为统计。 ● E系列单板，NVO3网关的增强模式默认为环回模式。可以通过执行命令**assign forward nvo3-gateway enhanced** { **l2** | **l3** }修改NVO3网关的增强模式为非环回模式。 ● F系列单版，NVO3网关的增强模式为非环回模式。 ● CE6870，NVO3网关的增强模式为非环回模式。 ● 对于F系列单板和CE6870，支持执行命令**if-match vxlan**或者**if-match vxlan acl**来匹配VXLAN内层报文的字段。 ● 对于F系列单板，V200R002C50版本之前，VXLAN的NVO3网关增强模式为三层非环回模式

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
				时，仅支持执行命令**if-match vxlan**或者**if-match vxlan acl**来匹配VXLAN内层报文的字段；VXLAN的NVO3网关增强模式为环回模式或二层非环回模式时，仅支持执行命令**if-match acl**匹配VXLAN内层报文的字段。 V200R002C50版本及之后版本，无论VXLAN的NVO3网关增强模式为何种模式，仅支持执行命令**if-match vxlan**或者**if-match vxlan acl**来匹配VXLAN内层报文的字段，**if-match acl**不支持匹配VXLAN内层报文的字段。
基于BD视图的VXLAN报文统计	BD Statistics	# bridge-domain 10 statistics enable l2 binding vlan 10 vxlan vni 5010 #	1	● 在BD视图下使能VXLAN报文统计。 ● E系列单板下发该分组。 ● F系列单板不下发该分组。 ● CE6870不下发该分组。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于接口的MQC限速	MQC CAR	# acl number 3000 rule 5 permit ip source 10.1.0.0 0.0.255.255 # traffic classifier n4 type or if-match acl 3000 # traffic behavior n4 car cir 4000000 kbps # traffic policy n4 classifier n4 behavior n4 precedence 5 #	1	在接口视图下配置流策略，匹配VXLAN报文源IP地址、目的IP地址、内层VLAN、外层VLAN，动作为限速。
VXLAN隧道流量统计	VP statistics	# interface Nve1 source 10.1.1.1 vni 5010 head-end peer-list 10.1.1.2 vxlan statistics peer 10.1.1.2 vni 5010 enable #	1	在NVE接口下使能VXLAN隧道流量统计。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于二层子接口的sFlow	sFlow	# interface 40GE4/0/2 undo portswitch ip address 10.1.1.1 255.255.0.0 # sflow agent ip 10.1.1.1 # sflow collector 2 ip 10.1.1.2 # interface 40GE4/0/2.1 mode l2 encapsulation dot1q vid 10 bridge-domain 10 sflow sampling collector 2 sflow sampling rate 5000 sflow sampling inbound sflow counter collector 2 sflow counter interval 120 #	1	在VXLAN接入侧二层子接口下配置sFlow采样。
基于流的QoS优先级控制（underlay）	MQC Global	# acl number 3000 rule 5 permit ip destination 10.1.0.0 0.0.255.255 # traffic classifier r1 type or if-match acl 3000 # traffic behavior r1 remark local-precedence af1 # traffic policy r1 classifier r1 behavior r1 precedence 5 # traffic-policy r1 global inbound #	1	在全局配置MQC，匹配源IP地址和目的IP地址，用于修改报文队列优先级（remark local-precedence）。此特性通常需要在整网部署。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
报文过滤（underlay）	MQC Vlanif Filter	# acl number 3005 rule 5 permit ip source 10.10.10.10 0 destination 20.20.20.20 0 rule 10 permit tcp tcp-flag established # traffic classifier n1 type or if-match acl 3005 # traffic behavior n1 deny statistics enable # traffic policy n1 classifier n1 behavior n1 precedence 5 # interface 10GE4/0/2 undo portswitch traffic-policy n1 inbound #	1	在VLANIF、三层主接口、三层子接口上匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型、TCP Flag（例如established状态），动作为permit、deny，也可以同时配置统计。此特性通常部署在汇聚层。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
策略路由（underlay）	MQC PBR	# acl number 3005 rule 5 permit ip source 10.10.10.10 0 destination 20.20.20.20 0 rule 10 deny ip # traffic classifier n1 type or if-match acl 3005 # traffic behavior n6 # traffic policy n6 classifier n1 behavior n6 precedence 5 # interface 10GE4/0/4 undo portswitch traffic-policy n6 inbound #	1	在三层主接口上匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型，重定向到防火墙。此特性通常部署在汇聚层。
路径探测	Path Detect	# ip path detection enable #	1	AC控制器通过构造探测报文对网络中两个节点之间的IP路径进行探测，协助网络管理员发现故障路径。（V200R001C00版本新增）
关闭BD的MAC地址学习功能	BD MAC Not Learn	# bridge-domain 10 mac-address learning disable #	1	在BD视图下配置关闭MAC地址学习功能。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于BD视图的流量抑制	VNI BC Suppress	# bridge-domain 2 storm suppression broadcast cir 1000 kbps storm suppression multicast cir 1000 kbps storm suppression unknown-unicast cir 1000 kbps #	1	在BD视图下配置风暴抑制。

在配置VXLAN时，需要固定占用KB资源。其中协议报文上送业务默认下发CPCARL3占用2个KB资源；VXLAN HASH默认下发ECMPHASH和LAGHASH，分别占用一个KB资源，可以通过执行**assign forward nvo3 eth-trunk hash disable**命令使LAGHASH组不下发。

在配置上述表格中的业务时，只要使用的KB资源总数小于等于6个，则各业务无论以哪种顺序下发一般都可以保证叠加成功。

说明

配置ECMPHASH、VXLAN DHCP Relay、报文过滤（underlay）、策略路由（underlay）业务时，请按照ECMPHASH、VXLAN DHCP Relay、报文过滤（underlay）、策略路由（underlay）的顺序依次配置，否则部分业务可能下发失败。

注意

1. ED、EF、EG系列单板支持外扩TCAM，如果外扩TCAM为ACL分配了资源（其中EG系列单板默认分配了ACL资源，ED、EF系列单板默认未分配ACL资源），且MQC相关业务配置的视图、匹配字段、执行动作全部在以下所列条件的子集中时，则MQC业务会优先下发到外扩TCAM中：
   a. 视图：VLAN视图、VLANIF接口视图、GE接口视图、10GE接口视图、40GE接口视图、100GE接口视图、Eth-Trunk接口视图；
   b. 匹配字段：源IP地址、目的IP地址、源端口号、目的端口号、协议类型、ICMP Type、ICMP Code、TCP Flag、IP Fragment；
   c. 执行动作：Permit、Deny、Redirect、Remark、Mirror、Mac-address Learning Disable。
2. 当MQC下发到外扩TCAM中时，需要消耗1或2个KB资源。如果KB资源不足时，建议取消外扩TCAM为ACL分配的资源，方法是配置TCAM模板并绑定单板，然后配置除ACL资源之外的其他资源，具体参见“**CloudEngine 12800产品文档-配置-配置指南-设备管理配置-硬件管理-配置单板外扩TCAM的资源规格**”。此时MQC业务占用的KB资源如上述列表中所示。

说明

- 如果单独执行Deny/Redirect或Remark动作，则占1个KB资源。
- 如果同时执行Deny/Redirect和Remark动作，则占2个KB。

3. 如果用MQC匹配传输设备上的内层VXLAN报文，需要执行命令**if-match vxlan** [**transit**] [**tag-format** { **none** | **single** }] **acl** { *acl-number* | *acl-name* }，此时需要消耗2个KB资源，但是在传输设备上没有任何VXLAN隧道的配置，不会下发上表中的VXLAN相关业务，所以在传输设备上不会出现ACL资源不足的问题。

2、出方向 VXLAN/EVPN 业务叠加场景

VXLAN/EVPN场景中出方向上常用的业务如下表所示：

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
M-LAG	Port Isolate	配置M-LAG业务时，在设备本端M-LAG成员口Down或两端M-LAG成员口均UP的场景下，出方向下发该组	1	通常部署在接入层和汇聚层。
报文出接口查询	Out Port Get	# display port forwarding-path dst-ip 1.1.1.1 #	1	执行**display port forwarding-path**命令查看报文的出接口时下发该组，查询到结果后，删除该组。占用的KB资源数目和查询条件有关。
VXLAN隧道流量统计	VP statistics	# interface Nve1 source 10.1.1.1 vni 5010 head-end peer-list 10.1.1.2 vxlan statistics peer 10.1.1.2 vni 5010 enable #	1	在NVE接口下使能VXLAN隧道流量统计。 F系列单板在增强模式不下发该组。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于二层子接口的sFlow	sFlow	# interface 40GE4/0/2 undo portswitch ip address 10.1.1.1 255.255.0.0 # sflow agent ip 10.1.1.1 # sflow collector 2 ip 10.1.1.2 # interface 40GE4/0/2.1 mode l2 encapsulation dot1q vid 10 bridge-domain 10 sflow sampling collector 2 sflow sampling rate 5000 sflow sampling outbound sflow counter collector 2 sflow counter interval 120 #	1	在VXLAN接入侧二层子接口下配置sFlow采样。

VXLAN/EVPN场景中出方向KB资源和入方向KB资源不同，仅有2个，所以能够支持叠加的业务数目也要少很多。

报文出接口查询业务所占用的KB资源的数目和查询条件有关，如果报文出接口查询业务下发失败，可以减少匹配条件。例如当报文出接口查询业务基于IP地址或者MAC地址查询时占用1个KB资源，这种情况下可以和M-LAG业务叠加。

在出方向VXLAN/EVPN业务叠加场景中，BDIF出接口不支持配置MQC业务。

2.1.4.2 CSS/M-LAG 业务叠加场景

M-LAG业务在入方向下发到默认下发的CPCARL3组中，不需要占用额外的ACL资源；在出方向上M-LAG业务需要占用1个组。

1、入方向 CSS/M-LAG 业务叠加场景

CSS/M-LAG 场景中入方向上常用的业务如下表所示：

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
协议报文上送	CPCARL3	系统默认下发	2	用户上送的IPv4协议类报文类型包括DHCP（Client、Server、Relay）、BFD、NTP、FTP、SSH、SNMP、Telnet、STP、VRRP、M-LAG等。
VLANIF接口视图下的流量统计统计	L3 Statistics	# interface Vlanif16 ip address 10.1.1.1 255.255.255.0 statistics enable #	1	通常部署在汇聚层。
策略路由	MQC PBR	# acl number 3002 rule 5 permit ip destination 10.1.0.0 0.0.255.255 # traffic classifier n1 type or if-match acl 3002 # traffic behavior n1 redirect nexthop 10.2.1.2 # traffic policy n1 classifier n1 behavior n1 precedence 5 #	1	在接口（通常为网络侧接口）、VLAN、VLANIF上匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型，重定向到防火墙。此特性通常部署在汇聚层。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
流镜像	MQC Mirror	# acl number 3003 rule 5 deny ip source 10.1.1.0 0.0.0.255 # traffic classifier c type or if-match acl 3003 # traffic behavior c mirroring observe-port 1 # traffic policy c classifier c behavior c precedence 5 # interface 10GE1/0/3 traffic-policy c inbound #		在接口下匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型进行流镜像。该特性可以部署在接入层、汇聚层、核心层。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
报文过滤	MQC Vlanif Filter	# acl number 3005 rule 5 permit ip source 10.10.10.10 0 destination 10.20.20.20 0 rule 10 permit tcp tcp-flag established # traffic classifier n1 type or if-match acl 3005 # traffic behavior n1 deny statistics enable # traffic policy n1 classifier n1 behavior n1 precedence 5 # interface 10GE4/0/2 undo portswitch traffic-policy n1 inbound #	1	在VLANIF接口、三层主接口、三层子接口上匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型、TCP Flag（例如established状态），动作为permit、deny，也可以同时配置统计。此特性通常部署在汇聚层。
流量抑制	QoS CAR	# vlan 16 storm suppression broadcast cir 100 kbps storm suppression multicast cir 80 kbps storm suppression unknown-unicast cir 100 kbps #	1	在VLAN视图下配置广播、组播、未知单播的流量抑制。通常部署在接入层和汇聚层。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
接口入方向报文限速		# qos car qoscar1 cir 10000 kbps cbs 10240 bytes # interface 10GE1/0/2 undo portswitch qos car inbound qoscar1 #		在接口的入方向配置报文限速功能。动作为统计。通常部署在接入层。
MQC流量统计	MQC Port Statistics	# acl number 3003 rule 5 permit ip source 10.10.10.10 0 destination 10.20.20.20 0 # traffic classifier mqc_l3 type or if-match acl 3003 # traffic behavior mqc_l3 statistics enable # traffic policy mqc_l3 classifier mqc_l3 behavior mqc_l3 precedence 5 # interface 10GE3/0/5 traffic-policy mqc_l3 inbound #	1	在接口下匹配源IP地址、目的IP地址进行流量统计时，下发该组；当匹配源端口号或目的端口号时，会复用报文过滤的组。该特性通常在全网部署。
VLAN视图下的流量统计	VLAN Statistics	# vlan 100 statistics enable #	1	在VLAN视图下使能流量统计。通常部署在接入层和汇聚层。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
基于流的QoS优先级控制	MQC Global	# acl number 3000 rule 5 permit ip destination 10.1.0.0 0.0.255.255 # traffic classifier r1 type or if-match acl 3000 # traffic behavior r1 remark local-precedence af1 # traffic policy r1 classifier r1 behavior r1 precedence 5 # traffic-policy r1 global inbound #	1	在全局下配置MQC，匹配源IP地址和目的IP地址，用于修改报文队列优先级（remark local-precedence）。该特性通常需要在整网部署。
级联MQC	MQC Cascade	# acl number 3000 rule 5 permit tcp tcp-flag rst # traffic classifier c type or if-match acl 3000 # traffic behavior b deny # traffic policy p classifier c behavior b precedence 5 # interface 10GE1/0/2 undo portswitch traffic-policy p outbound #	1	因为芯片存在出向无法匹配分片字段和TCP Flag的限制，所以当在出方向配置MQC匹配端口号或是TCP Flag时，入方向下发该组，用于匹配分片标记和TCP Flag，并将匹配结果由报文内部头携带到下行。

在配置上述表格中的业务时，只要使用的KB资源总数小于等于6个，则各业务无论以哪种顺序下发一般都可以保证叠加成功。

说明

- 基于流的QoS优先级控制、策略路由、流量抑制、报文过滤业务叠加时请按照报文过滤、策略路由、基于流的QoS优先级控制、流量抑制的顺序配置，否则部分业务可能下发失败。
- VLANIF接口视图下的流量统计、策略路由、报文过滤、级联MQC业务不支持叠加。

注意

1. ED、EF、EG系列单板支持外扩TCAM，如果外扩TCAM为ACL分配了资源（其中EG系列单板默认分配了ACL资源，ED、EF系列单板默认未分配ACL资源），且MQC相关业务配置的视图、匹配字段、执行动作全部在以下所列条件的子集中时，则MQC业务会优先下发到外扩TCAM中：
   a. 视图：VLAN视图、VLANIF接口视图、GE接口视图、10GE接口视图、40GE接口视图、100GE接口视图、Eth-Trunk接口视图；
   b. 匹配字段：源IP地址、目的IP地址、源端口号、目的端口号、协议类型、ICMP Type、ICMP Code、IP Fragment；
   c. 执行动作：Permit、Deny、Redirect、Remark、Mirror、Mac-address Learning Disable。
2. 当MQC下发到外扩TCAM中时，需要消耗1或2个KB资源。如果KB资源不足时，建议取消外扩TCAM为ACL分配的资源，方法是配置TCAM模板并绑定单板，然后配置除ACL资源之外的其他资源，具体参见“**CloudEngine 12800产品文档-配置-配置指南-设备管理配置-硬件管理-配置单板外扩TCAM的资源规格**”。此时MQC业务占用的KB资源如上述列表中所示。

   说明

   - 如果单独执行Deny/Redirect或Remark动作，则占1个KB资源。
   - 如果同时执行Deny/Redirect和Remark动作，则占2个KB。
3. 如果外扩TCAM为组播分配了资源，则组播业务会下发到外扩TCAM中，并消耗2个KB资源。当KB资源不足时，建议取消外扩TCAM为组播分配的资源，方法是配置TCAM模板并绑定单板，然后配置除组播资源之外的其他资源，具体参见“**CloudEngine 12800产品文档-配置-配置指南-设备管理配置-硬件管理-配置单板外扩TCAM的资源规格**”。

2、出方向 CSS/M-LAG 业务叠加场景

CSS/M-LAG 场景中出方向上常用的业务如下表所示：

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
VLANIF统计	L3 Statistics	# interface Vlanif16 ip address 10.1.1.1 255.255.255.0 statistics enable #	1	通常部署在汇聚层。
M-LAG	Port Isolate	配置M-LAG业务时，在设备本端M-LAG成员口Down或两端M-LAG成员口均UP的场景下，出方向下发该组	1	通常部署在接入层和汇聚层。
出方向报文过滤	MQC Vlanif Filter	# acl number 3005 rule 5 permit ip source 10.10.10.10 0 destination 10.20.20.20 0 rule 10 permit tcp tcp-flag established # traffic classifier n1 type or if-match acl 3005 # traffic behavior n1 deny # traffic policy n1 classifier n1 behavior n1 precedence 5 # interface Vlanif10 traffic-policy n1 outbound #	1	在VLAN、VLANIF接口下的出向应用MQC，匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型、TCP Flag，动作为permit、deny。
报文出接口查询	Out Port Get	# display port forwarding-path dst-ip 1.1.1.1 #	1	执行**display port forwarding-path**命令查看报文的出接口时下发该组，查询到结果后，删除该组。占用的KB资源数目和查询条件有关。

CSS/M-LAG 场景中出方向KB资源和入方向KB资源不同，仅有2个，所以能够支持叠加的业务数目也要少很多。

在V100R006C00版本及以后版本中VLANIF统计、M-LAG、报文过滤业务中任选两个都可以保证业务下发成功。

报文出接口查询业务所占用的KB资源的数目和查询条件有关，如果报文出接口查询业务下发失败，可以减少匹配条件。例如当报文出接口查询业务基于IP地址或者MAC地址查询时占用1个KB资源，这种情况下可以和其他三个业务中的任意一个叠加。

2.1.4.3 FCoE 业务叠加场景

1、入方向 FCoE 业务叠加场景

FCoE场景中入方向经常使用的业务如下表所示：

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
协议报文上送	CPCARL3	系统默认下发	2	用户上送的IPv4协议类报文类型包括DHCP（Client、Server、Relay）、BFD、NTP、FTP、SSH、SNMP、Telnet、STP、VRRP、M-LAG等。
FSB	FCOE	# fcoe 1 vlan 2501 # interface 10GE1/0/3 port link-type trunk port trunk allow-pass vlan 2501 #	2	配置FSB或FCF场景。
FCF		# fcoe fcf1 fcf vlan 2501 #		

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
FCF统计	FCOESTAT	# interface FCoE-Port1 statistic enable #	1	FCF端口流量统计。
策略路由	MQC_213	# acl number 3002 rule 5 permit ip destination 10.1.1.0 0.0.255.255 # traffic classifier n1 type or if-match acl 3002 # traffic behavior n1 redirect nexthop 10.2.2.2 # traffic policy n1 classifier n1 behavior n1 precedence 5 #	1	在接口（通常为网络侧接口）、VLAN、VLANIF上匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型，重定向到防火墙。此特性通常部署在汇聚层。
流镜像		# acl number 3003 rule 5 deny ip source 10.1.1.0 0.0.0.255 # traffic classifier c type or if-match acl 3003 # traffic behavior c mirroring observe-port 1 # traffic policy c classifier c behavior c precedence 5 #		在接口下匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型进行流镜像。该特性可以部署在接入层、汇聚层、核心层。

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
报文过滤	MQC Vlanif Filter	# acl number 3005 rule 5 permit ip source 10.1.1.1 24 destination 10.1.2.2 24 # traffic classifier n1 type or if-match acl 3005 # traffic behavior n1 deny # traffic policy n1 classifier n1 behavior n1 precedence 5 #	1	在VLANIF接口、三层主接口、三层子接口上匹配源IP地址、目的IP地址，动作为permit、deny，也可以同时配置统计。此特性通常部署在汇聚层。
VLANIF接口视图下的流量统计	L3 Statistics	# interface Vlanif16 ip address 10.1.1.1 255.255.255.0 statistics enable #	1	在VLANIF接口视图下配置流量统计，通常部署在汇聚层。

在FCoE场景中，协议报文上送业务默认下发CPCARL3占用2个KB资源。

在配置上述表格中的业务时，只要使用的KB资源总数小于等于6个，则各业务无论以哪种顺序下发一般都可以保证叠加成功。

2、出方向 FCoE 叠加场景

出方向FCOE叠加场景中经常使用到的业务，如下表所示：

业务	Group	命令行（配置该命令后，会下对应的Group）	占用KB资源	备注
M-LAG	Port Isolate	配置M-LAG业务时，在设备本端M-LAG成员口Down或两端M-LAG成员口均UP的场景下，出方向下发该组	1	通常部署在接入层和汇聚层。

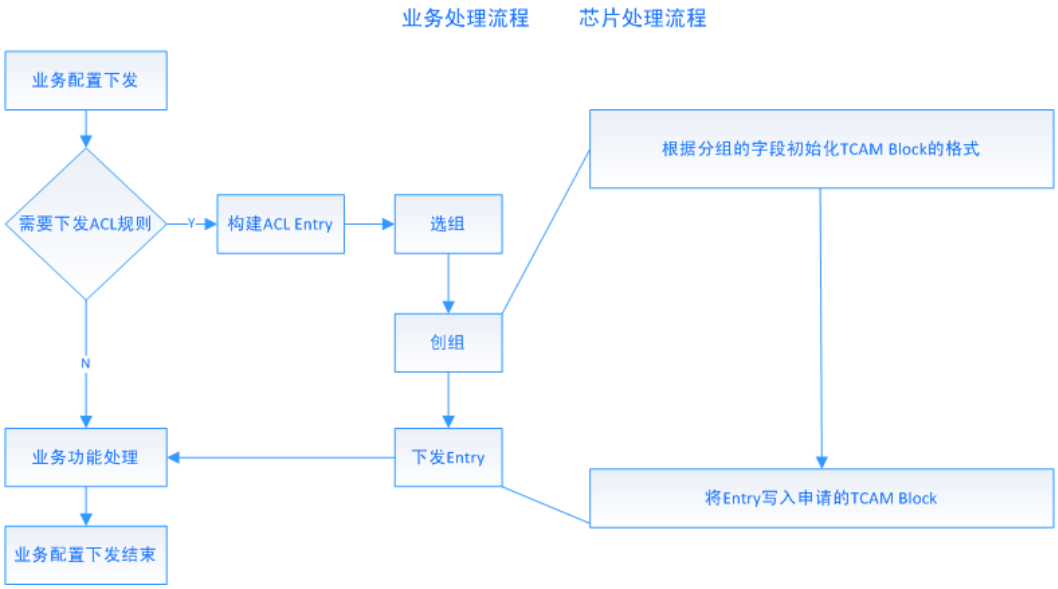
在出方向FCOE场景中，仅下发M-LAG分组，可以保证下发成功。

2.2 业务与 ACL（CE12800 和 CE6870 除外）

2.2.1 概述

ACL功能非常强大，一方面用户可以直接配置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依赖ACL完成，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。比如VLANIF流量统计业务，需要下发ACL针对对应VLANIF的流量进行统计。

业务下发ACL规则流程和对应的芯片处理流程如下图所示。



分组的选择方式有两种：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；一种是动态选组，即需要根据用户配置字段和动作信息去遍历预定义好的分组模板，找到一个合适的分组，该选组方式主要用于MQC业务。

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业务。当用户配置的MQC流策略时，会配置ACL规则，所以属于显式使用ACL的业务；当用户使能IPv6业务时，虽然会下发用于处理IPv6协议报文的ACL，但是用户没有直观的感知，所以就属于隐式的使用ACL的业务。

2.2.2 隐式使用 ACL 的业务

2.2.2.1 概述

由于业务应用场景需要，当使能一些配置时，如VXLAN、TRILL、MPLS、IPv6等业务，也会下发ACL规则进行某些处理，例如用于实现协议报文捕获等功能，但是不需要用户增加ACL的配置，ACL的作用不会被用户直接感知。又比如用于邻居设备发现的LLDP功能，用户能看到的是本设备的邻居设备信息，ACL负责捕获LLDP协议报文送给业务处理，作为整个LLDP功能的一个环节，也不为用户感知。

隐式使用ACL的业务，下发ACL规则时，选组的方式是静态选组。

2.2.2.2 默认下发的业务

为保证基础二三层业务默认可用，设备启动之后，会默认下发一个8号ACL分组，用于捕获基础二三层协议报文到CPU处理的ACL业务下发，如ARP、ICMP等协议。

分组ID	分组模式	业务名称
8	Double	ARP、BPDU、STP、LACP等协议报文捕获业务

通过诊断命令**display system tcam service brief** [**slot** *slot-id*]查看业务ACL规则下发情况：

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
-------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                  Count
-------------------------------------------------------------------------------
    0        8    Double     Ingress        CPCAR                           36
             8    Double     Ingress        L2 Protocol Tunnel               1
-------------------------------------------------------------------------------
```

2.2.2.3 其他配置类业务

除了默认下发的业务外，部分配置类业务也会隐式的使用ACL，例如：

Group ID	分组模式	业务名称
9	Double	MFF LACP
10	Double	Storm Control
19	Double	QoS CAR BD statistics
21	Double	FCoE
26	Single	ERPS
28	Double	VXLAN

例如，在接口下使能storm control业务后，会占用额外的ACL资源：

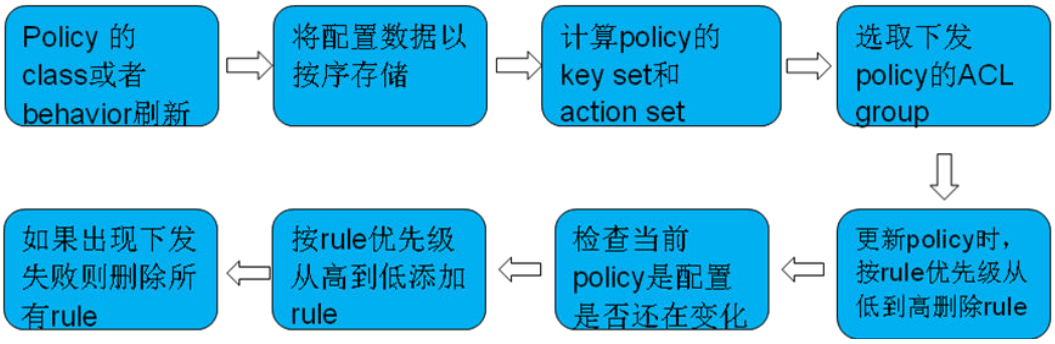
```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
-------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                  Count
-------------------------------------------------------------------------------
    0        8    Double     Ingress        CPCAR                           36
             8    Double     Ingress        L2 Protocol Tunnel               1
            10    Double     Ingress        Storm Ctrl BC Pass               1
            10    Double     Ingress        Storm Ctrl MC Query              1
-------------------------------------------------------------------------------
```


2.2.3 显式使用 ACL 的业务

MQC业务属于显示使用ACL的业务，因为MQC业务的ACL规则信息是用户配置的，用户可以感知到。用户可以指定匹配具备某些特征的报文，对其进行统计、限速、丢弃等处理。

MQC对用户赋予的配置灵活性是非常高的，理论上可以指定匹配任意内容和执行任意动作。MQC业务在下发ACL规则时，分组的选择是根据用户配置决定的，采用动态方式进行选组。当一个流策略绑定到一个视图下，称之为一个流策略应用实例。每个流策略应用实例都会进行选组，流策略应用实例与分组可能是一对一的关系，也可能是多对一的关系。

MQC业务的下发流程如下：



2.2.3.1 MQC 分组模板

产品预先定义了很多MQC分组模板，用于不同配置时进行选择。以V200R002C50版本为例，MQC业务部分预定义分组模板信息如下：

GroupID	Slice个数	报文格式	匹配条件	动作	应用视图
31	1	IPv4	SID、DIP、分片	丢弃、重定向、统计、镜像、限速、重标记	Interface/Vlan
34	1	IPv4	IP五元组、分片	丢弃、重定向、统计、镜像、限速、重标记	Interface/Vlan

2.2.4 ACL 业务叠加场景

当前现网中使用到硬件ACL资源的业务在相互叠加时，可能会出现ACL资源不足的问题。所以本章节对ACL业务典型的叠加场景做一个总结，用来指导用户部署相关业务。

2.2.4.1 FCoE 业务叠加场景

1、入方向 FCoE 叠加场景

入方向FCoE叠加场景中经常使用到业务如下表所示：

业务	ACL Group		配置命令	需要Slice资源数量		备注
NA	CE8860EI、CE8850EI和CE6860EI除外	CE8860EI、CE8850EI和CE6860EI	NA	CE8860EI、CE8850EI和CE6860EI除外	CE8860EI、CE8850EI和CE6860EI	NA
协议报文上送	CPCAR_8	CPCAR_8	系统默认下发	2	2	用户上送的IPv4协议类报文类型包括DHCP（Client、Server、Relay）、BFD、NTP、FTP、SSH、SNMP、Telnet、STP、VRRP、M-LAG等。
FSB场景	Service_21	Service_21	# fcoe 1 vlan 2501 # interface 10GE1/0/3 port link-type trunk port trunk allow-pass vlan 2501 #	1	2	创建FSB实例。

业务	ACL Group		配置命令	需要Slice资源数量		备注
	Service_22	Service_22	# fcoe routing 3.3.3 255.255.255 4.4.4 255.255.255 interface 25GE3/4/1 source-mac 0efc-0010-0004 vlan 2501 destination-mac 1-1-1 #	2	3	在系统视图下配置FCoE重定向。
FCF场景	Service_10	Service_29	# interface FCoE-Port1 statistic enable #	2	1	配置FCoE接口的流量统计功能。
	Service_22	Service_22	# fcoe fcf1 fcf vlan 2501 #	2	3	创建FCF实例。
	Service_23	Service_23	用户上线	2	3	用户上线时下发该组。
接口ARP报文限速	Service_28	Service_66	# arp anti-attack rate-limit interface 10 #	2	1	限制接口下ARP报文的速率。
VXLAN路径探测	Service_22	Service_22	# ip path detection enable #	2	3	AC控制器通过构造探测报文对VXLAN网络的路径进行探测，协助网络管理员发现故障路径。
隧道统计	Service_19	NA	# vxlan statistics peer 2.2.2.2 vni 5010 enable #	2	0	在NVE视图下配置VXLAN隧道的流量统计。

业务	ACL Group		配置命令	需要Slice资源数量		备注
BD视图下的流量抑制	Service_28 **说明** CE6855HI和CE7855HI占用Service_19组	Service_19	# bridge-domain 100 storm suppression broadcast cir 100 mbps vxlan vni 5000 #	2	1	在BD视图下配置流量抑制功能。
基于流的QoS优先级控制（Underlay）	MQC_38	MQC_35	# acl number 3000 rule 10 permit ip source 10.1.1.1 0 destination 10.2.2.2 0 # # traffic classifier cc type or if-match acl 3000 # # traffic behavior bb remark local-precedence af1 # # traffic policy pp classifier cc behavior bb precedence 5 #	1	1	在全局配置MQC，匹配SIP/DIP，修改报文队列优先级（remark local-precedence）。

业务	ACL Group		配置命令	需要Slice资源数量		备注
流量统计（Underlay）	MQC_41	MQC_35	# acl number 3000 rule 5 permit tcp source 10.1.1.1 0 destination 10.2.2.2 0 destination-port eq 1024 # # traffic classifier cc type or if-match acl 3000 # # traffic behavior bb statistics enable # # traffic policy pp classifier cc behavior bb precedence 5 #	1	1	在端口配置MQC，匹配源IP地址、目的IP地址、源端口号、目的端口号、协议类型，进行流量统计。
M-LAG场景	Service_19	Service_12	# interface Eth-Trunk10 peer-link 1 #	2	1	双归接入和流量隔离，通常部署在接入层和汇聚层。
	Service_10	Service_10	# interface Eth-Trunk11 dfs-group 1 m-lag 1 #	2	2	

上述表格中的Group ID和设备显示可能有所差异，只是用来说明不同业务是否下发到同一个分组。

在入方向FCoE场景中，如果多个业务下发到相同的Group中，且此Group已经建立，则不会再额外占用Slice资源。例如对于CE8860EI设备，基于流的QoS优先级控制（Underlay）和流量统计（Underlay）业务都是占用MQC_35分组，当两个业务同时配置时，只需要占用1个Slice资源。

当剩余的Slice资源满足要求时，可以保证业务叠加成功。

Slice资源的要求如下：

Slice资源从0开始编号，依次为0，1，2，3，4……。一个Group根据宽度的不同，需要申请1个、两个或三个Slice资源。但是当需要两个Slice资源时，这两个Slice的编号必须以偶数开始且连续，例如0和1，4和5等；当需要三个Slice资源时，这三个Slice资源的编号必须以3的倍数开始且连续，例如0至2，3至5等。

2、出方向 FCoE 叠加场景

出方向FCoE叠加场景中经常使用到的业务如下表所示：

业务	ACL Group		配置命令	需要Slice资源数量		备注
NA	CE8860EI、CE8850EI和CE6860EI除外	CE8860EI、CE8850EI和CE6860EI	NA	CE8860EI、CE8850EI和CE6860EI除外	CE8860EI、CE8850EI和CE6860EI	NA
FSB场景	Service_77	Service_77	# fcoe 1 vlan 2501 # interface 10GE1/0/3 port link-type trunk port trunk allow-pass vlan 2501 fcoe role vnp #	2	2	创建FSB实例。
FCF场景	Service_79	Service_79	# interface FCoE-Port1 statistic enable #	1	1	FCoE端口下使能流量统计。
隧道统计			# vxlan statistics peer 2.2.2.2 vni 5010 enable #			入方向配置隧道统计时，出方向下发下发该组。

上述表格中的Group ID和设备显示可能有所差异，只是用来说明不同业务是否下发到同一个分组。

在出方向FCoE场景中，仅需要占用3个Slice资源，可以保证业务下发成功。

3 ACL 应用最佳实践

文档中命令的回显如果没有特别说明都以V200R002C50版本为例。

3.1 减少组资源的占用（使用 TCAM ACL 资源自定义分组重新规划匹配字段和执行动作）

3.1.1 原理介绍

默认情况，用户配置的业务都下发到系统预置的分组中。系统预置的分组为了满足不同用户的需求，包含较多的匹配字段和动作，无法做到ACL资源的最大化利用。为了更好的满足客户的定制需求，设备提供了一种开放式的硬件资源可编程能力——TCAM ACL资源自定义。

通过TCAM ACL资源自定义功能，用户可以创建自定义的ACL资源分组，指定分组包含的匹配条件、动作和优先级，业务在下发时优先使用用户创建的自定义分组。通过这种方式，减少了下发到芯片中分组的冗余字段，从而实现用户需求和芯片资源的最优匹配。

3.1.2 应用场景

3.1.2.1 1：应用多个 traffic policy 包含不同匹配字段

用户下发多个traffic policy，包含的匹配字段不相同，使用系统预置分组下发时会占用多个分组。通过配置TCAM ACL资源自定义分组，分组中包含多个traffic policy中所有的匹配字段和执行动作，系统在选择分组时会优先选择配置的自定义分组，最终只创建一个分组，从而节省了分组资源。

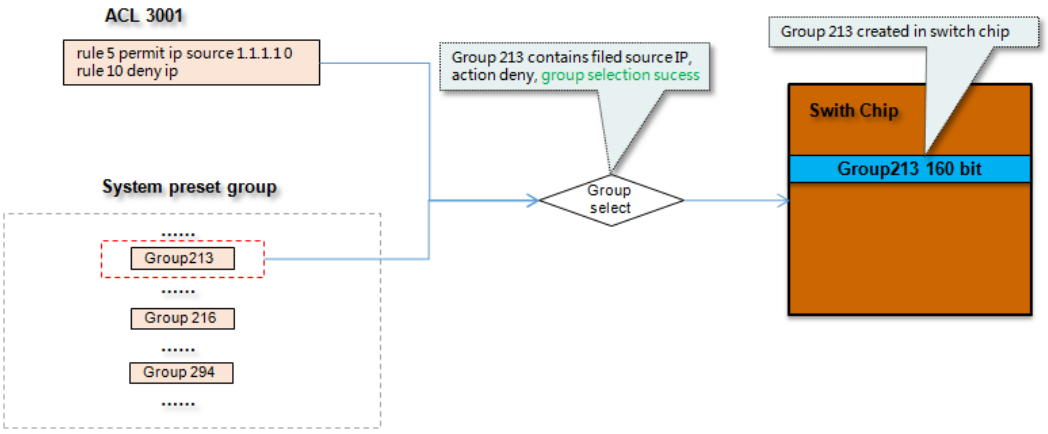
例如系统包含如下三个预置分组供traffic policy选取：

分组ID	分组模式	字段集合	动作集合
213	160bit	Source IP Destination IP Source Interface VSI	Redirect Interface Deny Statistics
216	160bit	Source IP Destination IP L4 Source Port L4 Destination Port IP Protocol IP Fragment Type Source Interface VSI	Redirect Interface Deny Remark DSCP Mirror
294	160bit	Source IP Destination IP L4 Source Port L4 Destination Port IP Protocol TCP Flag IP Fragment Type Source Interface VSI	Redirect Interface Deny Statistics

配置acl 3001，匹配source IP，执行动作deny：

```
#
acl 3001
 rule 5 permit ip source 1.1.1.1 0
 rule 10 deny ip
#
```

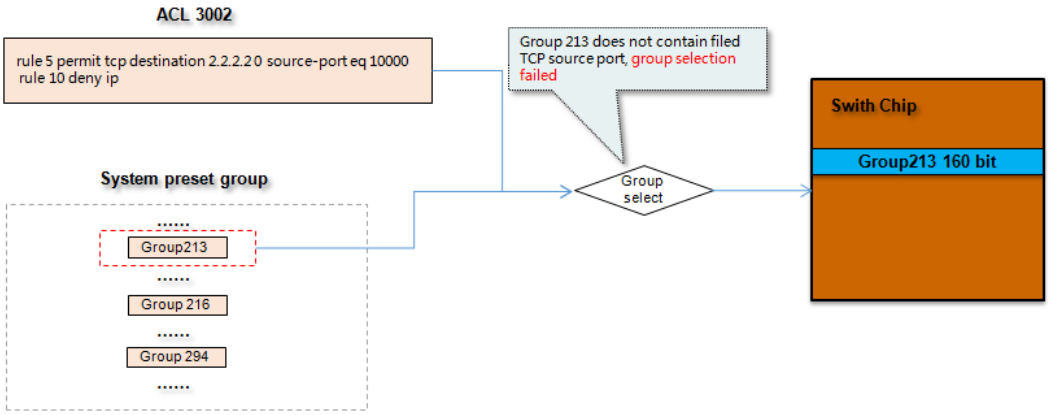
Group 213包含source IP字段和deny动作，满足需求，在芯片中创建分组Group 213。



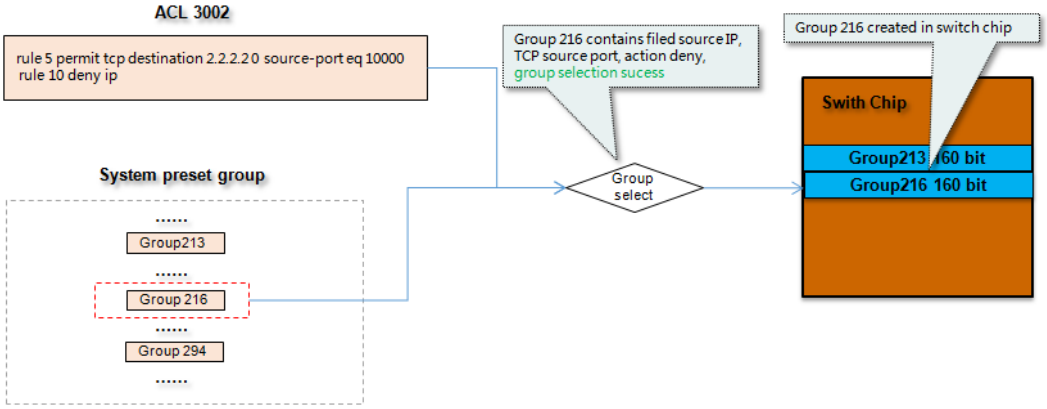
配置acl 3002，匹配destination IP和 source TCP port。

```
#
acl 3002
 rule 5 permit tcp destination 2.2.2.2 0 source-port eq 10000
 rule 10 deny ip
#
```

由于Group 213中不包含source TCP port字段，无法下发到Group 213，因此继续查找其他系统预置模板。



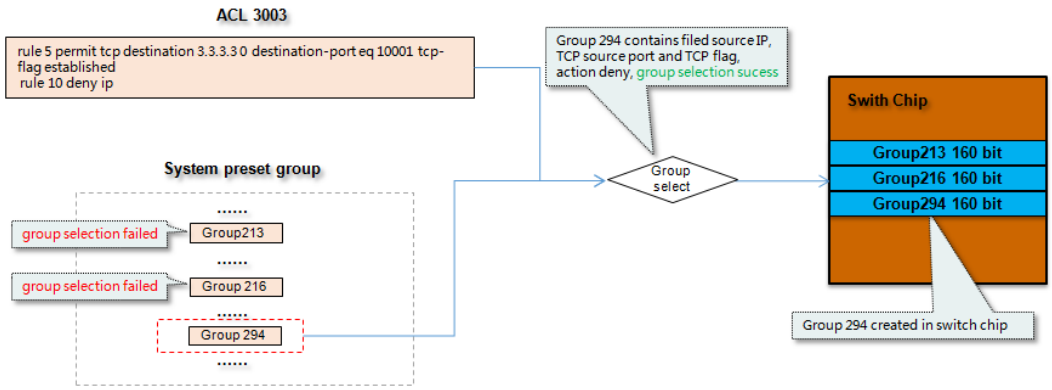
Group 216包含规则中字段和动作，满足需求，在设备上创建Group 216。



配置acl 3003，匹配destination IP，destination TCP port和TCP flag。

```
#
acl 3003
 rule 5 permit tcp destination 3.3.3.3 0 destination-port eq 10001 tcp-flag established
 rule 10 deny ip
#
```

原理同上，由于Group 213中不包含source TCP port字段，无法下发到Group 213；Group 216中不包含TCP flag字段，无法下发到Group 216，继续查找其他系统预置模板；Group 294包含规则中字段和动作，满足需求，因此在设备上创建Group 294。

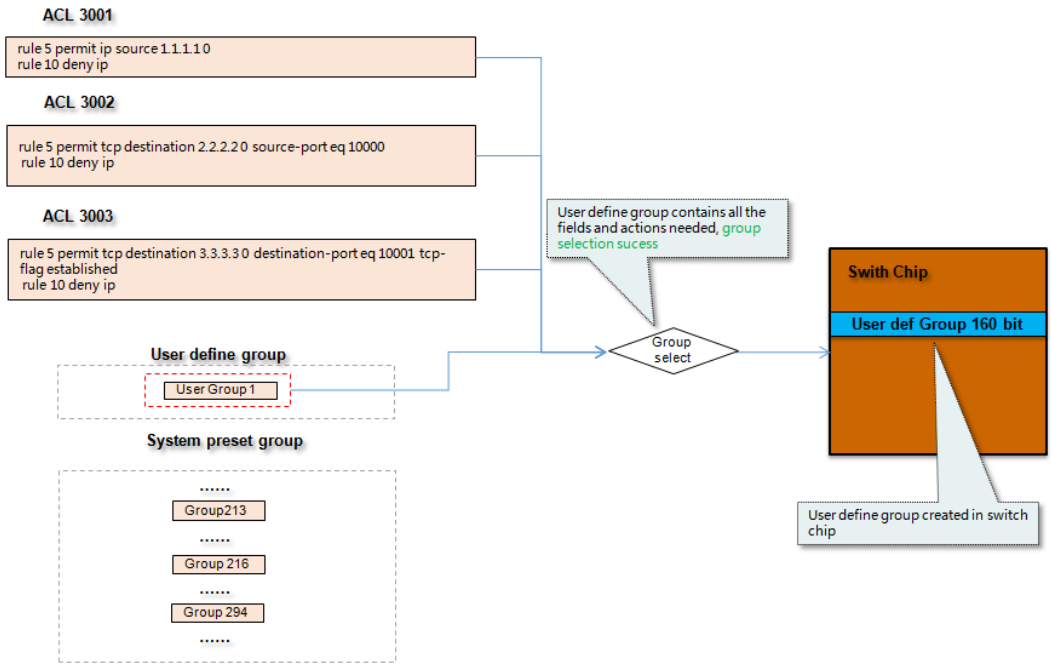


最终，用户应用了3个traffic policy，由于匹配字段的差异，选择了3个不同的系统预置分组，占用了3个芯片group资源。

可以使用如下TCAM ACL资源自定义分组减少traffic policy占用的group资源个数：

分组ID	分组模式	字段集合	动作集合
User Define Group	160bit	Source IP Destination IP L4 Source Port L4 Destination Port IP Protocol TCP Flag IP Fragment Type Source Interface VSI	Deny

在traffic policy进行选组时会优先判断用户配置的TCAM ACL资源分组是否能满足需求，因为用户配置的TCAM ACL资源自定义分组包含acl 3001、acl 3002、acl 3003匹配的所有字段和执行的动作，所以acl 3001、acl 3002、acl 3003对用户配置的TCAM ACL资源分组选组成功，不再下发到系统预置分组。



最终，通过配置TCAM ACL自定义模板，用户应用了3个traffic policy，包含不同的匹配字段，仅占用了1个芯片group资源。

3.1.2.2 2：应用多个 traffic policy 执行不同动作

用户下发多个traffic policy，执行不同的动作，使用系统预置分组下发时也会占用多个分组。通过配置TCAM ACL资源自定义分组，分组中包含多个traffic policy中所有的匹配字段和执行动作，系统在选择分组时会优先选择配置的自定义分组，最终只创建一个分组，从而节省了分组资源。

例如系统包含如下两个预置分组供traffic policy选取：

分组ID	分组模式	字段集合	动作集合
213	160bit	Source IP Destination IP Source Interface VSI	Redirect Interface Deny Statistics
295	160bit	Source IP Destination IP L4 Source Port L4 Destination Port IP Protocol IP Fragment Type Source Interface VSI	Redirect Interface Deny Car

如果配置如下：

1、配置acl 3001，匹配source IP，动作deny：

```
#
acl 3001
 rule 5 permit ip source 1.1.1.1 0
 rule 10 deny ip
#
```

2、配置traffic policy statistics，匹配acl 3001，动作为统计：

```
#
traffic classifier statistics
 if-match acl 3001
traffic behavior statistics
 statistics enable
traffic policy statistics
 classifier statistics behavior statistics
#
```

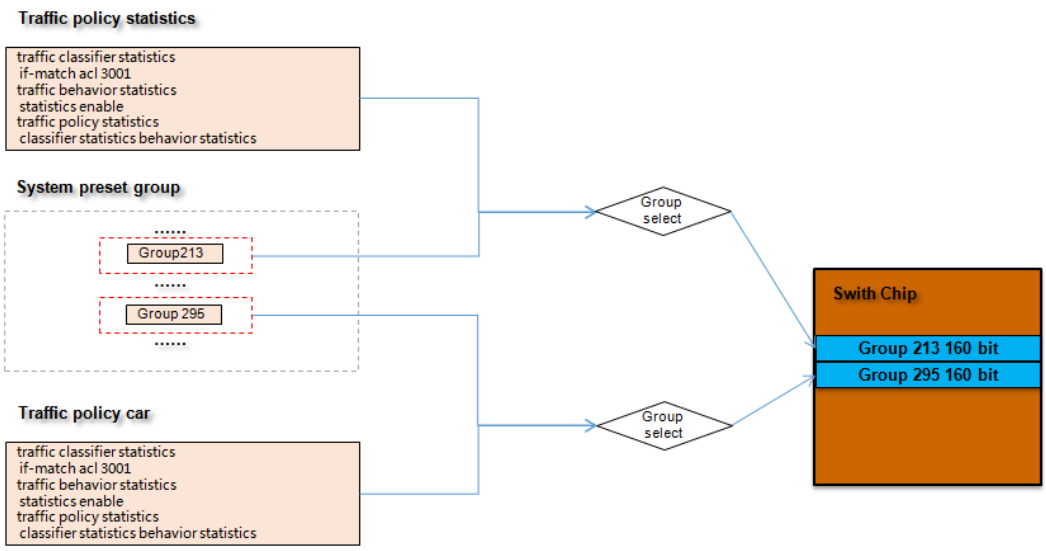
3、配置traffic policy car，匹配acl 3001，动作为car：

```
#
traffic classifier car
 if-match acl 3001
traffic behavior car
 statistics car
traffic policy car
 classifier car behavior car
#
```

按照系统预置分组，Group 213包含字段source IP address和动作statistics，满足traffic policy statistics需求，因此创建分组Group 213。

由于Group 213不包含car动作，而traffic policy car包含car动作，无法下发到Group 213，继续查找其他分组。

Group 295包含字段source IP address和动作car，满足traffic policy car需求，因此创建分组Group 295。

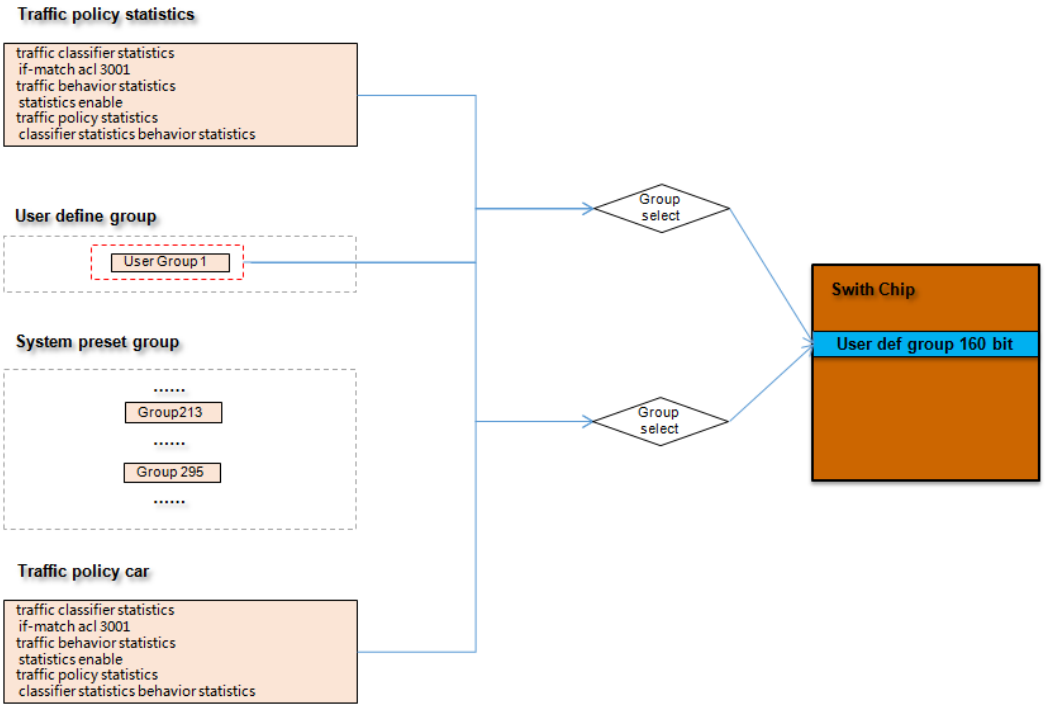


最终，用户应用了2个traffic policy，由于执行动作的差异，选择了2个不同的系统预置分组，占用了2个芯片group资源。

可以使用如下TCAM ACL资源自定义分组减少traffic policy占用的group资源个数：

分组ID	分组模式	字段集合	动作集合
User Define Group	160bit	Source IP Destination IP L4 Source Port L4 Destination Port IP Protocol TCP Flag IP Fragment Type Source Interface VSI	Statistics car

在traffic policy进行选组时会优先判断用户配置的TCAM ACL资源分组是否能满足需求，用户配置的TCAM ACL资源自定义分组包含source IP address和statistics、car动作，所以traffic policy statistics、traffic policy car对用户配置的TCAM ACL资源分组选组成功，不再下发到系统预置分组。



最终，通过配置TCAM ACL自定义模板，用户应用了2个traffic policy，包含不同的动作，仅占用了1个芯片group资源。

3.1.2.3 3：应用 traffic policy 匹配较少字段下发到 320bit 分组

用户下发traffic policy，仅包含少量的匹配字段，但是使用系统预置分组时会下发到320bit分组。可以通过配置TCAM ACL资源自定义分组，分组中包含多个traffic policy中所有的匹配字段和应用动作，删除预置分组的不必要字段，最终将分组宽度缩小到160bit，减少芯片资源的占用。

例如系统包含如下预置分组：

分组ID	分组模式	字段集合	动作集合
233	320bit	Source IP Destination IP L4 Source Port L4 Destination Port IP Protocol TCP Flag IP Fragment Type IP TOS IP TTL ICMP Type Source Interface VSI	Redirect Interface Deny Statistics Remark 8021p Remark VLAN Remark DSCP Mac learning disable

用户创建traffic policy匹配IP dscp字段，执行动作remark dscp，在所有系统预置模板中，仅Group 233可以满足，而Group 233为320bit的分组包含较多匹配字段和动作，所以占用了较多芯片资源。

可以配置如下TCAM ACL资源自定义分组：

分组ID	分组模式	字段集合	动作集合
User Define Group	160bit	Source IP Destination IP IP ToS VSI	remark dscp

创建的TCAM ACL资源自定义分组，位宽为160bit，仅包含用户需要的匹配的字段和动作，占用少量芯片Group资源。

当traffic policy进行选组时会优先判断用户配置的TCAM ACL资源分组是否能满足需求，用户配置的TCAM ACL资源自定义分组包含IP ToS和remark dscp动作，所以traffic policy对用户配置的TCAM ACL资源分组选组成功，不再下发到系统预置分组。

说明

其中TCAM ACL资源自定义分组中的IP ToS对应traffic policy中匹配的IP dscp字段。具体请参见 **3.1.6.1 匹配字段与自定义分组字段对照表**。

最终，通过配置TCAM ACL自定义模板，用户下发的policy占用较少的芯片资源，并且实现了用户的功能。

3.1.2.4 4：没有包含匹配字段和动作组合的系统预置模板，policy 下发失败

用户下发traffic policy，包含的匹配字段和动作的组合，所有系统预置模板均无法满足，导致traffic policy下发失败。

例如创建traffic policy匹配IP dscp，执行动作remak local-precedence和remark dscp。

```
#
traffic classifier dscp
 if-match dscp 15
traffic behavior dscp
 remark dscp af22
 remark local-precedence ef
traffic policy dscp
 classifier dscp behavior dscp
#
```

如下所示，所有系统预置模板均无法满足，在全局应用policy下发失败：

```
[~HUAWEI] display  traffic-policy applied-record
Total records : 1
-------------------------------------------------------------------------------
Policy Type/Name                Apply Parameter             Slot   State
-------------------------------------------------------------------------------
dscp                            Global inbound                 1   fail(3)
                                                               2   fail(3)
                                                               4   fail(3)
-------------------------------------------------------------------------------
Fail reason:
   3 — The numbers of matched conditions and actions in the traffic policy exceed the limit.
```

可以配置如下TCAM ACL资源自定义分组，将需要匹配的字段和执行的动作放到自定义分组中，使设备预置模板不支持的配置组合下发成功：

分组ID	分组模式	字段集合	动作
User Define Group	160bit	Source IP Destination IP IP ToS VSI	remark dscp remark local-predence

3.1.3 配置思路

1. 根据业务需求，规划traffic policy匹配字段、应用视图，以及执行动作；
2. 使能TCAM ACL自定义功能；
3. 创建TCAM ACL自定义资源模板，包含所有的traffic policy需要匹配的字段，应用的视图及执行的动作。

   说明

   用户匹配的字段、执行的动作、应用的视图和自定义分组中配置的字段、动作、视图不完全一样，其中的对应关系可以参见3.1.6 附录。
4. 应用TCAM ACL自定义资源模板；
5. 应用traffic policy。

3.1.4 配置举例

配置需求：配置三个policy，分别匹配IP, IP+TCP端口号，IP+TCP端口号+TCP flag，执行动作均为deny，并应用在不同的VALN上。

需要下发的policy配置如下：


```
#
acl 3001
 rule 5 permit ip source 1.1.1.1 0
 rule 10 deny ip
#
traffic classifier tc1
 if-match acl 3001
#
traffic behavior tb1
#
traffic policy p1
 classifier tc1 behavior tb1
#
vlan 100
 traffic-policy  p1 inbound
#
```

```
#
acl 3002
 rule 5 permit tcp destination 2.2.2.2 0 source-port eq 10000
 rule 10 deny ip
#
traffic classifier tc2
 if-match acl 3002
#
traffic behavior tb2
#
traffic policy p2
 classifier tc2 behavior tb2
#
vlan 200
 traffic-policy p2 inbound
#
```

```
#
acl 3003
 rule 5 permit tcp destination 3.3.3.3 0 destination-port eq 10001 tcp-flag established
 rule 10 deny ip
#
traffic classifier tc3
 if-match acl 3003
#
traffic behavior tb3
#
traffic policy p3
 classifier tc3 behavior tb3
#
vlan 300
 traffic-policy p3 inbound
#
```

1. 未使用TCAM ACL自定义分组的情况下，在三个vlan下分别应用三个traffic policy，占用三个分组资源。

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
-------------------------------------------------------------------------------
Chip  GroupID    Width      Stage          ServiceName                  Count
      (FEI/FE)
-------------------------------------------------------------------------------
   1     2/2     Quadruple  Ingress        BPDU Deny                       21
         2/2     Quadruple  Ingress        CPCAR                            6
         2/2     Quadruple  Ingress        L2 Protocol Tunnel               1
         3/3     Quadruple  Ingress        App-Session                      3
         3/3     Quadruple  Ingress        CPCAR                           26
       213/1     Double     Ingress        Traffic Policy VLAN              2
       216/4     Double     Ingress        Traffic Policy VLAN              3
       294/5     Double     Ingress        Traffic Policy VLAN              2
-------------------------------------------------------------------------------
```


2. 根据业务需求，规划traffic policy匹配的字段、应用的视图、执行动作。

   所有traffic policy所匹配字段合集：

   source IP address、destination IP address、IP protocol、TCP source port、TCP destination port、TCP flag。

   所有应用的视图合集：VLAN。

   所有的动作合集：deny。

3. 根据附录查表创建TCAM ACL自定义资源模板。

   a.使能TCAM ACL功能：

   ```
   #
   system tcam acl
   #
   ```

   b.创建名称为example的TCAM ACL模板：

   ```
   #
   system tcam acl template example
   #
   ```

   c.创建名为example的分组：

   ```
   #
   group example precedence 0
    match ip source-ip destination-ip protocol fragment
    match tcp destination-port source-port tcp-flag
    match forwarding vsi
    action deny
   #
   ```

   d.将example分组绑定policy l3业务：

   ```
   #
   service trafficpolicy-l3 group example
   #
   ```

   e.应用TCAM ACL模板：

   ```
   #
   system tcam acl template example all
   #
   ```

4. 应用流策略。

```
#
vlan 100
 traffic-policy  p1 inbound
#
vlan 200
 traffic-policy  p2 inbound
#
vlan 300
 traffic-policy  p3 inbound
#
```

5、策略应用后，使用命令查看，设备只为policy创建了一个分组。

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
------------------------------------------------------------------------------
 Chip  ServiceName               GroupName                        GroupID
                                                                 (FEI/FE)
------------------------------------------------------------------------------
    1  trafficpolicy-l3          example                            213/1
------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                Count
       (FEI/FE)
------------------------------------------------------------------------------
    1     2/2     Quadruple  Ingress        BPDU Deny                     21
          2/2     Quadruple  Ingress        CPCAR                          6
          2/2     Quadruple  Ingress        L2 Protocol Tunnel             1
```



```
        3/3     Quadruple  Ingress        App-Session                  3
        3/3     Quadruple  Ingress        CPCAR                       26
      213/1     Double     Ingress        Traffic Policy VLAN          5
------------------------------------------------------------------------------
```

3.1.5 注意事项

1. 在Group模式VS中，所有VS都支持配置TCAM ACL资源自定义功能。
2. V100R006C00之前的版本，在Port模式VS中，仅Admin-VS支持配置TCAM ACL资源自定义功能；V100R006C00及之后的版本，Port模式VS和TCAM ACL资源自定义功能，不支持同时配置。
3. 如果需要修改TCAM ACL资源的缺省分配，建议在设备空配置时进行修改，否则配置的TCAM ACL资源自定义模板无法直接生效，需要先删除对应的业务，或者复位单板。
4. TCAM ACL资源自定义模板应用后不能直接更改，需要先取消业务与模板的绑定，再对模板进行更改。
5. 不建议TCAM ACL模板创建的group绑定非MQC的业务，如果要绑定非MQC的业务，请联系技术支持人员。
6. 自定义分组添加的字段和动作长度的总和不能超过320bit，否则分组会创建失败。

3.1.6 附录

用户匹配的字段、执行的动作、应用的视图和自定义分组中配置的字段、动作、视图不完全一样，其中的对应关系可以通过本章节查看。

3.1.6.1 匹配字段与自定义分组字段对照表

类型	字段	配置举例	自定分组配置
L3	source IP address	rule permit ip source 10.0.0.0 0.255.255.255	match ip source-ip
	destination IP address	rule permit ip destination 10.0.0.0 0.255.255.255	match ip destination-ip
	IP protocol	rule permit icmp	match ip protocol
	IP DSCP	rule permit ip dscp af11	match ip tos
	IP TOS	rule permit ip tos max-reliability	match ip tos
	IP TTL	rule permit ip ttl-expired	match ip ttl
	IP fragment type	rule permit tcp fragment-type fragment	match ip fragment
	ICMP type and code	rule permit icmp icmp-type echo	match icmp icmp-type

类型	字段	配置举例	自定分组配置
	IGMP type	rule permit igmp igmp-type host-query	match igmp igmp-type
	TCP source port	rule permit tcp source-port eq ftp	match ip protocol match tcp source-port match ip fragment
	TCP destination port	rule permit tcp destination-port eq ftp	match ip protocol match tcp destination-port match ip fragment
	TCP flag	rule permit tcp tcp-flag established	match ip fragment match tcp tcp-flag
	UDP source port	rule permit udp source-port eq 1033	match udp source-port
	UDP destination port	rule permit udp destination-port eq 1033	match udp destination-port
L2	destination MAC address	rule permit destination-mac 1-1-1 ffff-ffff-ffff	match ethernet destination-mac
	source MAC address	rule permit source-mac 1-1-1 ffff-ffff-ffff	match ethernet source-mac
	Ethertype	rule permit type arp	match ethernet ethertype
	outer VLAN ID	rule permit vlan 10	match ethernet vlan
	outer 802.1p priority	rule permit 8021p 5	match ethernet 8021p
	inner VLAN ID	rule permit inner-vlan 10	match ethernet inner-vlan
	inner 802.1p priority	rule permit inner-8021p 3	match ethernet inner-8021p

特别注意：如上表，匹配TCP端口号的规则必须添加匹配IP fragment。

3.1.6.2 执行动作与自定义分组动作对照表

动作	配置举例	自定分组配置
deny	rule deny ip 1.1.1.1 0	action deny
car	[system-behavior-example] car cir 100 mbps	action car
mirror	[system-behavior-example] mirroring observe-port 1	action mirror
MAC learning disable	[system-behavior-example] mac-address learning disable	action mac-address-learning-disable
statistics	[system-behavior-example] statistics enable	action statistics
redirect interface	[system-behavior-example] redirect interface 10GE 1/0/1	action redirect interface
redirect nexthop	[system-behavior-example] redirect nexthop 1.1.1.1	action redirect nexthop
redirect remote	[system-behavior-example] redirect remote 1.1.1.1	action redirect nexthop
modify 8021p	[system-behavior-example] remark 8021p 1	action remark 8021p
modify DSCP	[system-behavior-example] remark dscp 8	action remark dscp
modify schedule priority	[system-behavior-example] remark local-precedence ef	action local-precedence

3.1.6.3 应用视图与自定义分组字段对照表

当自定义分组应用到某些视图时，需要在自定义分组中添加额外的匹配的字段，具体如下表所示。

应用视图	配置举例	自定分组配置
Global	[system] traffic-policy example global inbound	NA
VLAN	[system-vlan10] traffic-policy example inbound	match forwarding vsi
VLANIF	[system-Vlanif10] traffic-policy example inbound	match forwarding vsi

应用视图	配置举例	自定分组配置
物理接口或Eth-trunk接口	[system-10GE1/0/1] traffic-policy example inbound	match forwarding source-interface

说明

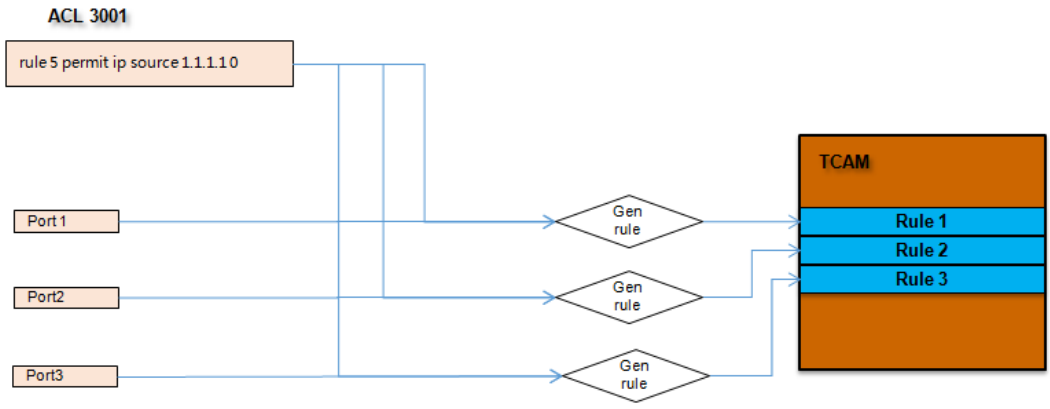
NA表示自定义分组中不需要增加特定的字段。

3.2 减少下发到芯片中的 ACL 规则数（将不同的 VLAN 或接口加入 QoS 组后应用相同流策略）

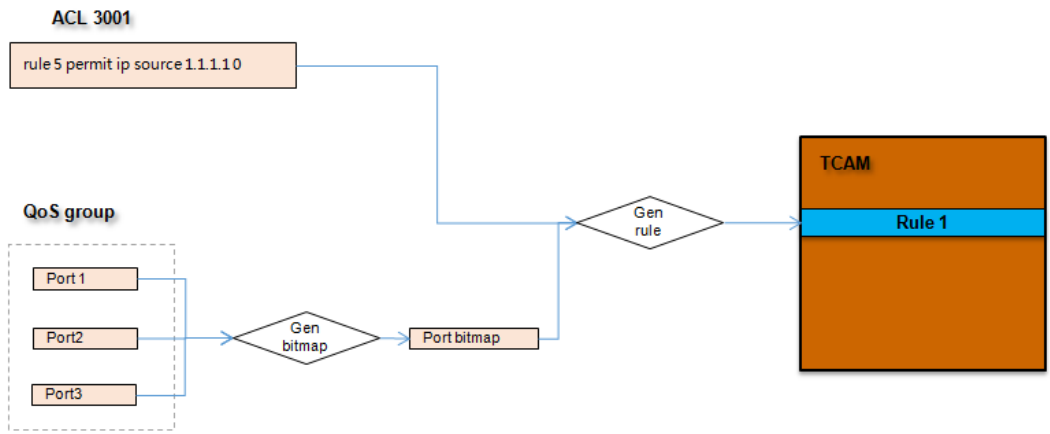
3.2.1 原理介绍

不同的接口在加入同一个QoS组时，系统会创建一个port bitmap，包含加入QoS组的所有端口；当traffic policy在QoS组视图下应用时，会直接匹配创建的port bitmap，从而实现一条rule对所有加入QoS组的端口生效，达到节省ACL资源的目的。

如果不使用QoS组，同一条rule匹配多个端口，占用多个ACL资源。

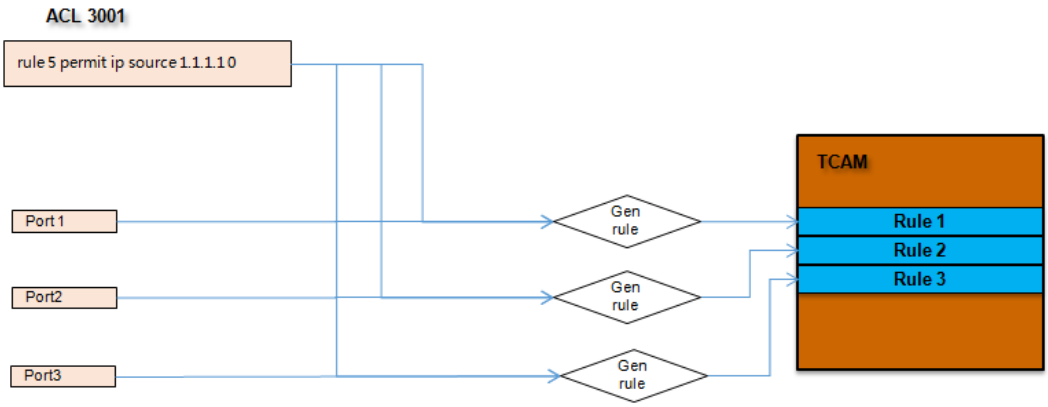


如果使用QoS组，同一条rule匹配多个端口，仅占用一份ACL资源。

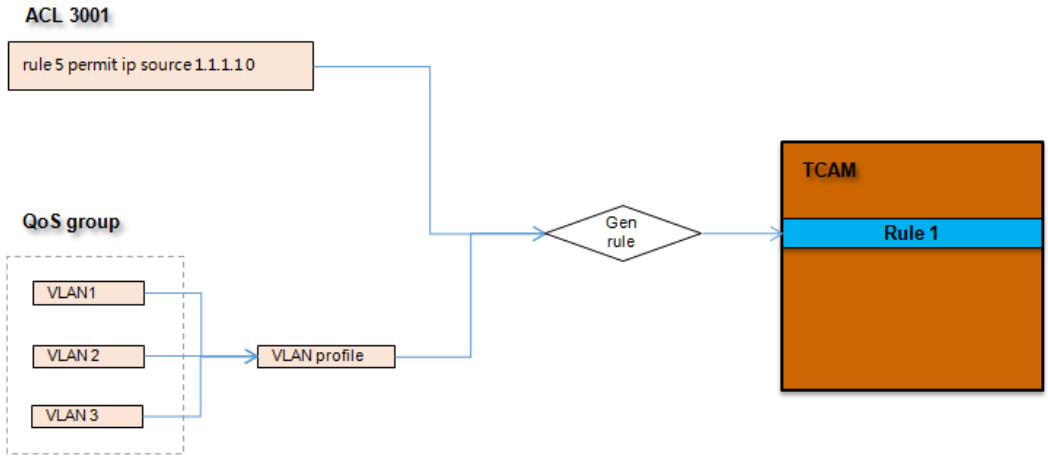


不同的VLAN在加入同一QoS组时，系统为加入QoS组的VLAN分配相同的VLAN pofile；traffic policy在QoS组视图下应用时，会直接匹配系统分配的VLAN profile，从而实现一条rule对所有加入QoS组的VLAN都生效，达到节省ACL资源的目的。

如果不使用QoS组，同一条rule匹配多个VLAN，占用多个ACL资源。



如果使用QoS组，同一条rule匹配多个VLAN，仅占用一份ACL资源。



3.2.2 应用场景：在多个物理接口、VLAN 或者 VLANIF 下应用相同的 traffic policy

当多个VLAN、VLANIF接口、物理接口要应用相同的流策略时，会消耗较多的ACL资源。将这些VLAN、VLANIF接口、物理接口加入同一个QoS组后，在QoS组下应用流策略，只需消耗一份ACL资源，从而可以节省设备的ACL资源占用。

3.2.3 配置思路

1. 将引用相同traffic policy的VLAN、VLANIF或者物理口加入同一个QoS组;
2. 在QoS组视图下应用traffic policy。

3.2.4 配置举例

配置需求：配置一个包含较多的ACL规则的traffic policy，同时应用在VLAN100、VLAN200、VLAN300、VLAN400、VLAN500下。

需要下发的traffic policy配置：


```
#
acl name example advance
 rule 5 permit ip destination 10.2.79.36 0
 rule 10 permit ip destination 10.19.240.8 0
 rule 15 permit ip destination 10.2.253.100 0
 rule 20 permit ip destination 10.2.145.34 0
 rule 25 permit ip destination 10.2.145.178 0
 rule 30 permit ip destination 10.2.145.181 0
 rule 35 permit ip destination 10.2.145.22 0
 rule 40 permit ip destination 10.2.253.210 0
 rule 45 permit ip destination 10.2.253.102 0
 rule 50 permit ip destination 10.19.240.4 0
#
traffic classifier tc1
 if-match acl example
#
traffic behavior tb1
#
traffic policy p1
 classifier tc1 behavior tb1
#
```

1. 直接在VLAN100、VLAN200、VLAN300、VALN400、VLAN500应用traffic-policy下发较多的ACL。

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                  Count
------------------------------------------------------------------------------
    1     2/2     Quadruple  Ingress        BPDU Deny                       21
          2/2     Quadruple  Ingress        CPCAR                            6
          2/2     Quadruple  Ingress        L2 Protocol Tunnel               1
          3/3     Quadruple  Ingress        App-Session                      6
          3/3     Quadruple  Ingress        CPCAR                           26
        213/1     Double     Ingress        Traffic Policy VLAN             50
------------------------------------------------------------------------------
```

2. 创建名为example的QoS组，将VLAN100、VLAN200、VLAN300、VLAN400、VLAN500加入QoS组。

```
#
qos group example
 group-member vlan 100 200 300 400 500
#
```

3. 在QoS组下应用traffic policy。

```
#
qos group example
 group-member vlan 100 200 300 400 500
 traffic-policy p1 inbound
#
```

4. 查看设备下发的ACl规则条数。

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                  Count
------------------------------------------------------------------------------
    1     2/2     Quadruple  Ingress        BPDU Deny                       21
          2/2     Quadruple  Ingress        CPCAR                            6
          2/2     Quadruple  Ingress        L2 Protocol Tunnel               1
          3/3     Quadruple  Ingress        App-Session                      6
          3/3     Quadruple  Ingress        CPCAR                           26
        296/6     Double     Ingress        Traffic Policy VLAN              5
------------------------------------------------------------------------------
```

3.2.5 注意事项

1. 同一个QoS组中只能包含相同类型的成员。

2. 成员为源IP的QoS组个数上限为63。
3. 对于CE12800和CE6870，成员为物理接口和Eth-Trunk接口的QoS组个数上限为15。
4. 对于CE12800和CE6870，成员为VLAN、VLANIF接口、二层子接口、三层子接口的QoS组个数总和上限为15。
5. 对于CE12800，当设备的互通模式为非增强模式时，配置成员为VLAN或VLANIF接口的QoS组后，不能配置EVN、VXLAN的ARP广播报文抑制、VLAN出方向PHB与DSCP值的映射功能。反之亦然。
6. 对于除CE12800和CE6870外的交换机，在QoS组上应用流策略时，只能应用在入方向。流分类规则只能匹配源IPv4地址、目的IPv4地址、协议类型、源端口号、目的端口号。
7. 对于CE12800和CE6870，在QoS组上应用流策略时，只能应用在入方向。流分类规则只能匹配源IPv4地址、目的IPv4地址、协议类型、源端口号、目的端口号。流行为只支持报文过滤、流量统计、重定向、策略路由。可以通过配置TCAM ACL资源自定义模板的方式修改QoS组支持的匹配字段和执行动作，示例如下：

```
#
system tcam acl
#
system tcam acl template example
 group l3 precedence 5
  match ip source-ip destination-ip protocol tos fragment
  match tcp destination-port source-port tcp-flag
  match udp destination-port source-port
  match icmp icmp-type
  match forwarding source-interface vsi
  action deny redirect nexthop
 service trafficpolicy-qosgroup group l3
#
system tcam acl template example all
#
```

3.3 减少系统组资源的占用（在内置 TCAM 中下发组播业务）

3.3.1 原理介绍

在ED、EF、EG系列单板中上，为了增大组播表项的规格，组播表项默认下发到外扩TCAM中。由于外扩TCAM中没有组播表项命中标记，所以在组播表项下发外扩TCAM时，系统需要借助ACL的统计功能来获取组播表项是否命中，此时需要占用内置TCAM中的2个分组资源，如下所示：

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
--------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                  Count
--------------------------------------------------------------------------------
    1     2/2     Quadruple  Ingress        BPDU Deny                       21
          2/2     Quadruple  Ingress        CPCAR                            6
          2/2     Quadruple  Ingress        L2 Protocol Tunnel               1
          3/3     Quadruple  Ingress        App-Session                      6
          3/3     Quadruple  Ingress        CPCAR                           26
         67/4     Single     Ingress        MC Mapping Statistics            1
         68/5     Single     Ingress        Multicast Statistics             7
--------------------------------------------------------------------------------
```

可以通过配置外扩TCAM资源模板，取消为组播分配的TCAM资源，这样组播表项会下发到内置TCAM中，因此可以直接读取内置TCAM的HIT标记来检测表项是否命中，不需要借助ACL实现，进而节省了ACL资源。

说明

从V200R001C00版本开始，组播表项不再默认下发到外扩TCAM中。

外扩TCAM分配的资源信息可以通过执行命令**display system tcam resource** [**slot***slot-id*] 查看。

```
[~HUAWEI] display system tcam resource
Resource Detail Information:
-------------------------------------------------------------------------------
Slot  Chip  TCAM      Service           Banks        Total         Used         Free
-------------------------------------------------------------------------------
1     0     internal  All                  12        24576          336        24240
1     0     internal  |- ACL               --           --          336           --
1     0     internal  |- UCv6Route         --           --            0           --
1     0     internal  |- MCv4Route         --           --            0           --
1     0     internal  |- MCv6Route         --           --            0           --
1     0     external  ACL                   0            0            0            0
1     0     external  MCv4Route            16        65536            0        65536
1     0     external  MCv6Route            16        65536            0        65536
1     0     external  UCv4Route           128       524288           12       524276
1     0     external  UCv6Route            96       393216            0       393216
-------------------------------------------------------------------------------
Resource Template Information:
------------------------------------------------------------------------
Slot       Type                RunningTemplate      NextTemplate
------------------------------------------------------------------------
1          CE-L48XS-EF         EF-extend            example
------------------------------------------------------------------------
```

说明

回显中UCv6Route表项数目和MCv6Route表项数目均为实际表项数目的两倍。

外扩TCAM为各个资源分配的规格和外扩TCAM资源的配置建议可以在产品文档中查看命令**external tcam**的描述。

3.3.2 应用场景：在支持外扩 TCAM 的单板上应用组播业务

在组播表项规格不大的情况下，配置TCAM资源模板，将组播表项下发到内置TCAM中，可以节省2个ACL分组资源。

3.3.3 配置思路

1. 配置TCAM资源模板，将外扩TCAM为组播分配的资源修改为0；
2. 应用TCAM资源模板；
3. 复位单板。

3.3.4 配置举例

1. 创建名为example的TCAM资源模板，将外扩TCAM为组播分配的资源修改为0。

```
#
system tcam example
 external tcam u4router 589824
 external tcam u6router 229376
#
```

说明

将外扩TCAM为组播分配的资源修改为0，需要把外扩TCAM为组播分配的资源全部分配给单播或者ACL，此举例中采用分配给单播的方法。

以上述命令**display system tcam resource**回显所示，可以采取以下方式分配：

UCv4Route表项数目=UCv4Route表项数目+MCv4Route表项数目=524288+65536=589824;

UCv6Route表项数目=UCv6Route表项数目/2+MCv6Route表项数目/2=393216/2+65536/2=229376。

2. 在slot 1应用TCAM资源模板。

```
#
system tcam example slot 1
#
```

3. 复位单板。

```
#
reset slot 1
#
```

4. 查看ACL资源，不再下发组播相关分组。

```
[~HUAWEI-diagnose] display system tcam service brief
Slot: 1
------------------------------------------------------------------------------
 Chip  GroupID    Width      Stage          ServiceName                 Count
------------------------------------------------------------------------------
    1     2/2     Quadruple  Ingress        BPDU Deny                      21
          2/2     Quadruple  Ingress        CPCAR                           6
          2/2     Quadruple  Ingress        L2 Protocol Tunnel              1
          3/3     Quadruple  Ingress        App-Session                     6
          3/3     Quadruple  Ingress        CPCAR                          26
------------------------------------------------------------------------------
```

3.3.5 注意事项

应用了TCAM模板后，需要设备重启后生效。

4 ACL 维护

4.1 查看资源使用情况

通过执行**display system tcam bank resource** [**slot** *slot-id* [**chip** *chip-id*]] 命令查看已下发的业务占用的ACL资源以及剩余的ACL资源。

说明

仅V200R002C50及之后版本支持此命令。

```
<HUAWEI> display system tcam bank resource slot 1 chip
0
Slot: 1    Chip:
0

-------------------------------------------------------------Bank
Usage-------------------------------------------------------------
BankId                  Entry     Entry     Entry     Stage     GroupId    KBType     KBId
ServiceName
                        Size      Free      Used                (FEI/
FE)
-------------------------------------------------------------------------------------------------
-------------------------
0,1                     320Bit    961       21        Ingress     2/2      L2           2,3   BPDU
Deny
                                            6                     2/2      L2           2,3   CPCAR
L2
                                            1                     2/2      L2           2,3   M-LAG
Protocol
                                            3                     3/3      IPv4         2,3   App-
Session
                                            25                    3/3      IPv4         2,3   CPCAR
L3
                                            1                     3/3      IPv4         2,3   DFS
Dual-active
                                            2                     3/3      IPv4         2,3   VXLAN
DFS
                                            1                     4/1      IPv6         2,3   CPCAR
Ipv6
2                       160Bit    1020      1         Egress    146/4                       M-LAG
IPv4 UC
                                            1                   146/4                       M-LAG
```

```
IPv6 UC
                                        1                   146/4                    M-LAG
Isolate
3                                                                   -           -
--
4                                                                   -           -
--
5                                                                   -           -
--
6                                                                   -           -
--
7                                                                   -           -
--
8                                                                   -           -
--
9                                                                   -           -
--
10                                                                  -           -
--
11                                                                  -           -
--
12                                                                  -           -
--
13                                                                  -           -
--
------------------------------------------------------------------------------------------------------------
-------------------------
-------------------------------------------------------KB
Usage-------------------------------------------------------
KBType    Total     Used
Free
------------------------------------------------------------------------------------------------------------
-------------------------
L2        8         2(2,3)
6(0,1,4,5,6,7)
IPv6      8         2(2,3)
6(0,1,4,5,6,7)
IPv4      8         2(2,3)
6(0,1,4,5,6,7)
------------------------------------------------------------------------------------------------------------
-------------------------
```

回显信息如下表所示：

项目	描述
Slot	显示单板槽位号。
Chip	显示芯片号。
Bank Usage	显示Bank资源使用情况。
Stage	显示报文在转发过程中的不同阶段： ● Ingress：入方向。 ● Egress：出方向。
BankId	Bank资源的ID号，不同设备的Bank资源不同，具体以设备显示为准。
Entry Size	显示Bank中表项的宽度。

项目	描述
Entry Free	显示Bank中剩余表项的个数。
Entry Used	显示Bank中已经使用的表项。
GroupId (FEI/FE)	显示组的ID。
KBType	显示KB资源的类型。
KBId	KB资源的ID号。
ServiceName	显示下发的具体业务名称。如果某Bank中没有业务下发，则显示为--。
KB Usage	显示KB资源使用情况。
Total	显示KB资源的总数。
Used	显示已经使用的KB资源。
Free	显示剩余的KB资源。

4.2 预判业务是否可以下发成功

通过执行**display system tcam acl resource** { **service** { *service-name* | **brief** } | **group** *group-id* } [**slot** *slot-id* [**chip***chip-id*]]命令可以预判业务是否可以下发成功。

```
<HUAWEI> display system tcam acl resource service
brief
KB : Key
Buffer

--------------------------------------------------------------------------------

Slot: 1    Chip:
0

--------------------------------------------------------------------------------

Direction  ServiceName                Group  KBType     NeedKBNumber   Configured   Pre-
State
--------------------------------------------------------------------------------

Ingress    BC Port Suppress             14  ALL                 1            N
OK
Ingress    DHCP Snooping Car            32  IPv4                1            N
OK
Ingress    Blacklist                    19  ALL                 1            N
OK
Ingress    Blacklist                    31  ALL                 1            N
OK
Ingress    Blacklist IPv6               26  IPv6                2            N
OK
Ingress    Blacklist                    33  IPv4                1            N
OK
Ingress    Blacklist                    34  ALL                 1            N
```



```
OK
Ingress    QoS CAR                  14  ALL          1          N
OK
Ingress    Auto-Defend              19  ALL          1          N
OK
Ingress    Auto-Defend              31  ALL          1          N
OK
Ingress    Auto-Defend IPv6         26  IPv6         2          N
OK
Ingress    Auto-Defend              33  IPv4         1          N
OK
Ingress    Auto-Defend              34  ALL          1          N
OK
Ingress    Stack Filter             33  IPv4         1          N
OK
Ingress    Stack Filter             34  ALL          1          N
OK
Ingress    Stack Filter             19  ALL          1          N
OK
Ingress    Stack Filter             31  ALL          1          N
OK
Ingress    App-Session IPv6          4  IPv6         2          Y
OK
Ingress    DiffServ IP              16  IPv4,IPv4    1          N
OK
Ingress    DiffServ IP              16  IPv4,IPv4    1          N
OK
Ingress    DiffServ IPv6            17  IPv6,IPv6    1          N
OK
Ingress    DiffServ IPv6            17  IPv6,IPv6    1          N
OK
Ingress    DiffServ MPLS             8  MPLS         1          Y
OK
Ingress    ECN IP                   16  IPv4,IPv4    1          N
OK
Ingress    ECN IP                   16  IPv4,IPv4    1          N
OK
Ingress    ECN IPv6                 17  IPv6,IPv6    1          N
OK
Ingress    ECN IPv6                 17  IPv6,IPv6    1          N
OK
Ingress    MPLS PHP                  8  MPLS         1          Y
OK
Ingress    Netstream                15  ALL          1          N
OK
Egress     Netstream                81  --           1          N
OK
Ingress    QoS Trust                24  IPv4         1          N
OK
Ingress    QoS Trust IPv6           25  IPv6         1          N
OK
Ingress    FSB VLAN Deny            13  ALL          1          N
OK
Ingress    FCoE FSB                 13  ALL          1          N
OK
Ingress    FCoE Session             13  ALL          1          N
OK
Ingress    BD Statistics            11  ALL          1          N
OK
Ingress    MC Mapping Statistics    67  IPv4,IPv6    1          N
OK
Ingress    Multicast Statistics     68  IPv4,IPv6    1          N
OK
Ingress    DCI                       6  L2,IPv4      2          N
OK
Ingress    DCI                      27  L2,IPv4      1          N
OK
Ingress    IP Force Forward         72  IPv4         1          N
OK
```


Ingress	EVN Packet	6	L2,IPv4	2	N
OK					
Ingress	Ping Packet Pass	6	L2,IPv4	2	N
OK					
Ingress	Ping Packet Pass	99	L2,IPv4	1	N
OK					
Ingress	EVN MAC Drif	71	ALL	1	N
OK					
Egress	M-LAG Isolate	122	--	1	N
OK					
Egress	M-LAG Isolate	146	--	1	N
OK					
Ingress	VLAN Mirror	15	ALL	1	N
OK					
Egress	VLAN Mirror	81	--	1	N
OK					
Ingress	ECMP Hash	105	IPv4	1	N
OK					
Ingress	LAG Hash	119	IPv4	1	N
OK					
Ingress	FCoE Fip	13	ALL	1	N
OK					
Ingress	FCoE VLAN Deny	13	ALL	1	N
OK					
Ingress	FCoE VLAN	13	ALL	1	N
OK					
Ingress	VLANIF Statistics	108	ALL	1	Y
OK					
Ingress	MAINIF Statistics	108	ALL	1	Y
OK					
Ingress	SUBIF Statistics	108	ALL	1	Y
OK					
Ingress	VLANIF Statistics RCY	109	ALLRCY	1	N
OK					
Ingress	MAINIF Statistics RCY	109	ALLRCY	1	N
OK					
Ingress	SUBIF Statistics RCY	109	ALLRCY	1	N
OK					
Egress	Out Vp L3 Statistic	150	--	1	Y
OK					
Ingress	Filter	19	ALL	1	N
OK					
Ingress	Filter	31	ALL	1	N
OK					
Ingress	Filter IPv6	26	IPv6	2	N
OK					
Ingress	Filter	33	IPv4	1	N
OK					
Ingress	Filter	34	ALL	1	N
OK					
Ingress	FCoE Port Statistics	93	ALL	1	N
OK					
Ingress	VLAN Mac-address Limit	128	ALL	1	N
OK					
Ingress	Storm Ctrl BC Query	14	ALL	1	N
OK					
Ingress	Storm Ctrl MC Query	14	ALL	1	N
OK					
Ingress	BD MAC Not Learn	128	ALL	1	N
OK					
Ingress	In VP Statistics	160	IPv4,IPv4	1	N
OK					
Ingress	Out VP Statistics	160	IPv4,IPv4	1	N
OK					
Ingress	In VP Statistics	161	IPv4,IPv4	1	N
OK					
Ingress	PNI MLD Deny	4	IPv6	2	Y
OK					
Ingress	PNI PIMv6 MC Deny	4	IPv6	2	Y


```
OK
Ingress    PNI IPSECv6 MC Deny            4  IPv6                2          Y
OK
Ingress    EVN Packet                   141  IPv4                1          N
NO
Ingress    VNI MC Suppress               14  ALL                 1          N
OK
Ingress    EVN Packet V6                607  IPv6                2          N
OK
Ingress    BFD MPLS                     612  MPLS                1          Y
OK
Ingress    MPLS RSVP                    612  MPLS                1          Y
OK
Ingress    VXLAN V6 Path Detect         607  IPv6                1          N
OK
Ingress    Cpcar VXLAN Ipv6             178  IPv4                1          N
OK
Ingress    VXLAN Path Detect            601  IPv4                1          N
OK
Ingress    Path Detect                  600  IPv4,IPv4           1          N
OK
Ingress    VXLAN DHCP                   600  IPv4,IPv4           1          N
OK
------------------------------------------------------------------------------
```

回显信息如下表所示：

项目	描述
KB : Key Buffer	KB资源。
Slot	显示单板槽位号。
Chip	芯片号。
Direction	报文在转发过程中的不同阶段。
ServiceName	业务名称。
Group	业务下发的分组。
KBType	分组所占用的KB资源类型。
NeedKBNumber	分组所需要的KB资源的个数。
Configured	业务是否已经配置： ● Y：业务已配置。 ● N：业务未配置。
Pre-State	当前状态下，业务是否可以下发成功： ● OK：当前状态下，业务可以下发成功。 ● NO：当前状态下，业务不可以下发成功。

4.3 常见问题诊断及解决方案

文档中命令的回显如果没有特别说明都以V200R002C50版本为例。

4.3.1 Traffic policy 应用失败

4.3.1.1 问题现象

下发traffic policy时，提示如下traffic policy下发失败的信息：

```
Error: Failed to apply the traffic policy p1 on slot 1. To check the cause, run the display
traffic-policy applied-record command.
```

4.3.1.2 查看下发失败原因

可以通过两种方式查看traffic policy下发失败的原因。

1、执行**display traffic-policy applied-record**命令行查看下发失败原因。

```
[~HUAWEI] display traffic-policy applied-record
Total records : 1
-------------------------------------------------------------------------------
Policy Type/Name                Apply Parameter             Slot   State
-------------------------------------------------------------------------------
P1                              Global inbound                 1   fail(3)
-------------------------------------------------------------------------------
Fail reason:
   3 -- The numbers of matched conditions and actions in the traffic policy exceed the limit.
```

其中fail(3)表示traffic policy下发失败，编号3代表下发失败的具体原因。常见原因见下表：

编号	设备显示的失败原因	原因描述
3	The numbers of matched conditions and actions in the traffic policy exceed the limit.	系统预置模板中没有动作和匹配字段的组合
4	Insufficient ACL resources.	KB、CE或者Bank资源不足

2、在诊断视图下执行**display system tcam fail-record**查看失败的原因。

```
[~HUAWEI-diagnose] display system tcam fail-record
-------------------------------------------------------------------------------
Slot  Chip Time                Service                 ErrInfo
-------------------------------------------------------------------------------
1     1    2017-03-28 10:31:38 Traffic Policy Global   Select group
Total: 1
```

其中ErrInfo表示traffic policy下发失败的原因，常见原因见下表：

设备显示的失败原因	原因描述
Select group.	系统预置模板没有动作和匹配字段的组合
Group resource full	KB或CE资源不足
Entry resource full	Bank资源不足

4.3.1.3 解决方案

本章节根据下面三种原因，分别给出解决traffic policy下发失败的解决方案。

4.3.1.3.1 KB 资源不足

如果traffic policy下发失败是因为KB或CE资源不足，可以在系统视图下执行**display system tcam acl group resource** [**slot** *slot-id* [**chip** *chip-id*]]命令行查看设备KB或CE资源使用情况：

```
[~HUAWEI] display system tcam acl group resource slot 1
STG : Stage                   KCP  : Key Construction Program
ING : Ingress                 EGR  : Egress
CYC : Cycle                   PTYPE: PortType
FRT : Front Ports             RCY  : Recycle Ports
16-L: 16bit-LSB Copy Engine   16-M : 16bit-MSB Copy Engine
32-L: 32bit-LSB Copy Engine   32-M : 32bit-MSB Copy Engine
F   : Free                    T    : Total
------------------------------------------------------------------------------
Slot: 1    Chip : 0   UseRate:Normal
------------------------------------------------------------------------------
STG KCP PacketType       PTYPE       CYC Group   UsedKey 16-L  32-L  16-M  32-M
                                                          F|T   F|T   F|T   F|T
------------------------------------------------------------------------------
ING   1 L2               FRT           0 2       2,3      2|8   5|8   7|8   6|8
ING   2 IPV4             FRT           0 3       2,3      0|8   4|8   4|8   6|8
ING   3 TRILL            FRT           0 1       2,3      6|8   5|8   7|8   6|8
ING   4 IPV6             FRT           0 4       2,3      2|8   5|8   1|8   6|8
------------------------------------------------------------------------------
```

其中，STG：代表占用的是入方向还是出方向的ACL资源，ING代表入方向，EGR代表出方向；

CYC：代表ACL的资源池编号，以E系列单板为例，资源池0包含3个KB资源，资源池1号包含4个KB资源；

Group：代表业务下发的group ID，与在诊断视图下执行**display system tcam service brief**中显示的的FE GroupID相对应；

UsedKey：代表当前已使用的KB资源编号；

16-L、32-L、16-M、32-M：代表CE资源的使用情况，T表示所有的CE资源、F表示剩余的CE资源。

其他具体信息请参照产品文档中**display system tcam acl group resource**命令的描述。

当相同KCP下，7个KB资源被全部使用时，说明traffic policy下发失败是因为KB资源不足造成的。则通过如下方案解决：

1、可以通过配置TCAM ACL资源自定义分组，节省KB资源的占用（推荐）。具体请参考**3.1 减少组资源的占用（使用TCAM ACL资源自定义分组重新规划匹配字段和执行动作）**。

2、在V100R006C00版本及之后版本中，执行命令**traffic-policy resource-saving-mode**开启应用流策略时采用资源节约模式的功能，重新整合并下发所有流策略需要的ACL资源，以尝试将其他业务应用成功。

说明

1. 开启此功能时，设备上的所有流策略都会自动重新下发，可能会导致业务短暂中断。
2. 开启此功能后，在设备上应用新的流策略或者已应用的流策略包含的流分类、流行为、ACL规则发生变化时，设备上的所有流策略都会自动重新下发，可能会导致业务短暂中断。

4.3.1.3.2 Bank 资源不足

如果traffic policy下发失败是因为Bank资源不足，可以在系统视图下执行**display system tcam resourceacl** [**slot** *slot-id*]命令行查看设备Bank资源使用的详细情况：

```
[~HUAWEI] display system tcam resource acl
------------------------------------------------------------------------------
Slot  Chip TCAM     Resource Stage              Total     Used  Limited     Free
------------------------------------------------------------------------------
1     0    Internal Banks    Ingress+Egress        12       12       12        0
1     0    Internal Rules    Ingress+Egress     24576    20672     3904        0
1     0    Internal Meters   Ingress+Egress     65536        0        0    65536
1     0    Internal Counters Ingress            16384        0        0    16384
1     0    Internal Counters Egress              2816        0        0     2816
------------------------------------------------------------------------------
```

当“Free”显示为0时，则表示Bank资源不足，不能再下发相关的ACL业务。

解决方案：可以通过配置QoS组，减少占用的ACL规则的条数，从而节省Bank资源的占用。具体请参考**3.2 减少下发到芯片中的ACL规则数（将不同的VLAN或接口加入QoS组后应用相同流策略）**

4.3.1.3.3 没有包含匹配字段和动作组合的系统预置模板

如果traffic policy下发失败是因为系统预置模板中没有匹配字段和动作的组合，则通过如下方案解决：

1、通过配置TCAM ACL资源自定义分组使系统预置模板不支持的匹配字段和动作组合下发成功（推荐）。

具体请参考**3.1.2.4 4：没有包含匹配字段和动作组合的系统预置模板，policy下发失败**。

2、在V100R006C00版本及之后版本中，执行命令**traffic-policy resource-saving-mode**开启应用流策略时采用资源节约模式的功能，重新整合并下发所有流策略需要的ACL资源，以尝试将其他业务应用成功。

说明

1. 开启此功能时，设备上的所有流策略都会自动重新下发，可能会导致业务短暂中断。
2. 开启此功能后，在设备上应用新的流策略或者已应用的流策略包含的流分类、流行为、ACL规则发生变化时，设备上的所有流策略都会自动重新下发，可能会导致业务短暂中断。

5 附录

5.1 ACL 实际占用规则数目的计算方法

用户在配置ACL规则时，实际占用的rule的数目和用户在设备上所配置的rule的数目是不一样的，为了明确实际占用的rule资源，需要了解rule数目的计算方法。

说明

从V200R002C50版本开始，可以在诊断视图下，执行命令**display system tcam acl port-division** { **range** *begin-port-numberend-port-number* | **eq** *begin-port-number* | **gt** *begin-port-number-gt* | **lt** *end-port-number-lt* }查看ACL实际占用规则数。

在这里分为两种情景：

一、如果配置的N条rule都没有匹配四层端口号范围（portrange）时，则：

1）在全局下配置时，实际占用数目为N;

2）在接口、VLAN视图下配置时，实际占用数目为N*接口数。

二、如果配置的N条rule中有S条匹配了四层端口号范围的rule，若每条匹配四层端口号的rule实际占用数目为M，则：

1）在全局下配置时，实际占用数目为N-S+S*M;

2）在接口、VLAN视图下配置时，实际占用数目为(N-S+S*M)*接口数。

其中M的计算方法可以通过举例说明，例如配置如下：

#

acl number 3000

rule 5 permit tcp source-port range 100 200

#

首先将100转换为二进制数1100100，从低位开始找到第一个为1的位，即第2位，

找到第一个端口范围100 100+2^2-1，即100 103。

其次将104转换为二进制数1101000，从低位开始找到第一个为1的位，即第3位，

找到第二个端口范围104 104+2^3-1，即104 111。

再次将112转换为二进制数1110000，从低位开始找到第一个为1的位，即第4位，

找到第三个端口范围112 112+2^4-1，即112 127。

同理，可以找到第四个端口范围128 191，第五个端口范围192 199 第六个端口范围200 200

所以本例中一个rule实际占用数目为6，如果一条rule匹配了两个range，例如：

#

acl number 3000

rule 5 permit tcp source-port range 100 200 destination-port range 100 200

#

则该条rule实际占用数目为6*6，即36条。

