



## 配置指南-ACL&QOS

---

本分册介绍 ACL&QOS 配置指南相关内容，包括以下章节：

1. ACL
2. QOS
3. MMU

# 1 ACL

## 1.1 概述

ACLs (Access Control Lists, 接入控制列表), 也称为访问列表 (Access Lists), 俗称为防火墙, 在有的文档中还称之为包过滤。通过定义一些规则对网络设备接口上的数据报文进行控制: 允许通过、丢弃。

根据使用 ACL 目的的不同可分为: 安全 ACLs 和 QoS ACLs。

- 安全 ACLs 用于控制哪些数据流允许从网络设备通过。
- QoS ACLs 对这些数据流进行优先级分类和处理。

配置访问列表的原因比较多, 最主要的主要有以下一些:

- 网络访问控制: 为了确保网络安全, 通过定义规则, 可以限制用户访问一些服务 (如只需要访问 WWW 和电子邮件服务, 其他服务如 TELNET 则禁止), 或者仅允许在给定的时间段内访问, 或只允许一些主机访问网络等等。
- 优先服务保证: 为一些重要的数据流进行优先分类处理, 这就是 QoS ACLs 作用。有关 QoS ACLs 的使用请参考 QoS 相关的配置手册。

 下文仅介绍 ACL 的相关内容。

### 协议规范

无

## 1.2 典型应用

典型应用	场景描述
企业内网访问控制应用	在企业网中根据需要对各个部门的网络访问权限进行控制和限制, 比如服务器的访问限制、QQ 和 MSN 等聊天工具的使用限制等。

### 1.2.1 企业内网络访问控制应用

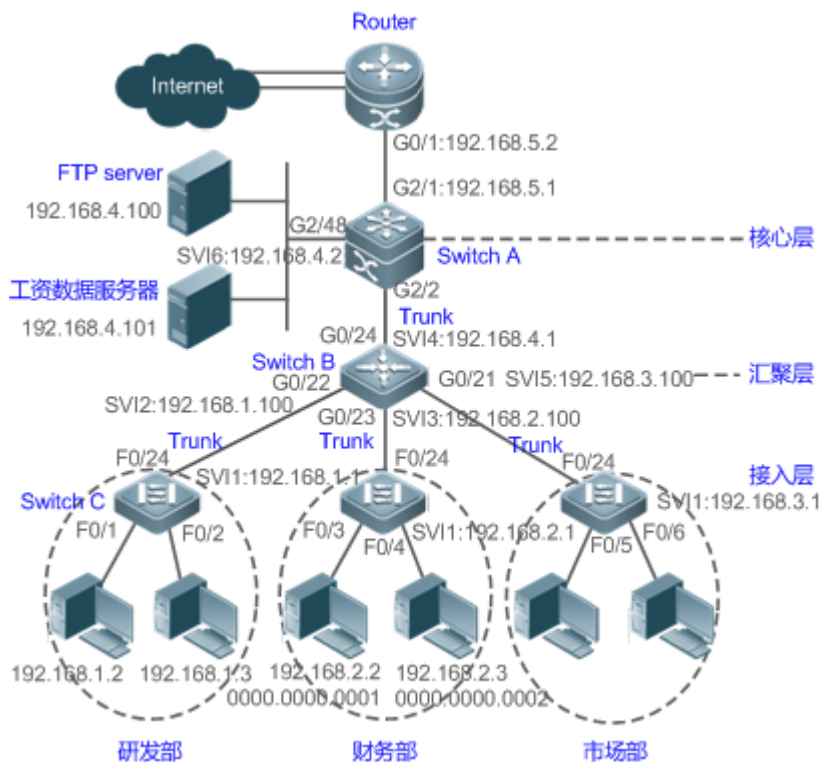
#### 应用场景

Internet 病毒无处不在, 需要封堵各种病毒的常用端口, 以保障内网安全:

- 只允许内部 PC 访问服务器, 不允许外部 PC 访问服务器。
- 不允许非财务部门 PC 访问财务部 PC; 不允许非研发部门 PC 访问研发部 PC。

- 不允许研发部门人员在上班时间（即 9:00~18:00）使用 QQ、MSN 等聊天工具。

图 1-1



- 【注释】 接入层设备 C：连接各部门的 PC，通过千兆光纤(trunk 方式)连接汇聚层设备。  
 汇聚层设备 B：划分多个 VLAN，每个部门为一个 VLAN，通过万兆光纤(trunk 方式)上连核心层设备。  
 核心层设备 A：连接各种服务器，如 FTP，HTTP 服务器等，通过防火墙与 Internet 相连。

## 功能部署

- 通过在核心层设备（本例为设备 A）上联 Router 的端口（本例为 G2/1 口）上设置扩展 ACL 来过滤相关端口的数据包来达到防病毒的目的。
- 要求内部 PC 对服务器进行访问，不允许外部 PC 访问服务器，可以通过定义 IP 扩展 ACL 并应用到核心层设备（本例为设备 A）的下联汇聚层设备和服务器的接口（本例为 G2/2 口/SVI 2）上实现。
- 要求特定部门间不能互访，可通过定义 IP 扩展 ACL 实现（本例中分别在设备 B 的 G0/22、G0/23 上应用 IP 扩展 ACL）；
- 可通过配置时间 IP 扩展 ACL，限制研发部门在特定时间内使用 QQ/MSN 等聊天工具（本例中在设备 B 的 SVI 2 上应用时间 IP 扩展 ACL）。

## 1.3 功能详解

### 基本概念

## 访问列表

访问列表有：基本访问列表和动态访问列表。

用户可以根据需要选择基本访问列表或动态访问列表。一般情况下，使用基本访问列表已经能够满足安全需要。但经验丰富的黑客可能会通过一些软件假冒源地址欺骗设备，得以访问网络。而动态访问列表在用户访问网络以前，要求通过身份认证，使黑客难以攻入网络，所以在一些敏感的区域可以使用动态访问列表保证网络安全。

**i** 通过假冒源地址欺骗设备即电子欺骗是所有访问列表固有的问题，使用动态列表也会遭遇电子欺骗问题：黑客可能在用户通过身份认证的有效访问期间，假冒用户的地址访问网络。解决这个问题的方法有两种，一种是尽量将用户访问的空闲时间设置小些，这样可以使黑客更难以攻入网络，另一种是使用 IPSEC 加密协议对网络数据进行加密，确保进入设备时，所有的数据都是加密的。

访问列表一般配置在以下位置的网络设备上：

- 内部网和外部网（如 INTERNET）之间的设备
- 网络两个部分交界的设备
- 接入控制端口的设备。

访问控制列表语句的执行必须严格按照表中语句的顺序，从第一条语句开始比较，一旦一个数据包的报头跟表中的某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

## 输入/输出 ACL、过滤域模板及规则

输入 ACL 在设备接口接收到报文时，检查报文是否与该接口输入 ACL 的某一条 ACE 相匹配；输出 ACL 在设备准备从某一个接口输出报文时，检查报文是否与该接口输出 ACL 的某一条 ACE 相匹配。

在制定不同的过滤规则时，多条规则可能同时被应用，也可能只应用其中几条。只要是符合某条 ACE，就按照该 ACE 定义的处理报文(Permit 或 Deny)。ACL 的 ACE 根据以太网报文的某些字段来标识以太网报文的，这些字段包括：

二层字段(Layer 2 Fields)：

- 48 位的源 MAC 地址(必须申明所有 48 位)
- 48 位的目的 MAC 地址(必须申明所有 48 位)
- 16 位的二层类型字段

三层字段(Layer 3 Fields)：

- 源 IP 地址字段(可以申明全部源 IP 地址值，或使用子网来定义一类流)
- 目的 IP 地址字段(可以申明全部目的 IP 地址值，或使用子网来定义一类流)
- 协议类型字段

四层字段(Layer 4 Fields)：

- 可以申明一个 TCP 的源端口、目的端口或者都申明，还可以申明源端口或目的端口的范围。
- 可以申明一个 UDP 的源端口、目的端口或者都申明，还可以申明源端口或目的端口的范围。

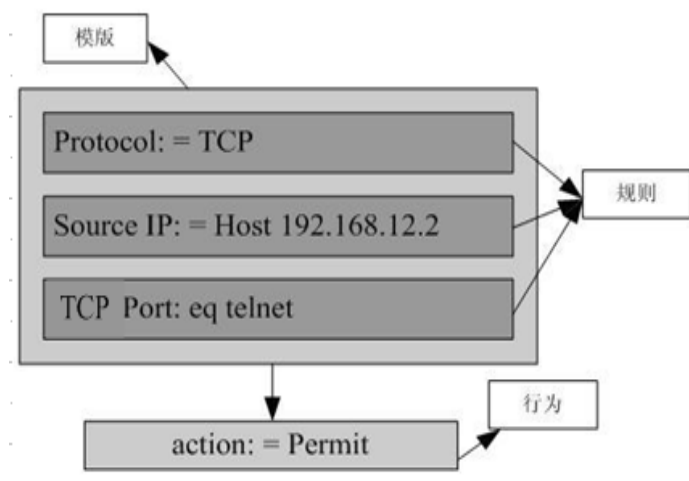
过滤域指的是，在生成一条 ACE 时，根据报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段组合的定义。比如，在生成某一条 ACE 时希望根据报文的目的 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据的是报文的源 IP 地址字段和 UDP 的源端口字段，这样，这两条 ACE 就使用了不同的过滤域模板。

规则(Rules)，指的是 ACE 过滤域模板对应的值。比如有一条 ACE 内容如下：

```
permit tcp host 192.168.12.2 any eq telnet
```

在这条 ACE 中，过滤域模板为以下字段的集合：源 IP 地址字段、IP 协议字段、目的 TCP 端口字段。对应的值(Rules)分别为：源 IP 地址 = Host 192.168.12.2；IP 协议 = TCP；TCP 目的端口 = Telnet。

图 1-2 对 ACE : permit tcp host 192.168.12.2 any eq telnet 的分析



- ❗ 过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。要使用二层、三层、四层字段集合，可以应用 Expert 扩展访问控制列表 (Expert ACLs)。
- ❗ OUT 方向 ACL 关联 SVI 的注意事项：支持 IP 标准，IP 扩展，MAC 扩展，专家级 ACL 应用。
- ❗ 对 ACL 中匹配目的 IP 和目的 MAC 有一些限制，如果在 MAC 扩展和专家级 ACL 中匹配目的 MAC，将这样的 ACL 应用到 SVI 的 OUT 方向时，表项会被设置，但无法生效。如果想要在 IP 扩展，专家级 ACL 中匹配目的 IP，而目的 IP 不在所关联的 SVI 的子网 IP 范围内时，该配置的 ACL 将无法生效。比如 VLAN 1 的地址为 192.168.64.1 255.255.255.0，创建一条 IP 扩展的 ACL，ace 为 deny udp any 192.168.65.1 0.0.0.255 eq 255，将该 ACL 应用到 VLAN 1 的出口，将无法生效，因为目的 IP 不在 VLAN 1 子网 IP 范围内，如果 ace 为 deny udp any 192.168.64.1 0.0.0.255 eq 255 将可以生效，因为目的 IP 符合规定。
- ✅ 交换机设备上，作用在物理口和 AP 口上的 OUT 方向 ACL，仅支持匹配知名报文（单播、组播），不支持匹配未知名单播，即对于未知名报文或者广播报文，端口上配置的 OUT 方向 ACL 不生效。
- ✅ 交换机设备上，输入 ACL 和 DOT1X，全局 IP+MAC 绑定，端口安全，IP SOURCE GUARD 共用时，PERMIT 和默认 DENY 的 ACE 不生效，其他 DENY 表项的 ACE 正常生效。
- ✅ 交换机设备上，输入 ACL 和 QOS 共用时，PERMIT ACE 不生效，其他 DENY 表项的 ACE 正常生效；默认 DENY 的表项在 QOS 表项的后面生效。
- ✅ 交换机设备上，通过 **no rgos-security compatible** 命令来使得基于端口的输入 ACL 和 DOT1X，全局 IP+MAC 绑定，端口安全，IP SOURCE GUARD 共用时，PERMIT，DENY 表项同时生效。

- ✓ 交换机设备上，ACL 同时应用于多个 SVI 的 IN 方向后，再添加 ACL 中的 ACE，保存配置后重启，由于硬件容量的原因，可能导致某几个 SVI 上的 ACL 无法配置上。
- i 当配置专家级的 ACL，并应用在接口的 out 方向时，如果该 ACL 中的某些 ACE 包含三层匹配信息（比如 IP，L4port 等），将导致从应用接口进入的非 IP 报文无法受该 ACL 的 permit 和 deny 规则控制。
- i 应用 ACL 时，如果 ACL（包括 IP 访问列表和 Expert 扩展访问列表）中的 ACE 匹配了非 L2 字段，比如 SIP，DIP 时，对于带标签的 MPLS 报文匹配是无效的。

## ACL logging

为了让用户更好的掌握 ACL 在设备中的运行状态，在添加规则时可以根据需要决定是否指定报文匹配日志输出选项，如果指定了该选项，则在规则匹配到报文时会输出匹配日志信息。ACL logging 信息是基于 ACE 来打印 log 信息的，也即设备周期性的打印命中报文的 ACE 信息，以及该 ACE 命中的报文数量。如下：

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

为合理控制 log 输出的数量和频率，ACL logging 支持配置 log 输出间隔的配置，并且支持分别配置 IPv4 ACL 和 IPv6 ACL 的 log 输出间隔。

- ! 带 ACL logging 选项的 ACE 使用更多的硬件资源，如果配置的所有 ACE 都带有 ACL logging 选项，则会导致设备的 ACE 容量减半。
- i 默认 ACL logging 的 log 输出间隔是 0，也即不输出 log。在为 ACE 指定了报文匹配日志输出选项后，若要输出相应的 log，需要配置 ACL logging 的输出间隔。
- i 对于带 ACL logging 选项的 ACE，如果指定的时间间隔内没有匹配到任何报文，则不会输出与该 ACE 有关的报文匹配日志；如果指定的时间间隔内有匹配到报文，则时间间隔到期后，会输出与该 ACE 有关的报文匹配日志。其中的报文中数目为该时间间隔内该 ACE 匹配到的报文总数，即为该 ACE 上一次输出 log 到本次输出 log 之间命中的报文数。
- i 仅在交换机设备上支持 ACL logging 功能。

## ACL 报文匹配计数

由于网络管理的需要，有时用户可能会想知道某条 ACE 有没有匹配到报文，匹配了多少个。因此，ACL 提供了基于 ACE 的报文匹配计数，用户可以基于 ACL 开启和关闭该 ACL 下的所有的 ACE 的报文匹配计数功能，支持的 ACL 类型包括：IP 访问列表、MAC 访问列表、Expert 访问列表和 IPv6 访问列表。此外，用户可通过 ACL 的统计清除命令将 ACL 规则的报文匹配计数器清 0，以便重新统计。

- ! 开启 ACL 的报文匹配计数功能需要更多的硬件表项，极端情况下会使设备可以配置的 ACE 容量减半。
- i 仅在交换机设备上支持 ACL 报文匹配计数功能。

## 功能特性

功能特性	作用
IP 访问列表	可以根据 IPv4 报文头部的三层或四层信息对进出设备的 IPv4 报文进行控制。
MAC 扩展访问列表	可以根据以太网报文的二层头部信息对进出设备的二层报文进行控制。
Expert 扩展访问列表	IP 访问列表和 MAC 扩展访问列表的组合，从而实现在同一条规则中可以实现同时根据报文的二层头部信息和报文三层或四层信息对进出设备的报文进行控制，以决定是丢弃还是放过指定的报文。
IPv6 访问列表	可以根据 IPv6 报文头部的三层或四层信息对进出设备的 IPv6 报文进行控制
ACL80	可以自定义匹配域和掩码，适应固定匹配域不能满足需求的场景
ACL 重定向	可以将进入设备的符合 ACL 规则的报文直接重定向到指定的出接口
全局安全 ACL	可以让 ACL 在所有接口的入方向上生效，无需在每个接口上分别应用 ACL
安全通道	可以让报文不经过 dot1x、web 认证等接入控制的检查，以满足特定场景的需求
SVI Router ACL	可以同一 VLAN 内的用户可以正常通信
报文匹配日志	可以根据需要每隔一段时间输出 ACL 的报文匹配日志信息，根据信息可以了解到指定规则的报文匹配情况

### 1.3.1 IP 访问列表

IP 访问列表主要用于对进出设备的 IPv4 报文进行精细化控制，用户可以根据实际需要阻止或允许特定的 IPv4 报文进入网络，从而实现控制 IP 用户访问网络资源的目的。

#### 工作原理

在 IP 访问列表中定义一系列的 IP 访问规则，然后将访问列表应用在接口的入方向或出方向上，当然还可以对 IP 访问列表进行全局应用，IPv4 报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。

下表列出了可以使用编号来指定访问列表的协议以及每种协议可以使用的访问列表编号范围。

协议	编号范围
标准 IP	1-99，1300 - 1999
扩展 IP	100-199，2000 - 2699

基本访问列表包括标准 IP 访问列表和扩展 IP 访问列表，访问列表中定义的典型规则主要包含以下匹配域：

- 源 IP 地址

- 目的 IP 地址
- IP 协议号
- 四层源端口号或 ICMP type
- 四层目的端口号或 ICMP code

标准 IP 访问列表（编号为 1 - 99，1300 - 1999）主要是根据源 IP 地址来进行转发或阻断分组的，扩展 IP 访问列表（编号为 100 - 199，2000 - 2699）可以对上述匹配域进行组合来控制报文的转发或阻断。

对于单一的访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越困难。

✔ 路由类产品上，ACL 规则中的 ICMP code 匹配域对于 ICMP type 为 3 的 ICMP 报文无效。如果 ACL 规则中配置了要匹配 ICMP 报文的 code 字段，当 type 为 3 的 ICMP 报文进入设备执行 ACL 匹配时，匹配结果可能与预期的不一样。

### 🔽 隐含“拒绝所有数据流”规则语句

在每个 IP 访问列表的末尾隐含着一行“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 1 permit host 192.168.4.12
```

此列表只允许源主机为 192.168.4.12 的报文通过，其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：  
access-list 1 deny any。

又如：

```
access-list 1 deny host 192.168.4.12
```

如果列表只包含以上这一条语句，则任何主机报文通过该端口时都将被拒绝。

❗ 在定义访问列表的时候，要考虑到路由更新的报文。由于访问列表末尾“拒绝所有数据流”，可能导致所有的路由更新报文被阻断。

### 🔽 输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后（但在默认规则语句之前），访问列表规则语句的输入次序非常重要，它决定了该规则语句在访问列表中的优先级，设备在决定转发还是阻断报文时，是按规则语句创建的次序将进行比较的，找到匹配的规则语句后，便不再检查其他规则语句。

假设创建了一条规则语句，它允许所有的数据流通过，则后面的语句将不被检查。

如下例：

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

由于第一条规则语句拒绝了所有的 IP 报文，所以 192.168.12.0/24 网络的主机 Telnet 报文将被拒绝，因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

## 相关配置



## 配置 IP 访问列表

缺省情况下，设备上无任何 IP 访问列表。

在配置模式下使用 **ip access-list { standard | extended } {acl-name | acl-id}** 命令可以创建一个标准 IP 访问列表或扩展 IP 访问列表，并进入标准或扩展 IP 访问列表模式。

## 配置 IP 访问列表匹配规则

缺省情况下，创建的 IP 访问列表中会有一条隐含的 deny 所有 IPv4 报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有 IPv4 报文，因此，如果用户想允许某些特定的 IPv4 报文进出设备，就得往访问列表中配置一些匹配规则。

对于标准 IP 访问列表，可以通过以下方式配置匹配规则：

- 不管是命名的标准 IP 访问列表，还是数值索引的标准 IP 访问列表，都可以在标准 IP 访问列表模式下使用 **[ sn ] { permit | deny } { host source | any | source source-wildcard } [ time-range time-range-name ] [ log ]** 命令为访问列表配置一条匹配规则。
- 数值索引的标准 IP 访问列表，除了可以在标准 IP 访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list acl-id { permit | deny } { host source | any | source source-wildcard } [ time-range tm-rng-name ] [ log ]** 命令为标准 IP 访问列表配置一条匹配规则。

对于扩展 IP 访问列表，可以通过以下方式配置匹配规则：

- 不管是命名的扩展 IP 访问列表，还是数值索引的扩展 IP 访问列表，都可以在扩展 IP 访问列表模式下使用 **[ sn ] { permit | deny } protocol { host source | any | source source-wildcard } { host destination | any | destination destination-wildcard } [ [ precedence precedence [ tos tos ] ] | dscp dscp ] [ fragment ] [ time-range time-range-name ] [ log ]** 命令为访问列表配置一条匹配规则。
- 数值索引的扩展 IP 访问列表，除了可以在扩展 IP 访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list acl-id { permit | deny } protocol { host source | any | source source-wildcard } { host destination | any | destination destination-wildcard } [ [ precedence precedence [ tos tos ] ] | dscp dscp ] [ fragment ] [ time-range time-range-name ] [ log ]** 命令为标准 IP 访问列表配置一条匹配规则。

## 应用 IP 访问列表

缺省情况下，设备上的所有接口下都没有应用 IP 访问列表，也就是说 IP 访问列表不会对进出设备的 IP 报文进行匹配过滤。

在接口下使用 **ip access-group { acl-id | acl-name } { in | out }** 命令可以让一个标准 IP 访问列表或扩展 IP 访问列表在指定的接口上生效。

## 1.3.2 MAC 扩展访问列表

MAC 扩展访问列表主要是基于报文的二层头部来对进出设备的报文进行精细化控制，用户可以根据实际需要阻止或允许特定的二层报文进入网络，从而实现控制保护网络资源不受攻击或者基于些控制用户访问网络资源的目的。

## 工作原理

在 MAC 扩展访问列表中定义一系列的 MAC 访问规则，将访问列表应用在接口的入方向或出方向上，报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置 MAC 扩展访问列表，必须给访问列表指定一个唯一的名称或编号，以便唯一标识每个访问列表。下表列出可以使用编号来指定 MAC 扩展访问列表编号范围。

协议	编号范围
MAC 扩展访问列表	700-799

MAC 扩展访问列表中定义的典型规则主要有以下：

- 源 MAC 地址
- 目标 MAC 地址
- 以太网协议类型

从上面的规则字段可以看出，MAC 扩展访问列表（编号 700 -799）主要是根据源或目的 MAC 地址以及报文的以太网类型来匹配报文分组的。

对于单一的 MAC 扩展访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越来越困难。

- ✔ 如果 MAC 扩展访问列表规则中没有指定是针对 IPv6 报文，即没有定义以太网类型字段或定义的以太网类型字段值不是 0x86dd，那么 MAC 扩展访问列表不对去匹配 IPv6 报文，如果用户想匹配过滤 IPv6 报文，请使用 IPv6 扩展访问列表。

### 隐含“拒绝所有数据流”规则语句

在每个 MAC 扩展访问列表的末尾隐含着一行“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 700 permit host 00d0.f800.0001 any
```

此列表只允许来自 MAC 地址为 00d0.f800.0001 的主机发出的报文通过，来自其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 700 deny any any。

## 相关配置

### 配置 MAC 扩展访问列表

缺省情况下，设备上无任何 MAC 扩展访问列表。

在配置模式下使用 **mac access-list extended** {acl-name | acl-id} 命令可以创建一个 MAC 扩展访问列表，并进入 MAC 扩展访问列表模式。

### 配置 MAC 扩展访问列表匹配规则

缺省情况下，创建的 MAC 扩展访问列表中会有一条隐含的 deny 所有二层报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有二层报文，因此，如果用户想允许某些特定的二层报文进出设备，就得往访问列表中配置一些匹配规则。

可以通过以下方式配置匹配规则：

- 不管是命名的 MAC 扩展访问列表，还是数值索引的 MAC 扩展访问列表，都可以在 MAC 扩展访问列表模式下使用[sn] { **permit** | **deny** } { **any** | **host** *src-mac-addr* | *src-mac-addr mask* } { **any** | **host** *dst-mac-addr* | *dst-mac-addr mask* } [*ethernet-type*] [**cos** *cos*] [**inner** *cos*] [ **time-range** *tm-rng-name* ]命令为访问列表配置一条匹配规则。
- 数值索引的 MAC 扩展访问列表，除了可以在 MAC 扩展访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list** *acl-id* { **permit** | **deny** } { **any** | **host** *src-mac-addr* | *src-mac-addr mask* } { **any** | **host** *dst-mac-addr* | *dst-mac-addr mask* } [*ethernet-type*] [**cos** *cos*] [**inner** *cos*] [ **time-range** *time-range-name* ]命令为 MAC 扩展访问列表配置一条匹配规则。

## 应用 MAC 扩展访问列表

缺省情况下，设备上的所有接口都没有应用 MAC 扩展访问列表，也就是说创建的 MAC 扩展访问列表不会对进出设备的二层报文进行匹配过滤。

在接口下使用 **mac access-group** { *acl-id* | *acl-name* } { **in** | **out** } 命令可以让一个 MAC 扩展访问列表在指定的接口上生效。

## 1.3.3 Expert 扩展访问列表

如果用户想在同一条规则中既对报文的二层信息匹配，又对报文的三层信息进行匹配，那么就可以选择 Expert 扩展访问列表。可以将 Expert 扩展访问列表看作是 IP 访问列表和 MAC 扩展访问列表的一种结合与增强，之所以说是一种结合与增强，是因为 Expert 扩展访问列表中的规则不仅可以包含 IP 访问列表规则和 MAC 扩展访问列表规则，同时可以指定基于 VLAN ID 来匹配报文。

### 工作原理

在 Expert 扩展访问列表中定义一系列的访问规则，将访问列表应用在接口的入方向或出方向上，报文进出设备时，设备就会通过判断报文是否与访问规则匹配来决定是否转发或阻断报文。

要在设备上配置 Expert 扩展访问列表，必须给协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出 Expert 访问列表的编号范围。

协议	编号范围
Expert 扩展访问列表	2700-2899

创建 expert 扩展访问列表时，定义的规则可以应用于所有的分组报文，通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

Expert 访问列表中定义的典型规则主要有以下：

- 基本访问列表和 MAC 扩展访问列表所有的信息
- VLAN ID

Expert 扩展访问列表（编号 2700 -2899）为基本访问列表和 MAC 扩展访问列表的综合体，并且能对 VLAN ID 进行过滤。

对于单一的 Expert 扩展访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句需引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。

- ✔ 如果 Expert 扩展访问列表规则中没有指定是针对 IPv6 报文，即没有定义以太网类型字段或以太网类型字段不是 0x86dd，那么 Expert 扩展访问列表不对去匹配 IPv6 报文，如果用户想匹配过滤 IPv6 报文，请使用 IPv6 扩展访问列表。

### 🔽 隐含“拒绝所有数据流”规则语句

在每个 Expert 扩展访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 2700 permit 0x0806 any any any any any
```

此列表只允许以太网类型为 0x0806(即 ARP)的报文通过，其他类型的报文都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 2700 deny any any any any。

## 相关配置

### 🔽 配置 Expert 扩展访问列表

缺省情况下，设备上无任何 Expert 扩展访问列表。

在配置模式下使用 **expert access-list extended** {acl-name | acl-id} 命令可以创建一个 Expert 扩展访问列表，并进入 Expert 扩展访问列表模式。

### 🔽 配置 Expert 扩展访问列表匹配规则

缺省情况下，创建的 Expert 扩展访问列表中会有一条隐含的 deny 所有报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有二层报文，因此，如果用户想允许某些特定的二层报文进出设备，就得往访问列表中配置一些匹配规则。

可以通过以下方式配置匹配规则：

- 不管是命名的 Expert 扩展访问列表，还是数值索引的 Expert 扩展访问列表，都可以在 Expert 扩展访问列表模式下使用[sn] { **permit** | **deny** } [protocol] [ [ ethernet-type ] [ **cos** [ out ] [ inner in ] ] ] [ [ **VID** [ out ] [ inner in ] ] ] { source source-wildcard | **host** source | **any** } { **host** source-mac-address | **any** } { destination destination-wildcard | **host** destination | **any** } { **host** destination-mac-address | **any** } [ **precedence** precedence ] [ **tos** tos ] [ **fragment** ] [ **range** lower upper ] [ **time-range** time-range-name ]命令为访问列表配置一条匹配规则。
- 数值索引的 MAC 扩展访问列表，除了可以在 MAC 扩展访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list** acl-id { **permit** | **deny** } [[protocol] [ [ ethernet-type ] [ **cos** [ out ] [ inner in ] ] ] [ [ **VID** [ out ] [ inner in ] ] ] ] { source source-wildcard | **host** source | **any** } { **host** source-mac-address | **any** } { destination destination-wildcard | **host** destination | **any** } { **host** destination-mac-address | **any** } [ **precedence** precedence ] [ **tos** tos ] [ **fragment** ] [ **range** lower upper ] [ **time-range** time-range-name ]命令为 Expert 扩展访问列表配置一条匹配规则。

## 应用 Expert 扩展访问列表

缺省情况下，设备上的所有接口都没有应用 Expert 扩展访问列表，也就是说创建的 Expert 扩展访问列表不会对进出设备的所有二三层报文进行匹配过滤。

在接口下使用 **expert access-group** { *acl-id* | *acl-name* } { **in** | **out** } 命令可以让一个 Expert 扩展访问列表在指定的接口模式上生效。

## 1.3.4 IPv6 访问列表

IPv6 访问列表主要用于对进出设备的 IPv6 报文进行精细化控制，用户可以根据实际需要阻止或允许特定的 IPv6 报文进入网络，从而实现控制 IPv6 用户访问网络资源的目的。

### 工作原理

在 IPv6 访问列表中定义一系列的 IPv6 访问规则，并将访问列表应用在接口的入方向或出方向上，IPv6 报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称。

- ❗ 与 IP 访问列表、MAC 扩展访问列表以及 Expert 扩展访问列表不同，创建 IPv6 访问列表时只能指定名称，不能指定编号。
- ❗ 设备接口的入方向或出方向上只能应用一条 IP 访问列表或一条 MAC 扩展访问列表，或者应用一条 Expert 扩展访问列表，除此之外，还可以再应用一条 IPv6 访问列表。

## 隐含“拒绝所有数据流”规则语句

在每个 IPv6 访问列表的末尾隐含着一一条“拒绝所有 IPv6 数据流”规则语句，因此如果报文与任何规则都不匹配，将被拒绝。

如下例：

```
ipv6 access-list ipv6_acl
10 permit ipv6 host 200::1 any
```

此列表只允许源主机为 200::1 的 IPv6 报文通过，其它主机发出的 IPv6 报文都将被拒绝。因为这条访问列表最后包含了一条规则语句：deny ipv6 any any。

- ❗ IPv6 访问列表虽然有默认拒绝所有 IPv6 报文的规则语句，但不会过滤 ND 报文。

## 输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后（但在默认规则语句之前），访问列表规则语句的输入次序非常重要，它决定了该规则语句在访问列表中的优先级，设备在决定转发还是阻断报文时，是按规则语句创建的次序将进行比较的，找到匹配的规则语句后，便不再检查其他规则语句。

假设创建了一条规则语句，它允许所有的 IPv6 数据流通过，则后面的语句将不被检查。

如下例：

```
ipv6 access-list ipv6_acl
 10 permit ipv6 any any
 20 deny ipv6 host 200::1 any
```

由于第一条规则语句放过了所有的 IPv6 报文，所以主机 200::1 发出的 IPv6 报文都无法命中序号为 20 的那条 deny 规则而被放过。因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

## 相关配置

### 配置 IPv6 访问列表

缺省情况下，设备上无任何 IPv6 访问列表。

在配置模式下使用 **ipv6 access-list *acl-name*** 命令可以创建一个 IPv6 访问列表，并进入 IPv6 访问列表模式。

### 配置 IPv6 访问列表匹配规则

缺省情况下，创建的 IPv6 访问列表中会有一条隐含的 deny 所有 IPv6 报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有 IPv6 报文，因此，如果用户想允许某些特定的 IPv6 报文进出设备，就得往访问列表中配置一些匹配规则。

在 IPv6 访问列表模式下使用 **[sn] {permit | deny} protocol {src-ipv6-prefix/prefix-len | host src-ipv6-addr | any} {dst-ipv6-pfx/pfx-len | host dst-ipv6-addr | any} [range lower upper] [dscp dscp] [flow-label flow-label] [fragment] [time-range tm-rng-name] [log]** 命令配置一条 IPv6 访问列表规则。

### 应用 IPv6 访问列表

缺省情况下，设备上的所有接口都没有应用任何 IPv6 访问列表，也就是说 IPv6 访问列表不会对进出设备的 IPv6 报文生效。

在接口下使用 **ipv6 traffic-filter *acl-name* { in | out }** 命令可以让一个 IPv6 访问列表在指定的接口上生效。

## 1.3.5 ACL80

ACL80 即 Expert 高级访问列表，同时也叫自定义访问列表，针对报文的前 80 个字节进行匹配过滤。报文的 SMAC/DMAC/SIP/DIP/ETYPE 不计算在任意指定的字段中，ACL80 在匹配报文的以上这些字段之后，还能再匹配额外指定的 16 个字节内容。

## 工作原理

报文是由一系列的字节流组成，ACL80 可以让用户对报文的前 80 个字节中的指定 16 个字节按比特（bit）位进行匹配过滤。对于任意一个 16 字节字段，可以按照 bit 形式与所设置的值进行比较或不比较。也就是说，它允许我们对这 16 个字节的任意一个比特设置该值为 0 或 1。在对任何一个字节进行过滤时，有三个要素：匹配域内容、匹配域掩码以及匹配的起始位置。匹配域内容和匹配域掩码二者的比特位是一一对应的。过滤规则指明需要过滤字段值，过滤域模板指明过滤规则中对应字段是否需要过滤（1 表示匹配对应过滤规则的比特位，0 表示不匹配），所以当需要匹配某个比特时，必须将过滤域模板中对应的比特位设置为 1。如果过滤域模板比特位设置为 0，无论过滤规则中对应的比特位是什么，都不会匹配。

例如：

```
Ruijie(config)# expert access-list advanced name
Ruijie(config-exp-dacl)# permit 00d0f8123456 ffffffff 0
Ruijie(config-exp-dacl)# deny 00d0f8654321 ffffffff 6
```

用户自定义访问控制列表根据用户的定义对二层数据帧的前 80 个字节中的任意字节进行匹配，对数据报文作出相应的处理。正确使用用户自定义访问控制列表需要用户对二层数据帧的构成有深入的了解。下表为二层数据帧的前 64 个字节的示意图( 每个字母代表一个 16 进制数，每两个字母代表一个字节 )。

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II JJ KK LL LL MM MM


NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT


UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

在上图中，各个字母的含义及偏移量取值如下表所示：

字母	含义	偏移量	字母	含义	偏移量
A	目的 MAC	0	O	TTL 字段	34
B	源 MAC	6	P	协议号	35
C	VLAN tag 字段	12	Q	IP 校验和	36
D	数据帧长度字段	16	R	源 ip 地址	38
E	DSAP(目的服务访问点)字段	18	S	目的 ip 地址	42
F	SSAP(源服务访问点)字段	19	T	TCP 源端口	46
G	Ctrl 字段	20	U	TCP 目的端口	48
H	Org Code 字段	21	V	序列号	50
I	封装的数据类型	24	W	确认字段	54
J	IP 版本号	26	XY	IP 头长度和保留比特位	58
K	TOS 字段	27	Z	保留比特位和 flags 比特位	59
L	IP 包的长度	28	a	Windows size 字段	60
M	ID 号	30	b	其他	62
N	Flags 字段	32			

上表中各个字段的偏移量是它们在 SNAP + tag 的 802.3 数据帧中的偏移量。在用户自定义访问控制列表中，用户可以使用规则掩码和偏移量两个参数共同从数据帧中提取前 80 个字节中的任意字节，然后和用户定义的规则比较，从而过滤出匹配的数据帧，作相应的处理。用户定义的规则可以是数据的某些固定属性，比如用户要将所有的 TCP 报文过滤出来，可以将规则定义为“06”，规则掩码定义为“FF”，偏移量定义为 35，此时规则掩码和偏移量共同作用，把接收到的数据帧中的 TCP 协议号字段的内容提取出来，和规则比较，匹配出所有的 TCP 报文。

 仅在交换机设备上支持 ACL80；

 ACL80 可以支持匹配以太网报文，803.3snap 报文，802.3llc 报文，如果设置匹配 DSAP 到 cntl 字段的值为 AAAA03，则表示希望匹配 803.3snap 报文，如果设置匹配 DSAP 到 cntl 字段的值为 E0E003，则表示希望匹配 803.3llc 报文。以太网报文不能设置匹配该字段；



- ❗ ACL80 可以任意匹配的资源只有 16 个字节，如果这 16 个字节的资源已经被使用，那么就无法再匹配这 16 个字节之外的字段。

## 相关配置

### 配置 Expert 高级访问列表

缺省情况下，设备上无任何 Expert 高级访问列表。

在配置模式下使用 **expert access-list advanced *acl-name*** 命令可以创建一个 Expert 高级访问列表，并进入 Expert 高级访问列表模式。

### 配置 Expert 高级访问列表匹配规则

缺省情况下，创建的 Expert 高级访问列表中会有一条隐含的 deny 所有报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有二层报文，因此，如果用户想允许某些特定的二层报文进出设备，就得往访问列表中配置一些匹配规则。

可以在 Expert 高级访问列表模式下使用 **[*sn*] { permit | deny } *hex hex-mask offset*** 命令为访问列表配置一条匹配规则。

### 应用 Expert 高级访问列表

缺省情况下，设备上的所有接口都没有应用 Expert 高级访问列表，也就是说创建的 Expert 高级访问列表不会对进出设备的所有报文进行匹配过滤。

在接口模式下使用 **expert access-group *acl-name* { in | out }** 命令可以让一个 Expert 高级访问列表在指定的接口上生效。

## 1.3.6 ACL 重定向

ACL 重定向功能的作用是使得设备能够对收到的报文进行分析并且重定向到指定端口转发出去。当要分析进入设备的特定报文时，可以配置 ACL 重定向功能，把符合规则报文重定向到指定端口上，在这个端口上把报文抓下来加以分析。

## 工作原理

ACL 重定向通过在一个接口上绑定不同的 ACL 策略，并给每个策略指定一个输出目的口，当该接口收到报文时，将逐条查找绑定在该接口上的 ACL 策略，如果报文符合某条策略描述的特征，将从该策略所指定的目的口转发，从而达到基于流来重定向报文的效果

- ❗ 仅在交换机设备上支持 ACL 重定向功能；
- ❗ ACL 重定向功能仅在接口入方向生效。

## 相关配置

### 配置访问列表



在配置 ACL 重定向功能之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

#### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

#### 配置 ACL 重定向

缺省情况下，设备上无任何的 ACL 重定向配置。

在接口模式下使用 **redirect destination interface** *interface-name* **acl** {*acl-id* | *acl-name*} **in** 命令配置 ACL 重定向功能。

❗ 只支持在以太口、聚合口、SVI 上配置 ACL 重定向功能。

### 1.3.7 全局安全 ACL

由于安全部署上的需要，端口安全 ACL 常被配置作为病毒报文过滤及防范使用，用于过滤符合某些特征的报文，比如：TCP 攻击端口。各种病毒报文在全局网络环境中存在，且各端口下的病毒报文识别特征相同或相似，因此通常情况下会创建一个 ACL，添加匹配各种病毒特征的 deny ace 后，通过端口安全 ACL 将 ACL 应用到交换机各个端口，以达到病毒过滤的作用。

端口安全 ACL 用于病毒过滤等抗攻击场景时，存在较多不便，一是需要逐个端口配置，存在重复配置、操作性能低下及 ACL 资源过度消耗的情况；二是安全 ACL 的访问控制作用被弱化，由于被用于病毒过滤，安全 ACL 的限制路由更新、限制网络访问等基本功能无法正常使用。而全局安全 ACL 可以在不影响端口安全 ACL 的情况下，进行全局抗病毒部署及防御。全局安全 ACL 只需要一条命令就可以在所有二层接口上生效，而不需要象端口安全 ACL 那样需要在每个接口上进行重复配置。

#### 工作原理

局安全 ACL 在所有二层接口上生效，当全局安全 ACL 与端口安全 ACL 同时配置时，两者共同生效，对于命中全局安全 ACL 的报文将被当作病毒报文直接过滤，对于没有命中全局安全 ACL 的报文将继续受端口安全 ACL 控制；如果想让某些端口不受全局安全 ACL 的控制，可以在这些接口上独立关闭全局安全 ACL 检查功能。

- ❗ 由于全局安全 ACL 主要用于病毒过滤，因此被关联于全局安全 ACL 的 ACL 中，只有 deny 类型的 ACE 会安装生效，permit 类型的 ACE 不会生效；
- ❗ 与端口上应用的安全 ACL 不同，全局安全 ACL 没有默认的 deny 所有表项，即没命中规则的报文都是放过的；
- ❗ 全局 ACL 可以在二层口上生效，也可以路由口上也生效。即可以在以下类型的端口上都生效：access、trunk、hibird、路由口、ap 口(二层或三层)。在 SVI 口上不生效。
- ❗ 允许在物理端口和 AP 口上独立关闭全局安全 ACL 功能，不支持在 AP 成员口上关闭；
- ❗ 全局安全 ACL 只支持关联 IP 标准 ACL、IP 扩展 ACL、MAC 扩展 ACL、Expert 扩展 ACL；

#### 相关配置

##### 配置访问列表

在配置全局安全 ACL 功能之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表的相关章节说明。

### 配置全局安全 ACL

缺省情况下，设备上无任何的全局安全 ACL 配置。

在配置模式下使用 `{ip | mac | Expert } access-group acl-id { in | out }` 命令开启全局安全 ACL 功能。

### 配置全局安全 ACL 例外口

缺省情况下，设备上无任何的全局安全 ACL 例外口配置。







在接口模式下使用 `no global access-group` 命令关闭指定接口上全局安全 ACL 功能。

## 1.3.8 安全通道

在某些应用场景中，可能会需要保证符合某些特征的报文绕过接入控制应用的检查，比如 dot1x 认证前，要允许用户登录到指定的资源站点上下载 dot1x 认证客户端；使用安全通道可以达到这个目的。将安全 ACL 通过安全通道配置命令应用到全局或者接口，就表示该 ACL 是一条安全通道

### 工作原理

安全通道其实也是一个访问控制列表，可以基于全局或者接口配置。报文进入到接口时，首先进行安全通道的检查，如果满足安全通道的匹配条件，将绕过接入控制比如端口安全，web 认证、dot1x，Ip+MAC 绑定的检查直接进入交换机。应用于全局的安全通道对所有非例外口都生效。

-  应用于安全通道的访问控制列表的 deny 行为不生效，并且不存在末尾隐含着一条“拒绝所有数据流”规则的语句，如果报文不符合安全通道的匹配条件，将按流程进行接入控制的检查；
-  全局安全通道的例外口最多可以设置 8 个且全局安全通道的例外口不能用来设置基于接口的安全通道。
-  如果接口上应用了安全通道，并且还在全局的安全通道，那么全局安全通道不在这个接口上生效。
-  基于端口可迁移认证模式和安全通道共用时，安全通道不生效。
-  不支持将 IPv6 访问列表配置成安全通道。
-  仅在交换机设备上支持安全通道。

### 相关配置

#### 配置访问列表

在配置安全通道功能之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表以及 Expert 扩展访问列表的相关章节说明。

### 配置接口安全通道

缺省情况下，设备上无任何的接口安全通道配置。

在接口模式下使用 **security access-group {acl-id | acl-name}** 命令配置接口安全通道。

### 配置全局安全通道

缺省情况下，设备上无任何的全局安全通道配置。

在配置模式下使用 **security global access-group {acl-id | acl-name}** 命令配置全局安全通道。

### 配置全局安全通道例外口

缺省情况下，设备上无任何的全局安全通道例外口配置。

在接口模式下使用 **security uplink enable** 命令将指定接口配置为全局安全通道例外口。

## 1.3.9 SVI Router ACL

默认情况下，应用在 SVI 接口上的访问列表会同时对 VLAN 内二层转发的报文及 VLAN 间的路由报文生效，从而导致同一 VLAN 内不同用户之间无法正常通信等异常现象。为此，提供了一种切换手段，可以使得应用在 SVI 接口上的访问列表仅对 VLAN 间的路由报文生效。

### 工作原理

缺省情况下，SVI Router ACL 功能默认关闭，SVI ACL 同时对 VLAN 间的三层转发报文及 VLAN 内的桥转发报文生效。SVI Router ACL 功能开启后，SVI ACL 仅对 VLAN 间的三层转发报文生效。



仅在交换机设备上支持 SVI Router ACL。

### 相关配置

#### 配置访问列表

在配置带 SVI Router ACL 之前，一般来说要先配置访问列表应用，在应用访问列表前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

#### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

#### 应用访问列表

访问列表的应用配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。应用时，在 SVI 对应的接口模式应用。

### 配置 SVI Router ACL

全局模式使用 **svi router-acls enable** 命令开启 SVI Router ACL 功能，使得应用在 SVI 接口上的访问列表仅对三层转发的报文生效，而不对同一 VLAN 内二层转发的报文生效。

## 1.3.10 报文匹配日志






报文匹配日志主要用于监控访问列表规则的运行状态，为日常网络维护以及网络优化提供必要的信息。

### 工作原理

为了让用户更好的掌握 ACL 在设备中的运行状态，在添加规则时可以根据需要决定是否指定报文匹配日志输出选项，如果指定了该选项，则在规则匹配到报文时会输出匹配日志信息。ACL logging 信息是基于 ACE 来打印 log 信息的，也即设备周期性的打印命中报文的 ACE 信息，以及该 ACE 命中的报文数量。如下：

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

为合理控制 log 输出的数量和频率，ACL logging 支持配置 log 输出间隔的配置。

-  带 log 选项的访问列表规则会使用更多的硬件资源，如果配置的所有规则都带有 log 选项，则会导致设备的硬件策略容量减半。
-  默认报文匹配日志输出间隔是 0，即不输出上层。在配置访问列表规则时指定了 log 选项后，还需要配置输出间隔，否则不会输出匹配日志。
-  对于带 log 选项的规则，如果指定的时间间隔内没有匹配到任何报文，则不会输出与该规则有关的报文匹配日志；如果指定的时间间隔内有匹配到报文，则时间间隔到期后，会输出与该规则有关的报文匹配日志。其中的报文命中数目为该时间间隔内该规则匹配到的报文总数，即为该规则上一次输出日志到本次输出日志之间命中的报文数。
-  仅在交换机设备上支持报文匹配日志功能。
-  仅支持为 IP 访问列表和 IPv6 访问列表规则配置 log 选项。

### 相关配置

#### 配置访问列表

在配置带 log 选项的访问列表规则之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

#### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表以及 IPv6 访问列表的相关章节说明。注意要配置 log 选项。

#### 配置报文匹配日志输出间隔

在配置模式下使用 `{ip | ipv6} access-list log-update interval time` 命令配置报文匹配日志输出间隔。

#### 应用访问列表

访问列表规则的应用方法请参考 IP 访问列表以及 IPv6 访问列表的相关章节说明。

### 1.3.11 报文匹配计数

除了报文匹配日志外，报文匹配计数为日常的网络维护和网络优化提供了另一种选择。

#### 工作原理

出于网络管理的需要，用户可能会想知道某条访问列表规则有没有匹配到报文，匹配了多少个。因此，ACL 提供了基于规则的报文匹配计数功能，用户可以基于 ACL 开启和关闭该 ACL 下的所有规则的报文匹配计数功能，当有报文匹配到了这条规则，对应的匹配计数就相应地增长。用户可通过 ACL 的统计清除命令将该 ACL 下所有规则的报文匹配计数器清 0，以便重新统计。

- ❗ 开启 ACL 的报文匹配计数功能需要更多的硬件表项，极端情况下会使设备可以配置的硬件策略容量减半。
- ✅ 支持在 IP 访问列表、MAC 访问列表、Expert 扩展访问列表和 IPv6 访问列表上开启报文匹配计数功能。
- ✅ 仅在交换机设备上支持 ACL 报文匹配计数功能。

#### 相关配置

##### 配置访问列表

在配置带 log 选项的访问列表规则之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

##### 配置访问列表规则

访问列表规则的配置方法请参考访问列表的相关章节说明。注意要配置 log 选项。

##### 开启报文匹配计数

如果用户想在 IP 访问列表、MAC 扩展访问列表或者 Expert 扩展访问列表上开始报文匹配计数功能，请在配置模式下使用 `{mac | expert | ip} access-list counter { acl-id | acl-name }` 命令来开启；如果用户想在 IPv6 访问列表上开始报文匹配计数功能，请在配置模式下使用 `ipv6 access-list counter acl-name`。

##### 应用访问列表

访问列表规则的应用方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

##### 清除报文匹配计数

在特权模式下使用 `clear counters access-list [acl-id | acl-name]` 命令来清除。

### 1.3.12 分片报文匹配模式

使用分片报文匹配模式可以使得访问列表对分片报文进行更精细化的控制。

#### 工作原理

对于 IP 报文,在网络传输时中可能会被分片。报文发生分片时,只有首片报文带有四层信息,比如 TCP 或 UDP 端口号、ICMP 类型和 ICMP 编码等,其他的分片报文都不带有这些四层信息。默认情况下,如果 ACL 规则带有 fragment 标识,则只会去匹配非首片报文;如果 ACL 规则不带有 fragment 标识,则匹配所有报文,包括首片报文和后续的所有分片报文。除了这种默认的分片报文匹配模式外,还提供了另一种新的分片报文匹配方法,用户可以根据需要在指定的 ACL 上进行切换。新的分片报文匹配模式与默认的分片报文匹配模式的区别就在于:当访问列表规则中不带有 fragment 标识时,如果报文被分片,首片报文会去匹配规则中用户定义的所有匹配域(包括三层和四层信息),而非首片报文则只会去匹配规则中的非四层信息。

- ❗ 分片报文新匹配模式下,如果 ACL 规则不带 fragment 标识,且匹配动作是 permit,这样的 ACL 规则需要占用更多的硬件表项资源,极端情况下会使得硬件策略表项容量减半;如果这样的 ACE 配置了 TCP flag 过滤控制的 established,则还会占用更多的硬件策略表项。
- ❗ 执行分片报文匹配模式切换时,会导致 ACL 的短时失效。
- ✅ 分片报文新匹配模式下,如果 ACL 规则不带 fragment 标识并且需要匹配报文的四层信息时,当匹配动作为 permit 时,ACL 规则会检查首片报文三层和四层信息,对于非首片报文只会检查报文的三层信息;当匹配动作为 deny 时,ACL 规则只会检查首片报文,不会去检查分片报文。
- ✅ 分片报文新匹配模式下,如果 ACL 规则带有 fragment 标识,不论 ACL 规则的匹配动作是 permit 还是 deny,都只检查非首片报文,而不会去检查首片报文。
- ✅ 仅在 IP 扩展 ACL 和 Expert 扩展 ACL 上支持分片报文匹配模式的切换。
- ✅ 仅在交换机设备上支持分片报文的匹配。

#### 相关配置

##### 配置访问列表

访问列表的配置说明请参考 IP 访问列表和 Expert 扩展访问列表的相关章节说明。

##### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表和 Expert 扩展访问列表的相关章节说明。配置时需要注意添加 fragment 选项。

##### 切换分片报文匹配模式

在配置模式下使用[ no ] {ip |expert} access-list new-fragment-mode { acl-id | acl-name }命令进行分片报文匹配模式的切换。

##### 应用访问列表

访问列表规则的应用方法请参考 IP 访问列表以及 Expert 扩展访问列表的相关章节说明。

## 1.4 产品说明



S6000E 系列产品，作用在 IN 方向的 acl 不支持 TCP、UDP 报文 4 层端口的“neq”匹配，作用在 OUT 方向的 ACL 仅支持 TCP、UDP 报文 4 层端口的“eq”匹配。



S6000E 系列产品，Ipv6 acl 可以支持匹配的区域为：Protocol, sip, l4\_src,dip, l4\_dst, dip, dscp, flow\_label.，在一个 ipv6 的 acl 内，只支持以下两种匹配域选择中的任意一种：

- protocol, sip, l4\_src, l4\_dst, dscp, flow\_label,range
- protocol, dip, l4\_src, l4\_dst, dscp, flow\_label,range
- 不支持在一个 acl 内匹配上述所有区域。此外,ipv6 acl 不支持匹配 fragment ;ipv6 acl 出口方向不支持 flowlabel。
- 当 sip 和 dip 都只要匹配高 64 位时（掩码长度小于等于 64），可以支持 ipv6 五元组的匹配。



S6000E 系列产品，作用于 SVI 上的安全 ACL 同时对于 VLAN 内的桥转发报文及 VLAN 间的路由报文生效，从而导致 VLAN 内用户无法通信等异常现象。



S6000E 系列产品，无法识别 IPv6 报文中的分片标识域。如果 IPv6 ACL 规则中带有 fragment 标识，匹配报文时规则中的 fragment 标识将被忽略，这种情况相当于 ACL 规则中不带有 fragment 标识，会去匹配所有报文，包括首片报文和非首片报文。







S6000E 系列产品，仅在 IP 扩展 ACL 和 Expert 扩展 ACL 上支持分片报文匹配模式的切换。



S6000E 系列产品，ACL80 只支持目的 MAC、源 MAC、VID、ETYPE、IP 协议号、ipv4 源 IP、IPV4 目的 IP、目的端口号，源端口号、ICMP TYPE、ICMP CODE 这几个常规字段。

## 1.5 配置详解

配置项	配置建议 & 相关命令	
配置 IP 访问列表功能	 可选配置。用于匹配过滤 IPv4 报文。	
	ip access-list standard	配置 IP 标准访问列表
	ip access-list extended	配置 IP 标准访问列表
	permit host any time-range log	配置 permit 类型的 IP 标准访问列表规则
	deny host any time-range log	配置 deny 类型的 IP 标准访问列表规则
	permit host any host any tos dscp precedence fragmenttime-range log	配置 permit 类型的 IP 扩展访问列表规则

	<b>deny host any host any tos dscp precedence fragmenttime-range log</b>	配置 deny 类型的 IP 扩展访问列表规则
	<b>ip access-group in out</b>	应用 IP 标准或 IP 扩展访问列表
配置 MAC 扩展访问列表	 可选配置。用于匹配过滤二层报文	
	<b>mac access-list extended</b>	配置 MAC 扩展访问列表
	<b>permit any host any host cos inner time-range</b>	配置 permit 类型的 MAC 扩展访问列表规则
	<b>deny any host any host cos inner time-range</b>	配置 deny 类型的 MAC 扩展访问列表规则
	<b>mac access-group in out</b>	应用 MAC 扩展访问列表
配置 Expert 扩展访问列表	 可选配置。用于匹配过滤二三层报文	
	<b>expert access-list extened</b>	配置 Expert 扩展访问列表
	<b>permit cos inner VID inner host any host any host any host any precedence tos fragment range time-range</b>	配置 permit 类型的 Expert 扩展访问列表规则
	<b>deny cos inner VID inner host any host any host any host any precedence tos fragment range time-range</b>	配置 deny 类型的 Expert 扩展访问列表规则
	<b>expert access-group in out</b>	应用 Expert 扩展访问列表
配置 IPv6 访问列表	 可选配置。用于匹配过滤 IPv6 报文	
	<b>ipv6 access-list</b>	配置 IPv6 访问列表
	<b>permit host any host any range dscp flow-label time-range</b>	配置 permit 类型的 IPv6 访问列表规则
	<b>deny host any host any range dscp flow-label time-range</b>	配置 deny 类型的 IPv6 访问列表规则
	<b>ipv6 traffic-filter in out</b>	应用 IPv6 扩展访问列表
配置 ACL80	 可选配置。用于自定义匹配域过滤二三层报文	
	<b>expert access-list advanced</b>	配置 Expert 高级访问列表
	<b>permit</b>	配置 permit 类型的 Expert 高级访问列表规则
	<b>deny</b>	配置 deny 类型的 Expert 高级访问列表规则
	<b>expert access-group in out</b>	应用 Expert 高级访问列表
配置 ACL 重定向	 可选配置。用于指定符合规则的报文重定向到指向的接口上	
	<b>redirect destination interface acl in</b>	配置 ACL 重定向
配置全局安全 ACL	 可选配置。用于让访问列表在全局上生效	
	<b>ip access-group in out</b>	在全局模式下配置全局安全 ACL 重定向



	<b>no global ip access-group</b>	在接口模式下将该接口配置为全局安全 ACL 的例外口。
配置安全通道	 可选配置。用于符合规则的报文直接跳过接入控制各种应用（比如 dot1x, web 认证）的检查。	
	<b>security access-group</b>	在接口模式下开启安全通道功能
	<b>security global access-group</b>	在配置模式下开启安全通道功能
	<b>security uplink enable</b>	在接口模式下将该接口配置成全局安全通道的例外口
配置访问列表注释信息	 可选配置。用于为访问列表或访问列表规则配置注释信息便于用户识别。	
	<b>list-remark</b>	在访问列表模式下为访问列表配置注释信息
	<b>access-list list-remark</b>	在全局模式为访问列表配置注释信息。
	<b>remark</b>	在访问列表模式下为规则配置注释信息

## 1.5.1 配置 IP 访问列表

### 配置效果

通过配置 IP 访问列表，并将访问列表应用到设备的接口上，就可以对在该接口进出的所有 IPv4 报文进行控制，禁止或允许特定的 IPv4 报文进入网络，从而实现控制 IP 用户访问网络资源的目的。

### 注意事项

无

### 配置方法

#### 配置 IP 访问列表

- 必须配置。要实际针对 IPv4 用户访问网络资源的控制，首先必须配置 IP 访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。IP 访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

#### 配置 IP 访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有 IPv4 报文进入设备。

#### 应用 IP 访问列表

- 必须配置。要使得 IP 访问列表真正生效，就必须将 IP 访问列表应用到设备的特定接口上。

- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IP 访问列表。

## 检验方法

可以通过以下方法检验 IP 访问列表的配置效果：

- 通过 ping 的方式检查 IP 访问列表是否真的在指定接口上生效。比如，IP 访问列表里配置了禁止某个 IP 主机或某个 IP 范围的主机不允许访问网络，通过 ping 的方式检验是否真的 ping 不通来验证。
- 通过访问网络相关资源的方式来检验 IP 访问列表是否真的在指定接口上生效，比如访问 internet 网，或通过 ftp 访问网络上的 ftp 资源等。

## 相关命令

### 配置 IP 访问列表

【命令格式】 **ip access-list { standard | extended } {acl-name | acl-id}**

【参数说明】 **standard**: 该选项若被配置，表示要创建一个标准 IP 访问列表。

**extended**: 该选项若被配置，表示要创建一个扩展 IP 访问列表。

**acl-name**: 该选项若被配置，表示创建一个命名的标准 IP 或扩展 IP 访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为 “in” 或 “out”。

**acl-id**: 为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的标准 IP 或扩展 IP 访问列表，如果创建的是标准 IP 访问列表，**acl-id** 的取值范围为 1-99，1300 – 1999，如果创建的是扩展 IP 访问列表，**acl-id** 的取值范围为 100-199，2000 – 2699。

【命令模式】 全局配置模式

【使用指导】 此命令可以用来配置标准 IP 或扩展 IP 访问列表，并进入标准 IP 或扩展 IP 访问列表配置模式。如果只想通过检查报文的源 IP 地址来控制用户的网络资源访问权限，那么可以配置标准 IP 访问列表；如果想通过检查报文的源 IP 地址、目的 IP 地址、报文的协议号、TCP/UDP 源或目的端口号来控制用户的网络资源访问权限，那么就需要配置扩展 IP 访问列表。

### 配置 IP 访问列表规则

- 为标准 IP 访问列表配置规则。

有两种方式可以为标准 IP 访问列表配置规则：

【命令格式】 **[ sn ] { permit | deny } { host source | any | source source-wildcard } [ time-range time-range-name ] [ log ]**

【参数说明】 **sn**: 为规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以由命令调整的。

**permit**: 该选项若被配置，表示本规则属于允许通过类的；

**deny**: 该选项若被配置，关键字表示本规则属于禁止通过类的；

**host source**: 该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；

**any:** 该选项若被配置，表示要匹配任意主机发出的 IP 报文；

**source source-wildcard:** 该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

**log:** 该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【命令模式】 标准 IP 访问列表模式

【使用指导】 此命令在标准 IP 访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

【命令格式】 **access-list acl-id { permit | deny } {host source | any | source source-wildcard } [ time-range tm-rng-name ] [ log ]**

【参数说明】 **acl-id:** 数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为： 1-99，1300 - 1999

**permit:** 该选项若被配置，表示本规则属于允许通过类的；

**deny:** 该选项若被配置，关键字表示本规则属于禁止通过类的；

**host source:** 该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；

**any:** 该选项若被配置，表示要匹配任意主机发出的 IP 报文；

**source source-wildcard:** 该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

**log:** 该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【命令模式】 标准 IP 访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 IP 访问列表配置规则。这种配置方式无法为命名的标准 IP 访问列表配置规则。

## ● 为扩展 IP 访问列表配置规则。

有两种方式可以为扩展 IP 访问列表配置规则：

【命令格式】 **[ sn ] { permit | deny } protocol{hostsource| any | sourcesource-wildcard } {hostdestination | any | destination destination-wildcard } [ [ precedenceprecedence [ tos tos ] ] | dscpdscp ] [fragment] [time-range time-range-name] [log]**

【参数说明】 **sn:** 规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的

**permit:** 该选项若被配置，表示本规则属于允许通过类的；

**deny:** 该选项若被配置，关键字表示本规则属于禁止通过类的；

**protocol:** IP 协议号，取值范围[0, 255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协

议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp。

**host source:** 该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；

**source source-wildcard:** 该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；

**host destination:** 该选项若被配置，表示要匹配目的 IP 为某一台特定主机的 IP 报文；**any** 关键字表示要匹配发往任意主机的 IP 报文。

**destination destination-wildcard:** 该选项若被配置，表示要匹配目标为某一个 IP 网段主机的报文。

**any:** 该选项若被配置，表示要匹配任意主机发出的 IP 报文或者要匹配发往任意主机的 IP 报文；

**precedence precedence:** 该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

**tos tos:** 该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。

**dscp dscp:** 该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。

**fragment:** 该选项若被配置，表示只要匹配非首片的 IP 分片报文。

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于时间区的描述，请参考 time range 的配置手册

**log:** 该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【命令模式】

扩展 IP 访问列表模式

【使用指导】

此命令在扩展 IP 访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

【命令格式】

**access-list acl-id { permit | deny } protocol[hostsource| any | sourcesource-wildcard] {hostdestination | any | destination destination-wildcard} [ [ precedenceprecedence [ tos tos ] ] | dscpdscp] [fragment] [time-rangetime-range-name] [log]**

【参数说明】

**acl-id:** 数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为：100-199，2000 - 2699

**sn:** 规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的

**permit:** 该选项若被配置，表示本规则属于允许通过类的；

**deny:** 该选项若被配置，关键字表示本规则属于禁止通过类的；

**protocol:** IP 协议号，取值范围[0, 255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp。

**host source:** 该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；

**source source-wildcard:** 该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；

**host destination:** 该选项若被配置，表示要匹配目的 IP 为某一台特定主机的 IP 报文；**any** 关键字表示要匹配发往任意主机的 IP 报文。

**destination destination-wildcard:** 该选项若被配置，表示要匹配目标为某一个 IP 网段主机的报文。

**any:** 该选项若被配置，表示要匹配任意主机发出的 IP 报文或者要匹配发往任意主机的 IP 报文；

**precedence precedence:** 该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

**tos tos:** 该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。

**dscp dscp:** 该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。

**fragment:** 该选项若被配置，表示只要匹配非首片的 IP 分片报文。

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于时间区的描述，请参考 time range 的配置手册

**log:** 该选项若被配置，表示本规则如果匹配到了报文需要定时输出匹配日志，有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【命令模式】 扩展 IP 访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 IP 访问列表配置规则。这种配置方式无法为命名的标准 IP 访问列表配置规则。

## 应用 IP 访问列表

【命令格式】 **ip access-group { acl-id | acl-name } { in | out }**

【参数说明】 **acl-id:** 该选项若被配置，表示要将一个数值索引的标准 IP 或扩展 IP 访问列表应用在接口上。

**acl-name:** 该选项若被配置，表示要将一个命名的标准 IP 或扩展 IP 访问列表应用在接口上。

**in:** 该选项若被配置，表示这个访问列表对进入该接口的 IP 报文进行控制。

**out:** 该选项若被配置，表示这个访问列表对从该接口发出的 IP 报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 IP 访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

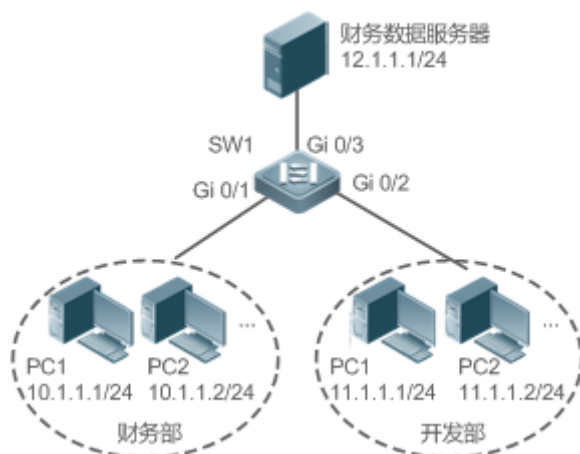
## 配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

### 通过 IP 访问列表，禁止财务部以外的部门访问财务数据服务器

【网络环境】

图 1-3



- 【配置方法】
- 配置 IP 访问列表
  - 在 IP 访问列表中添加访问规则

- 将 IP 访问列表应用在连接财务数据服务器接口的出方向上

**SW1**

```
sw1(config)#ip access-list standard 1
sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255
sw1(config-std-nacl)#exit
sw1(config)#int gigabitEthernet 0/3
sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
```

**【检验方法】**

- 从开发部的某台 PC 机上 ping 财务数据服务器，确认 ping 不通。
- 从财务部的某台 PC 机上 ping 财务数据服务器，确认 ping 得通

**SW1**

```
sw1(config)#show access-lists

ip access-list standard 1
 10 permit 10.1.1.0 0.0.0.255
 20 deny 11.1.1.0 0.0.0.255

sw1(config)#show access-group
ip access-group 1 out
Applied On interface GigabitEthernet 0/3
```

## 1.5.2 配置 MAC 扩展访问列表

### 配置效果

通过配置 MAC 扩展访问列表，并将访问列表应用到设备的接口上，就可以对在该接口上进出的所有二层报文进行控制，禁止或允许特定的二层报文进入网络，从而实现基于二层报文头来控制用户访问网络资源的目的。

### 注意事项

无

### 配置方法

#### 配置 MAC 扩展访问列表

- 必须配置。要基于二层报文头信息（比如用户 PC 的 MAC 地址）控制用户访问网络资源的权限，首先必须配置 MAC 扩展访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。MAC 扩展访问列表只在被配置的设备上有效，不会影响网络中的其他设备。

## 配置 MAC 扩展访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有以太网二层报文进入设备。

## 应用 MAC 扩展访问列表

- 必须配置。要使得 MAC 扩展访问列表真正生效，就必须将 MAC 扩展访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 MAC 扩展访问列表。

## 检验方法

可以通过以下方法检验 MAC 扩展访问列表的配置效果：

- 如果 MAC 扩展访问列表希望放过或过滤某些 IP 报文，可以通过 ping 的方式检查这样的 MAC 扩展访问列表规则是否真的在指定接口上生效。比如，MAC 扩展访问列表里配置了禁止以太网类型为 0x0800 即 IP 报文从接口进入设备，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 如果 MAC 扩展访问列表希望放过或过滤某些非 IP 报文，比如 ARP 报文，这种报文也可以通过 ping 的方式检查这样的 MAC 扩展访问列表规则是否真的在指定接口上生效，比如想过滤掉 ARP 报文，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 另外，还可以通过构造符合指定特征的二层报文来检验 MAC 扩展访问列表是否真的生效。典型地可以使用两台 PC 机，一台构造二层报文并发送，另一台开启抓包软件抓包，根据访问列表规则指定的动作检查报文的转发是否如预期（转发或不转发）。

## 相关命令

### 配置 MAC 扩展访问列表

【命令格式】 **mac access-list extended** {acl-name | acl-id }

【参数说明】 **acl-name**: 该选项若被配置，表示创建一个命名的 MAC 扩展访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为 “in” 或 “out”。

**acl-id**: 为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的 MAC 扩展访问列表，取值范围为 700-799。

【命令模式】 全局配置模式

【使用指导】 此命令可以用来配置 MAC 扩展访问列表，并进入 MAC 扩展访问列表配置模式。如果想通过检查以太网报文的二层信息来控制用户的网络资源访问权限，那么就可以配置 MAC 扩展访问列表。

### 配置 MAC 扩展访问列表规则

有两种方法为 MAC 扩展访问列表配置规则：

- 在 MAC 扩展访问列表模式中配置规则

【命令格式】 [sn] { **permit** | **deny** } {**any** | **host** src-mac-addr | src-mac-addr mask} {**any** | **host** dst-mac-addr | dst-mac-addr mask} [ethernet-type] [cos cos [inner cos]] [time-range tm-mng-name]

【参数说明】 **sn**: 为规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先

级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的。

**permit:** 该选项若被配置，表示本规则属于允许通过类的；

**deny:** 该选项若被配置，关键字表示本规则属于禁止通过类的；

**any:** 该选项若被配置，表示要匹配任意主机发出的二层报文；

**host src-mac-addr:** 该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；

**src-mac-addr mask:** 该选项若被配置，表示对源 MAC 进行取反；

**any:** 该选项若被配置，表示要匹配目的为任意主机发出的二层报文；

**host dst-mac-addr:** 该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；

**dst-mac-addr mask:** 该选项若被配置，表示对目的 MAC 进行取反；

**ethernet-type:** 该选项若被配置，表示要匹配指定以太网类型的二层报文；

**cos cos:** 该选项若被配置，表示要匹配二层报文里的外层 TAG 的优先级字段；

**inner cos:** 该选项若被配置，表示要匹配二层报文里的内层 TAG 的优先级字段；

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 MAC 扩展访问列表模式

【使用指导】 此命令在 MAC 扩展访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

#### ● 在全局模式中为 MAC 扩展访问列表配置规则

【命令格式】 **access-list acl-id { permit | deny } {any | host src-mac-addr | src-mac-addr mask } {any | host dst-mac-addr | dst-mac-addr mask } [ethernet-type] [cos cos [inner cos]] [ time-range tm-rng-name ]**

【参数说明】 **acl-id:** 数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为：700-799

**permit:** 该选项若被配置，表示本规则属于允许通过类的；

**deny:** 该选项若被配置，关键字表示本规则属于禁止通过类的；

**host src-mac-addr:** 该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；

**src-mac-addr mask:** 该选项若被配置，表示对源 MAC 进行取反；

**any:** 该选项若被配置，表示要匹配目的为任意主机发出的二层报文；

**host dst-mac-addr:** 该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；

**dst-mac-addr mask:** 该选项若被配置，表示对目的 MAC 进行取反；

**ethernet-type:** 该选项若被配置，表示要匹配指定以太网类型的二层报文；

**cos cos:** 该选项若被配置，表示要匹配二层报文里的外层优先级字段；

**inner cos:** 该选项若被配置，表示要匹配二层报文里的内层优先级字段；

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册。

【命令模式】 全局模式

【使用指导】 此命令在配置模式下为数字索引的 MAC 扩展访问列表配置规则。这种配置方式无法为命名的 MAC 扩展访问列表配置规则。



## 应用 MAC 扩展访问列表

【命令格式】 **mac access-group** { *acl-id* | *acl-name* } { *in* | *out* }

【参数说明】 *acl-id*: 该选项若被配置, 表示要将一个数值索引的 MAC 扩展访问列表应用在接口上。

*acl-name*: 该选项若被配置, 表示要将一个命名的 MAC 扩展访问列表应用在接口上。

*in*: 该选项若被配置, 表示这个访问列表对进入该接口的二层报文进行控制。

*out*: 该选项若被配置, 表示这个访问列表对从该接口发出的二层报文进行控制。

【命令模式】  
接口模式

【使用指导】 此命令可以让 MAC 扩展访问列表在指定的接口上生效, 同时需要指定对进入设备的报文生效, 还是从设备转发出去的报文生效。

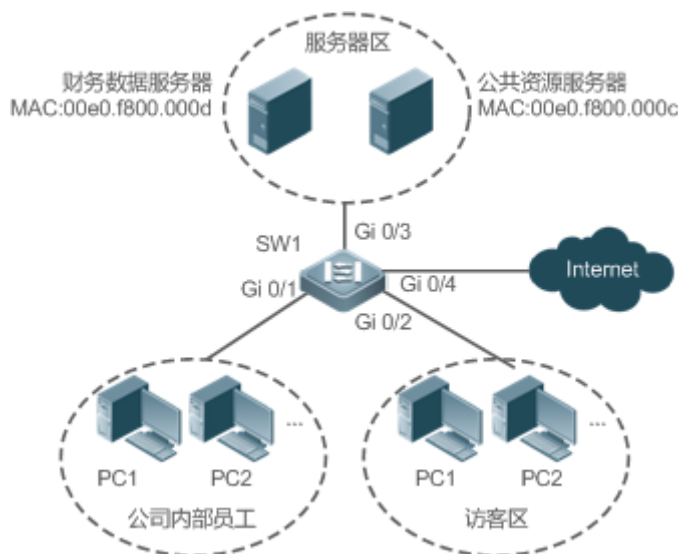
## 配置举例

以下配置举例, 仅介绍与 ACL 相关的配置。

### 通过 MAC 扩展访问列表, 限制来访客户可访问的资源

【网络环境】

图 1-4



- 【配置方法】
- 配置 MAC 扩展访问列表
  - 在 MAC 扩展访问列表中添加访问规则
  - 将 MAC 扩展访问列表应用在连接访客区接口的出方向上, 允许访客 PC 访问 Internet 以及公司内部的公共资源服务器, 但不允许访问公司的账务数据服务器, 即禁止访问 MAC 地址为 00e0.f800.000d 的服务器。

SW1

```
sw1(config)#mac access-list extended 700
sw1(config-mac-nacl)#deny any host 00e0.f800.000d
sw1(config-mac-nacl)#permit any any
sw1(config-mac-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in
```

- 【检验方法】
- 从访客 PC 机上 ping 财务数据服务器，确认 ping 不通。
  - 从访问 PC 机上 ping 公共资源服务器，确认可以 ping 得通。
  - 在访问 PC 机上访问 Internet，比如访问百度，确认可以打开主页。

**SW1**

```
sw1(config)#show access-lists
mac access-list extended 700
 10 deny any host 00e0.f800.000d etype-any
 20 permit any any etype-any
sw1(config)#show access-group
mac access-group 700 in
Applied On interface GigabitEthernet 0/2
```

### 1.5.3 配置 Expert 扩展访问列表

#### 配置效果

通过配置 Expert 扩展访问列表，并将访问列表应用到设备的接口上，可以同时基于二层和三层信息对在该接口上进出的报文进行控制，禁止或允许特定的报文进入网络；另外，还可以通过配置 Expert 扩展访问列表实现基于 VLAN 来对所有二层报文进行控制，从而实现允许或拒绝某些网段的用户访问网络资源。一般来说，如果想在一条访问列表中混合使用 IP 访问规则以及 MAC 扩展访问规则时，就可以使用 Expert 扩展访问列表

#### 注意事项

无

#### 配置方法

##### 配置 Expert 扩展访问列表

- 必须配置。要基于二层报文头信息（比如 VLAN ID）控制用户访问网络资源的权限，首先必须配置 Expert 扩展访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。Expert 扩展访问列表只在被配置的设备上有效，不会影响网络中的其他设备。

##### 配置 Expert 扩展访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有报文进入设备。

##### 应用 Expert 扩展访问列表

- 必须配置。要使得 Expert 扩展访问列表真正生效，就必须将访问列表应用到设备的特定接口上。

- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口的入或出方向上应用 Expert 扩展访问列表。

## 检验方法

可以通过以下方法检验 Expert 扩展访问列表的配置效果：

- 如果 Expert 扩展访问列表中配置了 IP 访问规则，放过或过滤某些 IP 报文，通过 ping 的方式来检验规则是否生效。
- 如果 Expert 扩展访问列表中配置了 MAC 访问规则，放过或过滤某些二层报文，比如 ARP 报文，这种报文也可以通过 ping 的方式检查这样的 MAC 访问列表规则是否真的在指定接口上生效，比如想过滤掉 ARP 报文，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 如果 Expert 扩展访问列表中配置了带有 VLAN ID 的访问规则，希望放过或过滤某些二层网段的报文，典型假设不想让 VLAN 1 的用户与 VLAN 2 的用户互访问，可以在 VLAN 1 所在的 PC 机上 ping VLAN 2 的 PC 机，如果 ping 不通就表示规则生效。

## 相关命令

### 配置 Expert 扩展访问列表

【命令格式】 **expert access-list extended** {acl-name | acl-id }

【参数说明】 **acl-name**: 该选项若被配置，表示创建一个命名的 Expert 扩展访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为 “in” 或 “out”。

**acl-id**: 为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的 Expert 扩展访问列表，取值范围为 2700-2899。

【命令模式】 全局配置模式

【使用指导】 此命令可以用来配置 MAC 扩展访问列表，并进入 Expert 扩展访问列表配置模式。

### 配置 Expert 扩展访问列表规则

有两种方法为 Expert 扩展访问列表配置规则：

- 在 Expert 扩展访问列表模式中配置规则

【命令格式】 [sn] { **permit** | **deny** } [ protocol ] [ ethernet-type ] [ **cos** [ out ] [ inner in ] ] [ **VID** [ out ] [ inner in ] ] [ **source** source-wildcard | **host** source | **any** ] { **host** source-mac-address | **any** } { **destination** destination-wildcard | **host** destination | **any** } { **host** destination-mac-address | **any** } [ **precedence** precedence ] [ **tos** tos ] [ **fragment** ] [ **range** lower upper ] [ **time-range** time-range-name ]

【参数说明】 **sn**: 为规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以由命令调整的。

**permit**: 该选项若被配置，表示本规则属于允许通过类的；

**deny**: 该选项若被配置，关键字表示本规则属于禁止通过类的；

**protocol:** IP 协议号,取值范围[0, 255];为方便使用,系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值,包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp

**ethernet-type:** 该选项若被配置,表示要匹配指定以太网类型的二层报文;

**cos out:** 该选项若被配置,表示要匹配指定二层报文外层 TAG 中的优先级字段;

**cos inner in:** 该选项若被配置,表示要匹配指定二层报文内层 TAG 中的优先级字段;

**VID out:** 该选项若被配置,表示要匹配指定二层报文外层 TAG 中的 VLAN ID 字段;

**VID inner in:** 该选项若被配置,表示要匹配指定二层报文内层 TAG 中的 VLAN ID 字段;

**source source-wildcard:** 该选项若被配置,表示要匹配某一个 IP 网段的内主机发出的报文;

**host source:** 该选项若被配置,表示要匹配源 IP 为某一台主机发出的 IP 报文;

**any:** 该选项若被配置,表示要匹配任意主机发出的 IP 报文;

**host source-mac-address:** 该选项若被配置,表示要匹配源 MAC 为某一台主机发出的二层报文;

**any:** 该选项若被配置,表示要匹配目的为任意主机发出的二层报文;

**destination destination-wildcard:** 该选项若被配置,表示要匹配目标为某一个 IP 网段的报文;

**host destination:** 该选项若被配置,表示要匹配目的 IP 为某一台主机的 IP 报文;

**any:** 该选项若被配置,表示要匹配发往任意目标的 IP 报文;

**host destination-mac-address:** 该选项若被配置,表示要匹配目的 MAC 为某一台主机的二层报文;

**any:** 该选项若被配置,表示要匹配目标为任意主机的二层报文;

**precedence precedence:** 该选项若被配置,表示要匹配 IP 报文头部中的优先级域。

**tos tos:** 该选项若被配置,表示要匹配 IP 报文头部中的服务类型域。

**dscp dscp:** 该选项若被配置,表示要匹配 IP 报文头部的 dscp 域。

**fragment:** 该选项若被配置,表示只要匹配非首片的 IP 分片报文。

**time-range time-range-name:** 该选项若被配置,表示该匹配规则关联了一个时间区,只有在指定的时间区间内该规则才会生效,否则不生效,更多关于时间区的描述,请参考 time range 的配置手册

【命令模式】 Expert 扩展访问列表模式

【使用指导】 此命令在 Expert 扩展访问列表模式下为访问列表配置规则,该访问列表可以是命名访问列表,也可以是数字索引的访问列表。

- 在全局模式下为 Expert 扩展访问列表配置规则

【命令格式】 **access-list acl-id { permit | deny } [ protocol ] [ ethernet-type ] [ cos [ out ] [ inner in ] ] [ [ VID [ out ] [ inner in ] ] ] { source source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [ precedence precedence ] [ tos tos ] [ fragment ] [ range lower upper ] [ time-range time-range-name ]**

【参数说明】 **acl-id:** 数值索引访问列表的编号,以此来唯一标识一条访问列表。取值范围: 2700-2899

**permit:** 该选项若被配置,表示本规则属于允许通过类的;

**deny:** 该选项若被配置,关键字表示本规则属于禁止通过类的;

**protocol:** IP 协议号,取值范围[0, 255];为方便使用,系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值,包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp

**ethernet-type:** 该选项若被配置,表示要匹配指定以太网类型的二层报文;

**cos out:** 该选项若被配置,表示要匹配指定二层报文外层 TAG 中的优先级字段;

**cos inner in:** 该选项若被配置,表示要匹配指定二层报文内层 TAG 中的优先级字段;

**VID out:** 该选项若被配置,表示要匹配指定二层报文外层 TAG 中的 VLAN ID 字段;

**VID inner in:** 该选项若被配置,表示要匹配指定二层报文内层 TAG 中的 VLAN ID 字段;

**source source-wildcard:** 该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；

**host source:** 该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；

**any:** 该选项若被配置，表示要匹配任意主机发出的 IP 报文；

**host source-mac-address:** 该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；

**any:** 该选项若被配置，表示要匹配目的为任意主机发出的二层报文；

**destination destination-wildcard:** 该选项若被配置，表示要匹配目标为某一个 IP 网段的报文；

**host destination:** 该选项若被配置，表示要匹配目的 IP 为某一台主机的 IP 报文；

**any:** 该选项若被配置，表示要匹配发往任意目标的 IP 报文；

**host destination-mac-address:** 该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；

**any:** 该选项若被配置，表示要匹配目标为任意主机的二层报文；

**precedence precedence:** 该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

**tos tos:** 该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。

**dscp dscp:** 该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。

**fragment:** 该选项若被配置，表示只要匹配非首片的 IP 分片报文。

**time-range time-range-name:** 该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于时间区的描述，请参考 time range 的配置手册。

【命令模式】 Expert 扩展访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 Expert 扩展访问列表配置规则。这种配置方式无法为命名的 Expert 扩展访问列表配置规则。

## 应用 Expert 扩展访问列表

【命令格式】 **expert access-group { acl-id | acl-name } { in | out }**

【参数说明】 **acl-id:** 该选项若被配置，表示要将一个数值索引的 Expert 扩展访问列表应用在接口上。

**acl-name:** 该选项若被配置，表示要将一个命名的 Expert 扩展访问列表应用在接口上。


**in:** 该选项若被配置，表示这个访问列表对进入该接口的二层报文进行控制。

**out:** 该选项若被配置，表示这个访问列表对从该接口发出的二层报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 Expert 扩展访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

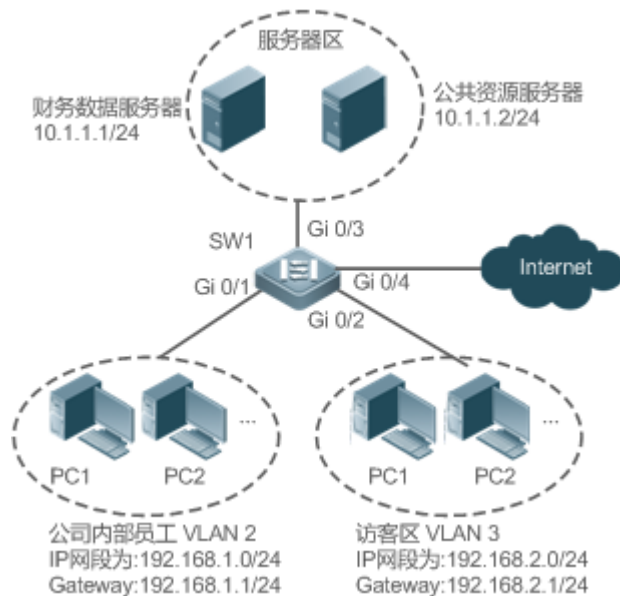
## 配置举例

 以下配置举例，仅介绍与 ACL 相关的配置。

通过 Expert 扩展访问列表，限制来访客区用户可访问的资源，要求访客不能与公司内部员工互访，但能访问公共资源服务器，且不能访问公司核心的账务数据服务器。

## 【网络环境】

图 1-5



## 【配置方法】

- 配置 Expert 扩展访问列表
- 在访问列表中添加规则,禁止访客区 VLAN 3 网段内主机发出目标为内部员工 VLAN2 网段的报文进入网络。
- 在访问列表中添加规则,禁止访客访问核心账务数据服务器规则,
- 再添加一条规则,允许所有报文通过;
- 最后再将访问列表应用在与访客区相连交换机接口的入方向上。

## SW1

```
sw1(config)#expert access-list extended 2700
sw1(config-exp-nacl)#deny ip any any 192.168.1.0 0.0.0.255 any
sw1(config-exp-nacl)#deny ip any any host 10.1.1.1 any
sw1(config-exp-nacl)#permit any any any any
sw1(config-exp-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
```

## 【检验方法】

- 从访客 PC 机上 ping 财务数据服务器,确认 ping 不通。
- 从访客 PC 机上 ping 公共资源服务器,确认可以 ping 得通。
- 从访客 PC 机上 ping 公司内部员工网关 192.168.1.1,确定 ping 不通。
- 在访问 PC 机上访问 Internet,比如访问百度,确认可以打开主页。

## SW1

```
sw1(config)#show access-lists
expert access-list extended 2700
 10 deny ip any any 192.168.1.0 0.0.0.255 any
 20 deny ip any any host 10.1.1.1 any
 30 permit ip any any any any

sw1(config)#show access-group
```

```
expert access-group 2700 in
Applied On interface GigabitEthernet 0/2
```

## 1.5.4 配置 IPv6 扩展访问列表

### 配置效果

通过配置 IPv6 访问列表，并将访问列表应用到设备的接口上，就可以在该接口上进出的所有 IPv6 报文进行控制，禁止或允许特定的 IPv6 报文进入网络，从而实现控制 IPv6 用户访问网络资源的目的。

### 注意事项

无

### 配置方法

#### 配置 IPv6 访问列表

- 必须配置。要实际针对 IPv6 用户访问网络资源的控制，首先必须配置 IPv6 访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。IPv6 访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

#### 配置 IPv6 访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有 IPv6 报文进入设备。

#### 应用 IPv6 访问列表

- 必须配置。要使得 IPv6 访问列表真正生效，就必须将 IPv6 访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IPv6 访问列表。

### 检验方法

可以通过以下方法检验 IPv6 访问列表的配置效果：

- 通过 ping 的方式检查 IPv6 访问列表是否真的在指定接口上生效。比如，IPv6 访问列表里配置了禁止某个 IPv6 主机或某个 IPv6 地址范围内的主机不允许访问网络，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 通过访问网络相关资源的方式来检验 IPv6 访问列表是否真的在指定接口上生效，比如访问 IPv6 网站等。

## 相关命令

### 配置 IPv6 访问列表

- 【命令格式】 **ipv6 access-list *acl-name***
- 【参数说明】 *acl-name*: 该选项若被配置, 表示创建一个命名的标准 IP 或扩展 IP 访问列表, 长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头, 也不能为 “in” 或 “out”。
- 【命令模式】 配置模式
- 【使用指导】 此命令可以用来配置 IPv6 访问列表, 并进入 IPv6 访问列表配置模式。

### 配置 IPv6 访问列表规则

- 当要匹配 TCP 或 UDP 报文时。可以使用如下方式为 IPv6 访问列表配置规则：

【命令格式】 **[sn]{permit | deny }protocol{src-ipv6-prefix/prefix-len|hostsrc-ipv6-addr|any}{dst-ipv6-pfix/pfix-len|hostdst-ipv6-addr|any} [op dstport | range lower upper ] [dscp dscp][flow-label flow-label][fragment] [time-range tm-rng-name][log]**

【参数说明】 *sn*: 为规则表项的序号, 取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级, 序号越小, 优先级越大, 优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号, 系统会自动分配一个序号, 序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值, 递增值默认为 10, 假设当前访问列表最后一条匹配规则的序号为 100, 则缺省情况下新增的这条匹配规则序号就为 11, 此外, 递增值是可以通过命令调整的。

**permit**: 该选项若被配置, 表示本规则属于允许通过类的;

**deny**: 该选项若被配置, 关键字表示本规则属于禁止通过类的;

**protocol**: IPv6 协议号, 取值范围[0, 255]; 为方便使用, 系统提供了常用 IPv6 协议号的简称以取代对应的协议号具体数值, 包括 **icmp**、**ipv6**、**tcp**、**udp**。

**src-ipv6-prefix/prefix-len**: 该选项若被配置, 表示要匹配某一个 IPv6 网段的内主机发出的报文;

**host src-ipv6-addr**: 该选项若被配置, 表示要匹配源 IP 为某一台主机发出的 IPv6 报文;

**any**: 该选项若被配置, 表示要匹配任意主机发出的 IPv6 报文;

**dst-ipv6-pfix/pfix-len**: 该选项若被配置, 表示要匹配目标 IP 是某一个 IPv6 网段的内主机的 IPv6 报文;

**host dst-ipv6-addr**: 该选项若被配置, 表示要匹配目标 IP 为某一台主机的 IPv6 报文;

**any**: 该选项若被配置, 表示要匹配发往任意主机的 IPv6 报文;

**op dstport**: 该选项若被配置, 表示要匹配 TCP 或 UDP 报文中的四层目的端口号, 其中 **op** 参数可以是 **eq**、**neq**、**gt**、**lt**, 分别对应等于、不等于、大于、小于这四个不同的操作;

**range lower upper**: 该选项若被配置, 表示要匹配 TCP 或 UDP 报文中某个范围内的四层目的端口号;

**dscp dscp**: 该选项若被配置, 表示要匹配 IPv6 报文头部的 dscp 域;

**flow-label flow-label**: 该选项若被配置, 表示要匹配 IPv6 报文头部的流标签域;

**fragment**: 该选项若被配置, 表示只要匹配非首片的 IPv6 分片报文;

**time-range time-range-name**: 该选项若被配置, 表示该匹配规则关联了一个时间区, 只有在指定的时间区间内该规则才会生效, 否则不生效, 更多关于关时间区的描述, 请参考 **time range** 的配置手册

**log**: 该选项若被配置, 表示本规则如果匹配到了报文需要定时输出匹配日志, 有关匹配日志更详细描述请参考



考本手册的 ACL logging 一节。

【命令模式】 IPv6 访问列表模式

【使用指导】 此命令在 IPv6 访问列表模式下为访问列表配置规则。

- 当要匹配 TCP 或 UDP 以外的 IPv6 报文时。可以使用如下方式为标准 IPv6 访问列表配置规则：

【命令格式】 `[sn]{permit | deny }protocol{src-ipv6-prefix/prefix-len|hostsrc-ipv6-addr|any}{dst-ipv6-pfix/pfix-len|hostdst-ipv6-addr|any} [dscpdscp][flow-labelflow-label ][fragment ] [time-range tm-rng-name] [ log ]`

【参数说明】 **sn**: 为规则表项的序号, 取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级, 序号越小, 优先级越大, 优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号, 系统会自动分配一个序号, 序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值, 递增值默认为 10, 假设当前访问列表最后一条匹配规则的序号为 100, 则缺省情况下新增的这条匹配规则序号就为 11, 此外, 递增值是可以通过命令调整的。

**permit**: 该选项若被配置, 表示本规则属于允许通过类的;

**deny**: 该选项若被配置, 关键字表示本规则属于禁止通过类的;

**protocol**: IPv6 协议号, 取值范围[0, 255]; 为方便使用, 系统提供了常用 IPv6 协议号的简称以取代对应的协议号具体数值, 包括 **icmp**、**ipv6**、**tcp**、**udp**。

**src-ipv6-prefix/prefix-len**: 该选项若被配置, 表示要匹配某一个 IPv6 网段的内主机发出的报文;

**host src-ipv6-addr**: 该选项若被配置, 表示要匹配源 IP 为某一台主机发出的 IPv6 报文;

**any**: 该选项若被配置, 表示要匹配任意主机发出的 IPv6 报文;

**dst-ipv6-pfix/pfix-len**: 该选项若被配置, 表示要匹配目标 IP 是某一个 IPv6 网段的内主机的 IPv6 报文;

**host dst-ipv6-addr**: 该选项若被配置, 表示要匹配目标 IP 为某一台主机的 IPv6 报文;

**any**: 该选项若被配置, 表示要匹配发往任意主机的 IPv6 报文;

**dscp dscp**: 该选项若被配置, 表示要匹配 IPv6 报文头部的 dscp 域;

**flow-label flow-label**: 该选项若被配置, 表示要匹配 IPv6 报文头部的流标签域;

**fragment**: 该选项若被配置, 表示只要匹配非首片的 IPv6 分片报文;

**time-range time-range-name**: 该选项若被配置, 表示该匹配规则关联了一个时间区, 只有在指定的时间区间内该规则才会生效, 否则不生效, 更多关于关时间区的描述, 请参考 time range 的配置手册

**log**: 该选项若被配置, 表示本规则如果匹配到了报文需要定时输出匹配日志, 有关匹配日志更详细描述请参考本手册的 ACL logging 一节。

【命令模式】 IPv6 访问列表模式

【使用指导】 此命令在 IPv6 访问列表模式下为访问列表配置规则。

## 应用 IPv6 访问列表

【命令格式】 `ipv6 traffic-filter acl-name { in | out }`

【参数说明】 **acl-name**: IPv6 访问列表的名称。

**in**: 该选项若被配置, 表示这个访问列表对进入该接口的 IPv6 报文进行控制。

**out**: 该选项若被配置, 表示这个访问列表对从该接口发出的 IPv6 报文进行控制。

【命令模式】 接口模式

- 【使用指导】 此命令可以让 IPv6 访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

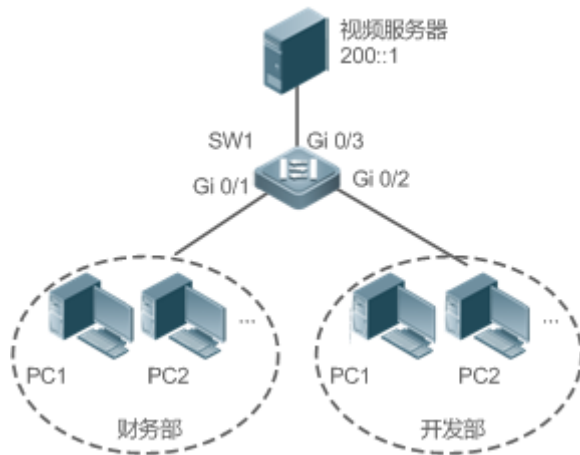
## 配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

### 通过 IPv6 访问列表，禁止开发部门访问视频服务器

【网络环境】

图 1-6



【配置方法】

- 配置 IP6 访问列表
- 在 IPv6 访问列表中添加禁止访问视频服务器 IPv6 地址规则
- 在 IPv6 访问列表中添加允许所有 IPv6 报文通过规则
- 将 IPv6 访问列表应用在开发部门所在接口的入方向上

SW1

```
sw1(config)#ipv6 access-list dev_deny_ipv6video
sw1(config-ipv6-nacl)#deny ipv6 any host 200::1
sw1(config-ipv6-nacl)#permit ipv6 any any
sw1(config-ipv6-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in
```

【检验方法】

- 从开发部的某台 PC 机上 ping 视频服务器，确认 ping 不通。

SW1

```
sw1(config)#show access-lists

ipv6 access-list dev_deny_ipv6video
 10 deny ipv6 any host 200::1
 20 permit ipv6 any any

sw1(config)#show access-group
ipv6 traffic-filter dev_deny_ipv6video in
Applied On interface GigabitEthernet 0/2
```

## 1.5.5 配置 ACL80

### 配置效果

---

当固定匹配域的 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表都无法满足要求时，那么可以通过配置 ACL80，由用户自己定义自己想匹配的报文域，从而实现自定义匹配域的目的。

### 注意事项

无

### 配置方法

---

#### 📌 配置 Expert 高级访问列表

- 必须配置。要实现 ACL80 的功能，首先就是要配置 Expert 高级访问列表，Expert 高级访问列表配置请参考相关章节的说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。Expert 高级访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

#### 📌 配置 Expert 高级访问列表规则

- 必须配置。要实现自定义匹配域，必须配置自定义的访问列表规则。如果不配置访问列表规则，则默认的 deny 所有表项将会将所有报文丢弃。Expert 访问列表规则配置请参考相关章节的说明

#### 📌 应用 Expert 高级访问列表

- 必须配置。要使得 Expert 高级访问列表真正生效，就必须将 Expert 高级访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 Expert 高级访问列表。

### 检验方法

---

可以通过以下方法检验 Expert 高级访问列表的配置效果：

- 通过 ping 的方式来验证配置是否生效。
- 通过构造符合访问列表规则的报文来验证规则是否生效。

### 相关命令

---

#### 📌 配置 Expert 高级访问列表

【命令格式】 **expert access-list advanced** *acl-name*

【参数说明】 *acl-name*: Expert 高级访问列表的名称，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为“in”或“out”。

【命令模式】 配置模式

【使用指导】 此命令可以用来配置 MAC 扩展访问列表，并进入 Expert 扩展访问列表配置模式。

## 配置 Expert 高级访问列表规则

【命令格式】 [*sn*] { **permit** | **deny** } *hex hex-mask offset*

【参数说明】 *sn*: 为规则表项的序号，取值范围为[1, 2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的。

**permit**: 该选项若被配置，表示本规则属于允许通过类的；

**deny**: 该选项若被配置，关键字表示本规则属于禁止通过类的；

*hex*: 以 16 进制表示的自定义匹配内容。比如 00d0f800。

*hex-mask*: 匹配掩码；

*offset*: 匹配开始的位置，比如匹配内容为 00d0f800，匹配掩码为 00ff0000，开始位置为 6，表示要匹配报文中的目的 MAC 地址，所有目的 MAC 地址中的第二字节为 d0 的报文都能匹配到这条规则；

【命令模式】 Expert 高级访问列表模式

【使用指导】 此命令在 Expert 高级访问列表模式下为访问列表配置自定义规则。

## 应用 Expert 高级访问列表

【命令格式】 **expert access-group** { *acl-id* | *acl-name* } { **in** | **out** }

【参数说明】 *acl-id*: 该选项若被配置，表示要将一个数值索引的 Expert 扩展访问列表应用在接口上。

*acl-name*: 该选项若被配置，表示要将一个命名的 Expert 扩展访问列表应用在接口上。


**in**: 该选项若被配置，表示这个访问列表对进入该接口的二层报文进行控制。

**out**: 该选项若被配置，表示这个访问列表对从该接口发出的二层报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 Expert 扩展访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

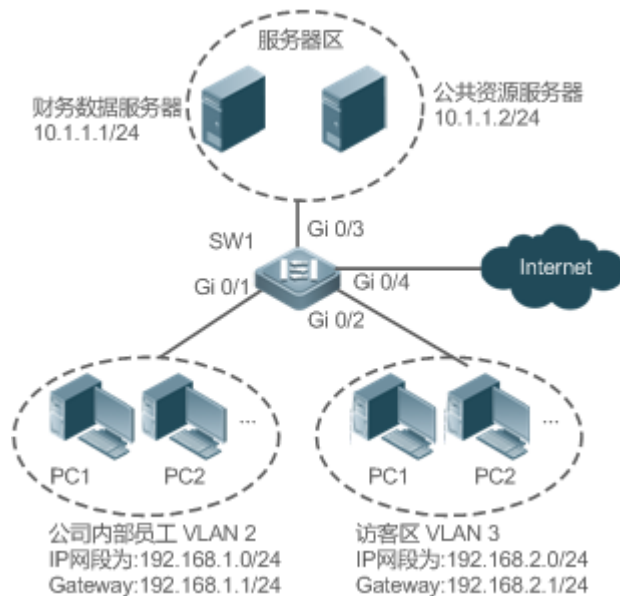
## 配置举例

 以下配置举例，仅介绍与 ACL 相关的配置。

## 通过 ACL80 即 Expert 高级访问列表，限制来访客区户可访问的资源，要求访客不能与公司内部员工互访，但能访问公共资源服务器，且不能访问公司核心的账务数据服务器。

## 【网络环境】

图 1-7



## 【配置方法】

- 配置 Expert 高级访问列表
- 在访问列表中添加规则,禁止访客区 VLAN 3 网段内主机发出目标为内部员工 VLAN2 网段的报文进入网络。
- 在访问列表中添加规则,禁止访客访问核心账务数据服务器规则,
- 再添加一条规则,允许所有报文通过;
- 最后再将访问列表应用在与访客区相连交换机接口的入方向上。

## SW1

```
sw1(config)#expert access-list advanced acl80-guest
sw1(config-exp-dacl)#deny C0A801 FFFFFFFF 42
sw1(config-exp-dacl)#deny 0A010101 FFFFFFFF 42
sw1(config-exp-dacl)#permit 0806 FFFF 24
sw1(config-exp-dacl)#permit 0800 FFFF 24
sw1(config-exp-dacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)#expert access-group acl80-guest in
```

## 【检验方法】

- 从访客 PC 机上 ping 财务数据服务器,确认 ping 不通。
- 从访客 PC 机上 ping 公共资源服务器,确认可以 ping 得通。
- 从访客 PC 机上 ping 公司内部员工网关 192.168.1.1,确定 ping 不通。
- 在访问 PC 机上访问 Internet,比如访问百度,确认可以打开主页。

## SW1

```
sw1(config)#show access-lists
expert access-list advanced sss
10 deny C0A801 FFFFFFFF 42
20 deny 0A010101 FFFFFFFF 42
30 permit 0806 FFFF 24
40 permit 0800 FFFF 24
```

```
expert access-group acl80-guest in
Applied On interface GigabitEthernet 0/2
```

## 1.5.6 配置 ACL 重定向

### 配置效果

---

通过在指定接口上配置 ACL 重定向功能，可以对进入在该接口的指定报文直接重定向指定端口转发出去。

### 注意事项

无

### 配置方法

---

#### 📌 配置访问列表

- 必须配置。要实现 ACL 重定向，首先就是要配置访问列表，比如 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表等，访问列表配置请参考相关章节的说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。IPv6 访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

#### 📌 配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于 ACL 重定向功能不存在。访问列表规则配置请参考相关章节的说明

#### 📌 配置 ACL 重定向

- 必须配置。要使得 ACL 重定向起作用，就必须在指定接口上开启重定向功能。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上配置 ACL 重定向功能。

### 检验方法

---

可以通过在配置 ACL 重定向所在的端口上发送符合规则的报文，然后在目标端口上使用抓包软件验证 ACL 重定向功能是否生效。

### 相关命令

---

#### 📌 配置访问列表

访问列表的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

#### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

#### 配置 ACL 重定向

【命令格式】 **redirect destination interface** *interface-name* **acl** {*acl-id* | *acl-name*} **in**

【参数说明】 **interface** *interface-name*: 重定向目标端口名称。

*acl-id*: 访问列表的编号。

*acl-name*: 访问列表的名称。

**in**: 对进入接口的报文进行重定向。

【命令模式】 接口模式

【使用指导】 通过该命令，从指定接口进来的报文如果符合 ACL 规则就会被重定向到目标端口转发出去。

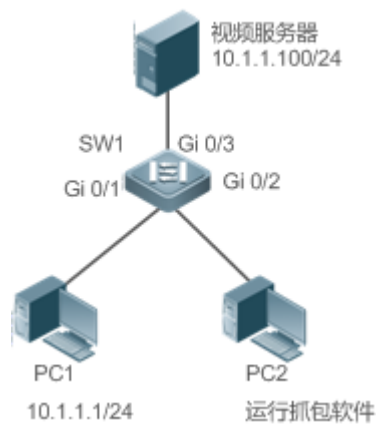
### 配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

#### 通过 ACL 重定向功能，主机 10.1.1.1 发出的报文重定向到抓包设备上进行分析

【网络环境】

图 1-8



- 【配置方法】
- 配置 IP 访问列表
  - 在 IP 访问列表中添加允许主机 10.1.1.1 地址规则
  - 在 Gi 0/1 接入上配置 ACL 重定向，目标端口为 Gi 0/2

SW1

```
sw1(config)#ip access-list standard 1
sw1 (config-std-nacl)#permit host 10.1.1.1
sw1(config-std-nacl)#exit
sw1(config)#int gigabitEthernet 0/1
sw1(config-if-GigabitEthernet 0/1)# redirect destination interface gigabitEthernet 0/2 acl 1
```

- 【检验方法】 ● 在 PC2 上开启抓包，从 PC1 ping 视频服务器，在 PC2 上确认有抓到 PC1 发出的 ICMP 请求报文。

**SW1**

```
sw1#show access-lists
ip access-list standard 1
  10 permit host 10.1.1.1
sw1#show redirect interface gigabitEthernet 0/1
acl redirect configuration on interface gigabitEthernet 0/1
redirect destination interface gigabitEthernet 0/2 acl 1 in
```

## 1.5.7 配置全局安全 ACL

### 配置效果

通过配置全局安全 ACL 功能，可以起到阻止企业内部访问非法网站，或者阻止病毒进入企业内部网络的目的。另外，通过配置全局安全 ACL 例外口，允许企业内部某些特殊部门可以访问外部一些站点。

### 注意事项

无

### 配置方法

#### 配置访问列表

- 必须配置。要实现全局防护内部网络的目的，首先要配置访问列表，相关的配置方法请参考各访问列表章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

#### 配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于全局安全 ACL 功能不存在。访问列表规则配置请参考相关章节的说明

#### 配置全局安全 ACL

- 必须配置。要使得全局安全 ACL 起作用，就必须在开启全局安全功能。
- 可以根据用户的分布，在接入、汇聚或核心设备配置全局安全 ACL 功能。

### 检验方法

可以在受全局安全 ACL 防护的网络内部 ping 被规则拒绝的站点或设备来验证全局安全 ACL 是否生效。



## 相关命令

---

### 配置访问列表

配置方法请参考访问列表的相关章节说明。

### 配置访问列表规则

配置方法请参考访问列表的相关章节说明。

### 配置全局安全 ACL

【命令格式】 `{ ip | mac | expert } access-group acl-id { in | out }`

【参数说明】 `acl-id`: 访问列表的编号。

`in`: 对进入设备的报文进行匹配过滤。

`out`: 对从设备转发出去的报文进行匹配过滤。

【命令模式】 配置模式

【使用指导】 通过该命令开启全局安全 ACL 功能，使得 ACL 在设备的所有二层口上生效。

### 配置全局安全 ACL 例外口

【命令格式】 `no global access-group`


【参数说明】 无

【命令模式】 接口模式

【使用指导】 通过该命令使得全局安全 ACL 在指定的接口上不生效。

## 配置举例

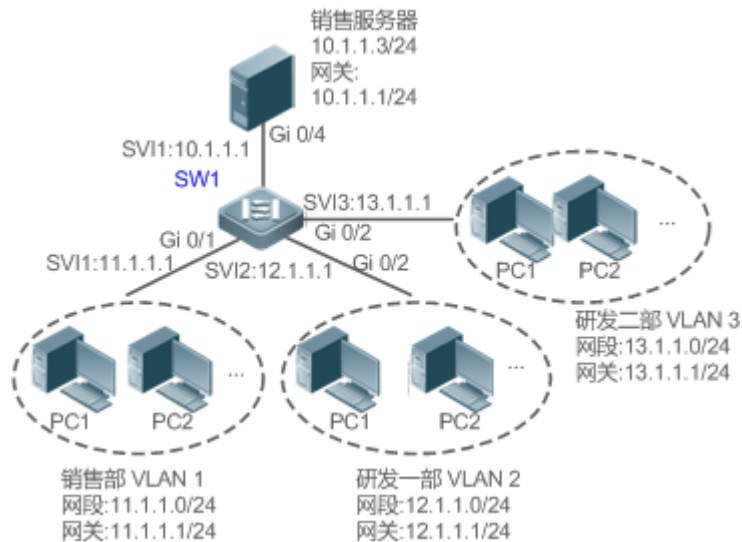
---

 以下配置举例，仅介绍与 ACL 相关的配置。

### 通过全局安全 ACL 功能，禁止研发部门访问销售服务器，但要允许销售部门访问

## 【网络环境】

图 1-9



## 【配置方法】

- 配置 IP 扩展访问列表 ip\_ext\_deny\_dst\_sale\_server
- 在 IP 访问列表中添加禁止目的主机 10.1.1.3/24 地址规则
- 将访问列表 ip\_ext\_deny\_dst\_sale\_server 配置为全局安全 ACL
- 将与销售部直连的端口配置为全局安全 ACL 例外口

## SW1

```
sw1(config)#ip access-list extended ip_ext_deny_dst_sale_server
sw1(config-ext-nacl)# deny ip any host 10.1.1.3
sw1(config-ext-nacl)#exit
sw1(config)#ip access-group ip_ext_deny_dst_sale_server in
sw1(config)#int gigabitEthernet 0/1
sw1(config-if-GigabitEthernet 0/1)# no global access-group
```

## 【检验方法】

- 在销售部内的某台 PC 机 ping 销售服务器地址，确认可以 ping 得通。
- 在研发一部和研发二部的 PC 机上 ping 销售服务器地址，确认 ping 不通。

```
sw1#show access-lists
ip access-list extended ip_ext_deny_dst_sale_server
 10 deny ip any host 10.1.1.3
sw1#show running
.....
!
ip access-group ip_ext_deny_dst_sale_server in
!
!
!
!
!
!
!
```

```
!  
interface GigabitEthernet 0/1  
    no global access-group  
!  
.....
```

## 1.5.8 配置安全通道

### 配置效果

通过配置安全通道功能，可以使得符合安全通道规则的报文绕过接入控制相关业务。如果用户上联的设备接口上开启了某个接入控制应用比如 dot1x，但在进行 dot1x 认证前，又要允许用户登录到某个站点上下载一些资源（比如下载锐捷 SU 客户端），这种情况就可以通过配置安全通道来实现。

### 注意事项

无

### 配置方法

#### 配置访问列表

- 必须配置。要实现安全通道功能，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

#### 配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于安全通道功能不生效。访问列表规则配置请参考相关章节的说明。

#### 配置接口安全通道或全局安全通道

- 如果想让安全通道在接口上生效，就在接口上配置安全通道；如果想让安全通道全局生效，就要配置全局安全通道，必须配置其中之一。
- 可以根据用户的分布，在接入、汇聚或核心设备配置安全通道功能。

#### 配置全局安全通道例外口

- 可选配置。如果配置了全局安全通道，但又不想让安全通道在某些接口上生效，就需要将这些接口配置为全局安全通道的例外口。

## 配置接入控制应用

- 可选配置，为了验证安全通道功能，可以在接口上开启 dot1x 或 web 认证功能。
- 可以根据用户的分布，在接入、汇聚或核心设备配置接入控制功能。

## 检验方法

可以通过在受接入控制业务控制的用户 PC 机上 ping 安全通道指定放过的资源（设备或服务器）来验证安全通道。

## 相关命令

### 配置访问列表

访问列表的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

### 配置接口安全通道

【命令格式】 **security access-group {acl-id | acl-name }**

【参数说明】 **acl-id**: 该选项若被配置，表示要将指定编号的访问列表配置成安全通道。

**acl-name**: 该选项若被配置，表示要将指定的命名访问列表配置成安全通道

【命令模式】 接口模式

【使用指导】 通过该命令在指定接口上将指定的 ACL 配置成安全通道。

### 配置全局安全通道

【命令格式】 **security global access-group {acl-id | acl-name }**

【参数说明】 **acl-id**: 该选项若被配置，表示要将指定编号的访问列表配置成安全通道。

**acl-name**: 该选项若被配置，表示要将指定的命名访问列表配置成安全通道

【命令模式】 全局配置模式

【使用指导】 通过该命令将指定的 ACL 配置成全局安全通道。

### 配置全局安全通道例外口


【命令格式】 **security uplink enable**

【参数说明】 无

【命令模式】 接口模式

【使用指导】 通过该命令将指定的接口配置成全局安全通道例外口。

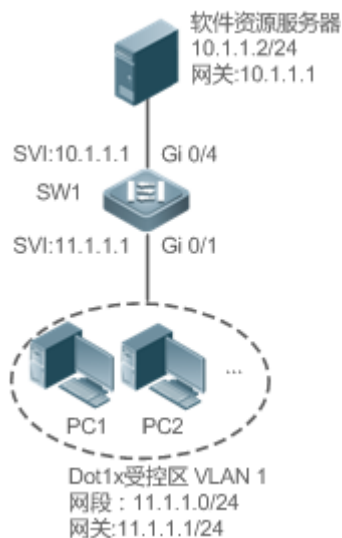
## 配置举例

 以下配置举例，仅介绍与 ACL 相关的配置。

### 在 dot1x 认证环境中，通过安全通道，允许用户认证前从服务器上下载 SU 客户端软件

#### 【网络环境】

图 1-10



#### 【配置方法】

- 配置 Expert 扩展访问列表 exp\_ext\_esc
- 在访问列表中添加允许目的主机 10.1.1.2 地址规则
- 在访问列表中添加允许 DHCP 报文通过规则
- 在访问列表中添加允许 ARP 报文通过规则
- 在 dot1x 受控区接口上将访问列表 exp\_ext\_esc 配置为安全通道

#### SW1

```
sw1(config)#expert access-list extended exp_ext_esc
sw1(config-exp-nacl)# permit ip any any host 10.1.1.2 any
sw1(config-exp-nacl)# permit 0x0806 any any any any any
sw1(config-exp-nacl)# permit tcp any any any any eq 67
sw1(config-exp-nacl)# permit tcp any any any any eq 68
sw1(config)#int gigabitEthernet 0/1
sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc
```

#### 【检验方法】

- 在销售部内的某台 PC 机 ping 销售服务器地址，确认可以 ping 得通。
- 在研发一部和研发二部的 PC 机上 ping 销售服务器地址，确认 ping 不通。

```
sw1#show access-lists
expert access-list extended exp_ext_esc
 10 permit ip any any host 10.1.1.2 any
 20 permit arp any any any any any
 30 permit tcp any any any any eq 67
 40 permit tcp any any any any eq 68.....

sw1#show running-config interface gigabitEthernet 0/1
```

```
Building configuration...
Current configuration : 59 bytes

interface GigabitEthernet 0/1
 security access-group exp_ext_esc
```

## 1.5.9 配置基于时间区的规则

### 配置效果

如果想让访问列表的某些规则在指定的时间生效，或在指定的时间内失效，比如让 ACL 在一个星期的某些时间段内生效等。可以配置基于时间区的访问列表规则。

### 注意事项

无

### 配置方法

#### 配置访问列表

- 必须配置。要实现基于时间区生效的规则，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

#### 配置带时间区的访问列表规则

- 必须配置。配置时需要带上对应的时间区选项，时间区的配置请参考时间区相关的配置手册。

#### 应用访问列表

- 必须配置。要使得访问列表规则在指定的时间区内生效，就必须访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IP 访问列表。

### 检验方法

在生效时间区内，可以通过 ping 或构造符合规则报文的方式来进行检验规则是否生效来检验；在失效时间区内，可以通过 ping 或构造符合规则报文的方式来进行检验规则是否不生效来检验。

### 相关命令

#### 配置访问列表

访问列表的配置命令请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

### 配置带时间区的访问列表规则

访问列表规则的配置命令请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

### 应用访问列表

访问列表规则的应用命令请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

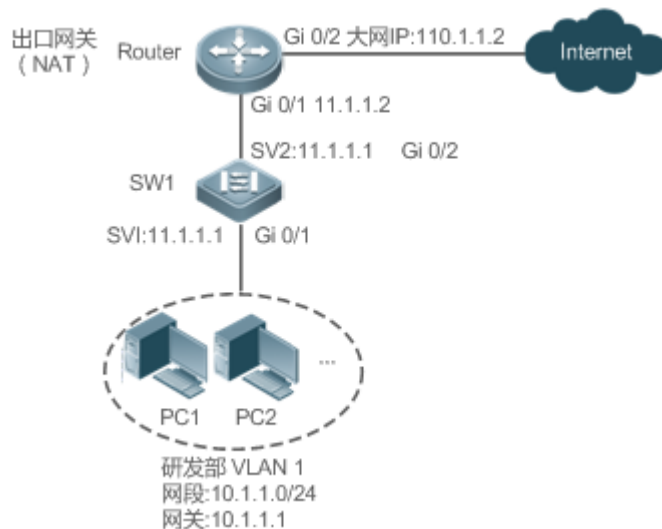
## 配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

### 配置基于时间区的访问列表规则，只允许研发部门在每天的 12:00 到 13:30 访问 internet

【网络环境】

图 1-11



【配置方法】

- 配置名称为 access-internet 的时间区，并添加每天 12:00 到 13:30 的时间段表项。
- 配置 IP 访问列表 ip\_std\_internet\_acl。
- 在访问列表中添加允许源 IP 网段为 10.1.1.0/24 的地址规则，关联的时间区为 access-internet。
- 在访问列表中添加禁止源 IP 网段为 10.1.1.0/24 的地址规则。表明时间区之外都不允许访问 internet
- 在访问列表中添加允许所有的地址规则
- 将访问列表应用在设备与出口网关相连接接口的出方向上。

SW1

```
Ruijie(config)# time-range access-internet
Ruijie(config-time-range)# periodic daily 12:00 to 13:30
Ruijie(config-time-range)# exit
sw1(config)# ip access-list standard ip_std_internet_acl
sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet
sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255
sw1(config-std-nacl)# permit any
sw1(config-std-nacl)# exit
```

```
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out
```

- 【检验方法】
- 在时间区生效期内（12:00 至 13:30），从研发部分内的某台 PC 机访问百度主页，确认可以访问。
  - 在时间区失效期（12:00 至 13:30 这个时段外），从研发部分内的某台 PC 机访问百度主页，确认不能访问。

**SW1**

```
sw1#show time-range

time-range entry: access-internet (inactive)
    periodic Daily 12:00 to 13:30

sw1#show access-lists

ip access-list standard ip_std_internet_acl
  10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive)
  20 deny 10.1.1.0 0.0.0.255
  30 permit any

sw1#show access-group
ip access-group ip_std_internet_acl out
Applied On interface GigabitEthernet 0/2
```

## 1.5.10 配置访问列表注释信息

### 配置效果

在实际的网络维护过程中，如果配置了很多访问列表且没有为这些访问列表配置注释信息，时间一长往往会难以区分这些访问列表的用途。为访问列表配置注释信息，可以方便理解 ACL 用途。

### 注意事项

无

### 配置方法

#### 配置访问列表

- 必须配置。要实现安全通道功能，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。



### 配置访问列表注释信息

- 可选配置。为便于管理和理解所配置的访问列表，可以为访问列表配置注释信息。

### 配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于安全通道功能不生效。访问列表规则配置请参考相关章节的说明。

### 配置访问列表规则注释信息

- 可选配置。为便于理解所配置的访问列表，除了可以为访问列表本身配置注释信息外，还可以为规则配置注释信息。

## 检验方法

可以通过在设备上使用 **show access-lists** 命令验证访问列表注释信息。

## 相关命令

### 配置访问列表

访问列表的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

### 配置访问列表注释信息

有以下两种方式为访问列表配置注释信息：

【命令格式】 **list-remark** *comment*

【参数说明】 *comment*: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 访问列表模式

【使用指导】 通过该命令为指定的访问列表配置注释信息

【命令格式】 **access-list** *acl-id* **list-remark** *comment*

【参数说明】 *acl-id*: 访问列表编号

*comment*: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 配置模式

【使用指导】 通过该命令为指定的访问列表配置注释信息

### 配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

### 配置访问列表规则注释信息

有以下两种方式为访问列表规则配置注释信息：

【命令格式】 **[sn] remark comment**

【参数说明】 *comment*: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符  
*sn*: 需要注释规则的序列号

【命令模式】 访问列表模式

【使用指导】 通过该命令为指定的访问列表规则配置注释信息，若 *sn* 未配置默认注释访问列表中最后一个规则

【命令格式】 **access-list acl-id sn remarkcomment**

【参数说明】 *acl-id*: 访问列表编号  
*comment*: 注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符  
*sn*: 需要注释规则的序列号

【命令模式】 配置模式

【使用指导】 通过该命令为访问列表规则添加注释信息，若 *sn* 未配置默认注释访问列表中最后一个规则

## 配置举例

无

## 1.6 监视与维护

### 清除各类信息

作用	命令
清除访问列表报文匹配计数	<b>clear counters access-list [ acl-id   acl-name ]</b>
清除访问列表 deny 报文匹配计数	<b>clear access-list counters [acl-id  acl-name ]</b>

### 查看运行情况

作用	命令
查看基本访问列表	<b>show access-lists [ acl-id   acl-ame ] [summary]</b>
显示指定接口上绑定的重定向表项，不输入接口则显示所有接口上绑定的重定向表项。	<b>show redirect [ interface interface-name ]</b>
显示接口上应用的访问列表配置信息。	<b>show access-group [interface interface-name ]</b>
显示接口上应用的 IP 访问列表配置信息。	<b>show ip access-group [interface interface-name ]</b>
显示接口上应用的 MAC 扩展访问列表配置信息。	<b>show mac access-group [interface interface-name ]</b>

显示接口上应用的 Expert 扩展访问列表配置信息。	<b>show expert access-group</b> [interface <i>interface-name</i> ]
显示接口上应用的 IPv6 访问列表配置信息。	<b>show ipv6 traffic-filter</b> [interface <i>interface-name</i> ]
显示所有的 TCAM 信息或指定的 TCAM 信息	<b>show acl res</b> [ dev <i>dev-num</i> [ slot <i>slot-num</i> ]]

## 查看调试信息



输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
监视访问列表运行过程信息	<b>debug acl acld event</b>
调试查看 ACL 客户端的信息	<b>debug acl acld client-show</b>
调试查看所有 ACL 客户端创建的访问列表信息	<b>debug acl acld acl-show</b>

## 2 QoS

### 2.1 概述

QoS ( Quality of Service , 服务质量 ) 指一个网络能够利用各种基础技术 , 为指定的网络通信提供更好的服务能力。

当网络带宽充裕的时候 , 所有的数据流都得到了较好的处理 ; 而当网络发生拥塞的时候 , 所有的数据流都有可能被丢弃 ; 为满足用户对不同应用不同服务质量的要求 , 就需要网络能根据用户的要求分配和调度资源 , 对不同的数据流提供不同的服务质量 : 对实时性强且重要的数据报文优先处理 ; 对于实时性不强的普通数据报文 , 提供较低的处理优先级 , 网络拥塞时甚至丢弃。

传统网络所采用的 “尽力而为” 的转发机制 , 已经不能满足这些需求 , QoS 应运而生。支持 QoS 功能的设备 , 能够提供传输品质服务 ; 针对某种类别的数据流 , 可以为它赋予某个级别的传输优先级 , 来标识它的相对重要性 , 并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。配置了 QoS 的网络环境 , 增加了网络性能的可预知性 , 并能够有效地分配网络带宽 , 更加合理地利用网络资源。

### 2.2 典型应用

典型应用	场景描述
端口限速+优先级重标记应用	基于校园网的不同业务需求 , 对教学楼、实验室、宿舍楼的出口流量进行限速控制及优先级处理。
优先级重标记+队列调度应用	对于企业内部访问服务器的流量进行优先级处理及带宽控制。

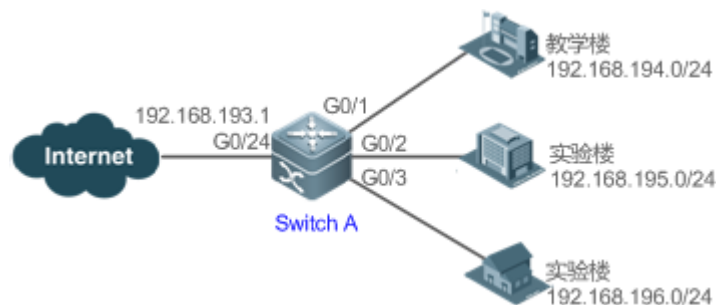
#### 2.2.1 端口限速+优先级重标记

##### 应用场景

某学校为了满足正常的教学业务需要 , 要求满足以下四点需求 :

- 限制该学校访问 Internet 的流量为 100M , 丢弃超出限制的报文 ;
- 限制宿舍楼的出口流量为 50M , 同样丢弃超出限制的报文 ;
- 限制实验楼发出 DSCP 优先级为 7 的报文的速率为 20M , 将速率超过 20M 的此类报文的 DSCP 优先级修改为 16 ;
- 限制教学楼的出口流量为 30M , 丢弃超出限制的报文。

图 2-1



【注释】 某学校通过 SwitchA 的 GigabitEthernet 0/24 上联 Internet，SwitchA 的 GigabitEthernet 0/1、GigabitEthernet 0/2 和 GigabitEthernet 0/3 分别下联的教学楼、实验楼和宿舍楼。

## 功能部署

- 在 SwitchA 连接 Internet 的 G0/24 端口配置 QoS 端口速率限制；
- 在 SwitchA 上配置对宿舍楼发出的报文进行 QoS 限速；
- 在 SwitchA 上配置对实验楼发出的 DSCP 优先级为 7 的报文限速为 20M，并将超过限速的报文的 DSCP 优先级重标记为 16；
- 在 SwitchA 上配置对教学楼发出的报文进行 QoS 限速；

## 2.2.2 优先级重标记+队列调度应用

### 应用场景

配置优先级重标记和队列调度，实现下述需求：

- 当研发部和市场部访问服务器时，服务器报文的优先级为：邮件服务器> 文件服务器>工资查询服务器；
- 无论人事管理部访问 Internet 或访问服务器，交换机都优先处理；
- 交换机在运行过程中，时常发现网络拥塞，为了保证业务顺利运转，要求使用 WRR 队列调度，对研发部和市场部访问邮件数据库、访问文件数据库、访问工资查询数据库的 IP 数据报按照 6：2：1 的比例来调度。

图 2-2



【注释】 研发部、市场部和人事管理部分别接入 SwitchA 的端口 GigabitEthernet 0/1、GigabitEthernet 0/2 和 GigabitEthernet 0/3；工资查询服务器、邮件服务器和文件服务器连接在 SwitchA 的端口 GigabitEthernet 0/23 下。

## 功能部属

- 通过配置访问不同服务器数据流的 CoS 值，实现设备处理访问各种服务器报文的优先级；
- 通过配置接口的缺省 CoS 值为特定值，实现设备优先处理人事管理部发出的报文；
- 通过配置 WRR 队列调度实现按特定个数比进行数据报文传输调度。

## 2.3 功能详解

### 基本概念

#### 差分服务模型

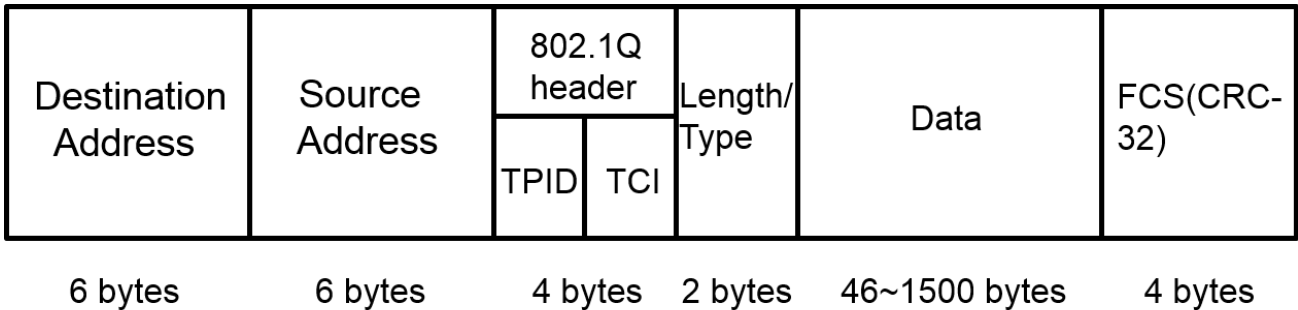
DiffServ ( Differentiated Services Mode , 差分服务模型 )，锐捷产品的 QoS 实现以 IETF 的 DiffServ 体系为基础。DiffServ 体系规定网络中的每一个传输报文将被划分成不同的类别，分类信息包含在二层/三层报文头中，包括：802.1P 优先级、IP 优先级、IP DSCP 优先级。

在遵循 DiffServ 体系的网络中，各设备对包含相同分类信息的报文采取相同的传输服务策略，对包含不同分类信息的报文采取不同的传输服务策略。报文的分类信息可以由网络上的主机或者其它网络设备赋予，也可以基于不同的应用策略或者基于报文内容的不同为报文赋予类别信息。设备根据报文所携带的类别信息，为各种报文流提供不同的传输优先级，或者为某种报文流预留带宽，或者适当地丢弃一些优先级较低的报文，或者采取其他一些操作等等。

#### 802.1P(PRI)优先级

802.1 P 优先级位于带有 802.1Q 标签头的二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合，结构如下：

图 2-3

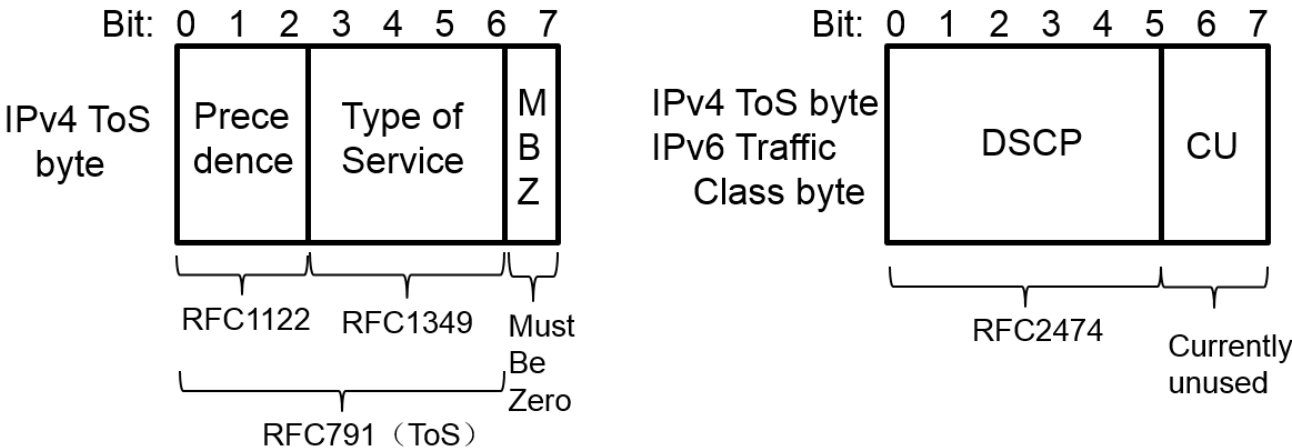


如上图所示，4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID(Tag ProtocolIdentifier，标签协议标识，取值为 0x8100)和 2 个字节的 TCI(Tag ControllInformation，标签控制信息)，其中 TCI 中的前 3 位即 802.1P 优先级。

📌 IP 优先级(IP PRE)和 DSCP 优先级

IP 报文使用 IP 优先级和 DSCP 优先级表示报文优先级。IPv4 头的 ToS (Type Of Service，服务类型) 字段有 8 个 bit，其中前 3 个 bit 表示的就是 IP PRE (IP precedence)，取值范围为 0~7。在 RFC 2474 中，重新定义了 IPv4 报文头部的 ToS 域，称之为 DS(Differentiated Services，差分服务)域，其中 DSCP (Differentiated Services Code Point) 优先级用该域的前 6 位 (0~5 位)表示；IPv6 中使用报文头中的 Traffic Class 字段的前 6 个比特，表示 DSCP。IPv4/IPv6 报文的 IP PRE 和 DSCP 优先级位置如下图：

图 2-4



📌 服务类别

CoS (Class of Service，服务类别) 锐捷产品中将报文优先级转化为 CoS 用于本地优先级，用于确定出端口发送时的入队列号。

功能特性

功能特性	作用
流分类	流分类采用一定的规则识别符合某类特征的报文，它是对网络业务进行区分服务的前提和基础。
优先级标记与映射	优先级标记与映射即标记报文的优先级为指定的值，并映射到相应的 CoS 值去。

流量监管	流量监管是监控进入网络的某一流量的规格，把它限制在一个合理的范围之内，丢弃超出部分的流量或者修改其优先级。
拥塞管理	拥塞管理根据数据包的优先级，来确定数据包从接口发送的顺序，在拥塞发生时，确保关键业务能够得到及时的服务。
拥塞避免	拥塞避免通过监控出端口队列的使用情况，在网络拥塞时，采取主动丢弃报文，调整网络流量的方式来解除网络过载。

### 2.3.1 流分类

流分类采用一定的规则识别符合某类特征的报文。它是对网络业务进行区分服务的前提和基础，通过流分类规则区分网络中不同的报文，再为不同服务等级的报文指定不同的 QoS 参数。

#### 工作原理

流分类的规则可以是匹配 IP 报文的 PRE 或 DSCP 优先级、或者通过 ACL 识别报文的内容进行分类。用户可以通过命令定义多个流与流行为的绑定关系形成策略应用在接口上进行流分类与处理。

#### QoS 策略

QoS 策略包含了三个要素：类、流行为、策略：

- 类  
类是用来识别流的。类的要素包括：类的名称和类的规则。用户可以通过命令定义类的规则，来对报文进行分类。
- 流行为  
流行为用来定义针对报文采取的 QoS 动作。流行为包括对报文进行优先级标记与流量监控。
- 策略  
策略用来将指定的类和指定的流行为绑定起来。策略的要素包括：策略名称、绑定在一起的类的名称和流行为。用户通过 QoS 策略将指定的类和流行为绑定起来，然后再将策略应用到一个或多个端口上生效。

#### QoS 逻辑端口组

可以指定一系列端口为一个 QoS 逻辑端口组（这里端口可以是 AP，也可以是以太网口），并针对这个逻辑端口组关联策略进行 QoS 处理，以流行为限速为例，对符合限速条件的报文，在同一个逻辑端口组内所有的端口共享策略所限定的带宽值。

#### 相关配置

##### 创建类

缺省情况下，未定义任何类。

使用 **class-map** 命令，创建类并进入类配置模式。

##### 匹配 ACL



缺省情况下，类中未定义任何规则。

在类配置模式下，使用 **match access-group** 命令，定义类的规则为匹配 ACL，ACL 规则需先创建。

#### 匹配 IP 报文的 PRE 优先级

缺省情况下，类中未定义任何规则。

在类配置模式下，使用 **match ip precedence** 命令，定义类的规则为匹配 IP 报文的 PRE 优先级，IP PRE 的取值范围为 0~7。

#### 匹配 IP 报文的 DSCP 优先级

缺省情况下，类中未定义任何规则。

在类配置模式下，使用 **match ip dscp** 命令，定义类的规则为匹配 IP 报文的 DSCP 优先级，DSCP 优先级的取值范围为 0~63。

#### 创建策略

缺省情况下，未定义任何策略。

使用 **policy-map** 命令，创建策略并进入策略配置模式。

#### 关联类

缺省情况下，策略未关联任何类。

在策略配置模式下，使用 **class** 命令，关联类并进入策略类配置模式。

#### 绑定流行为

缺省情况下，类未绑定任何流行为。

在策略类配置模式下，使用 **set** 命令对指定流修改 CoS、DSCP 或 VID 值，其中 CoS 取值范围为 0~7，DSCP 取值范围为 0~63，VID 取值范围为 1~4094；使用 **police** 命令对指定流进行带宽限制及超限处理，带宽限制范围由产品决定。

#### 配置逻辑端口组

缺省情况下，未定义任何逻辑端口组，接口也未加入任何逻辑端口组。

在全局模式下，使用 **virtual-group** 命令，来创建一个逻辑端口组；在接口配置模式下，使用 **virtual-group** 命令，将接口加入一个逻辑端口组，如果此时逻辑接口组还未创建，则创建逻辑接口组并将接口加入。可以创建 128 个逻辑端口组，取值范围为 1~128。

#### 接口上应用策略

缺省情况下，接口上未应用任何策略。

在接口配置模式下，使用 **service-policy** 命令，在接口的输入/输出方向上应用策略；在全局配置模式下，使用 **service-policy** 命令，在所有接口的输入/输出方向上应用策略。

## 2.3.2 优先级标记与映射

优先级用以标识报文的调度权重或者转发处理优先级别的高低。根据报文类型不同，有不同的优先级类型：802.1P ( PRI ) 优先级、IP 优先级 ( IP PRE )、DSCP 优先级。报文优先级标记与映射即标记报文的优先级为指定的值，并映射到相应的 CoS 值去。

### 工作原理

报文数据流进入设备端口之后，设备会根据端口配置的信任模式来分配报文的各类优先级。有如下几种形式：

- 端口信任模式为非信任时，即不信任报文中携带的优先级信息：  
根据端口的默认 CoS ( 可配置，默认为 0 ) 和 COS-DSCP 映射表、DSCP-COS 映射表修改 CoS，根据最终的 CoS 入队列，如果报文出口带 802.1Q tag 那么报文优先级也会被修改成对应的 Cos。
- 端口信任模式为信任 CoS 时：  
如果是带 802.1Q tag 的报文，根据报文的 PRI 值和 CoS-DSCP 映射表、DSCP-COS 映射表修改 COS，根据最终的 CoS 入队列，如果报文出口带 802.1Q tag 那么报文优先级也会被修改成对应的 Cos；  
如果是不带 802.1Q tag 的报文，根据端口的默认 CoS (可配置，默认为 0)和 CoS-DSCP 映射表、DSCP-COS 映射表修改 COS，根据最终的 CoS 入队列，如果报文出口带 802.1Q tag 那么报文优先级也会被修改成对应的 Cos。
- 端口信任模式为信任 DSCP 时：  
如果是非 IP 报文，按照信任 CoS 处理；  
如果是 IP 报文，此时根据报文的 DSCP 值和 DSCP-CoS 映射表修改 CoS，根据最终的 CoS 入队列。
- 端口信任模式为信任 IP PRE 时：  
如果是非 IPv4 报文，按照信任 CoS 处理；  
如果是 IPv4 报文，此时根据报文的 IP PRE 值和 IP-PRE-DSCP 映射表，得到并修改报文的 DSCP，再根据 DSCP-CoS 映射表得到 CoS，根据最终的 CoS 入队列。
- 端口信任模式与应用于端口的策略同时作用情况下的关系：  
当端口信任模式和应用于端口的策略同时作用时，端口信任模式修改 DSCP 和 CoS 的优先级低于策略修改 CoS、DSCP，并根据 DSCP-CoS 映射表得到 CoS 的优先级；  
端口应用策略，但策略没有设置修改 DSCP 和 CoS 值时，按照此时端口的信任模式执行。

### 相关配置

#### 📌 配置端口的信任模式

缺省情况下，端口的信任模式为非信任。

在接口配置模式下，使用 **mls qos trust** 命令，修改信任模式，可配置的信任模式为信任 CoS、信任 DSCP、信任 IP PRE。

#### 📌 配置接口的缺省 CoS 值

缺省情况下，接口的 CoS 值为 0。

在接口配置模式下，使用 **mls qos cos** 命令，来修改接口缺省的 CoS 值，CoS 取值范围为 0~7。

#### 📌 流的优先级标记

缺省情况下，不对流的优先级进行重标记。

在策略类配置模式下，使用 **set** 命令，来修改流的 CoS、DSCP、VID，其中 CoS 取值范围为 0~7，DSCP 取值范围为 0~63，VID 取值范围为 1~4094。

#### 📌 配置 CoS-to-DSCP Map

缺省情况下，CoS 值 0 1 2 3 4 5 6 7 分别映射到 DSCP 值 0 8 16 24 32 40 48 56。

使用 **mls qos map cos-dscp** 命令，来配置 CoS 值到 DSCP 值的映射，DSCP 取值范围为 0~63。

#### 📌 配置 DSCP-to-CoS Map

缺省情况下，DSCP 0~7 映射到 CoS 0，DSCP 8~15 映射到 CoS 1，DSCP 16~23 映射到 CoS 2，DSCP 24~31 映射到 CoS 3，DSCP 32~39 映射到 CoS 4，DSCP 40~47 映射到 CoS 5，DSCP 48~55 映射到 CoS 6，DSCP 56~63 映射到 CoS 7。

使用 **mls qos map dscp-cos** 命令，来配置 DSCP 值到 CoS 值的映射，其中 CoS 取值范围为 0~7，DSCP 取值范围为 0~63。

#### 📌 配置 IP-PRE-to-DSCP Map

缺省情况下，IP PRE 值 0 1 2 3 4 5 6 7 分别映射到 DSCP 值 0 8 16 24 32 40 48 56。

使用 **mls qos map ip-prec-dscp** 命令，来配置 IP PRE 值到 DSCP 值的映射，DSCP 取值范围为 0~63。

## 2.3.3 流量监管

流量监管是监控进入网络的某一流量的规格，把它限制在一个合理的范围之内，丢弃超出部分的流量或者修改报文优先级。同时能监控端口总的流量，丢弃超出部分的流量。

### 工作原理

流量监管监控进入网络的某一流量的规格，依据不同的评估结果，实施预先设定好的监管动作。这些动作可以是：

- 转发：对未超过流量限制的报文正常转发处理；
- 丢弃：对超过流量限制的报文进行丢弃；
- 改变优先级并转发：对超过流量限制的报文，修改其优先级后再转发。

对于超过端口总流量限制的报文，直接丢弃。

### 相关配置

#### 📌 配置流量超限后的动作

缺省情况下，未配置流量超限后动作。

在策略类配置模式下，使用 **police** 命令，来配置流量超限后的动作，可以配置为对超限流量丢弃，修改 CoS 或者 DSCP 值。流量超限范围由产品决定，流量超限后可修改的 CoS 取值范围为 0~7，DSCP 取值范围为 0~63。

#### 配置端口总流量限制

缺省情况下，未配置端口总流量限制。

在接口配置模式下，使用 **rate-limit** 命令，来配置端口输入/输出方向总流量限制。流量限制范围由产品决定。

### 2.3.4 拥塞管理

当报文的接收速率超过发送速率时，在发送端口上就会出现拥塞，如果不能提供足够的缓冲区来保存这些报文，就会造成报文的丢失。拥塞管理机制根据数据包的优先权，来确定数据包发送出接口的顺序，拥塞管理功能允许对拥塞进行控制，对于一些重要的数据，提高数据报文的优先权，在拥塞发生时，优先发送，确保关键业务能够得到及时服务。

#### 工作原理

使用队列调度机制进行拥塞管理，处理过程如下：

- 每个报文经过设备内部各个 QoS 处理环节，最终都会得到一个 CoS 值；
- 在出端口，设备会根据这个 CoS 值将报文归类到对应发送队列中；
- 出端口根据各种调度策略（SP、WRR、DRR、WFQ、SP+WRR、SP+DRR、SP+WFQ），选取其中一个队列的报文进行发送。

#### 调度策略

队列调度策略分为 SP、WRR、DRR、WFQ、SP+WRR、SP+DRR、SP+WFQ。

- SP (Strict-Priority，严格优先级)调度，严格按照队列 ID 进行调度。即每次发送报文之前，先检查高优先级队列中是否有报文待发送，如果有则发送；如果没有则检查下一优先级队列中是否有待发送报文，以此类推；
- WRR(Weighted Round Robin，加权循环队列算法)调度，在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以 1 个 1000Mbps 端口 8 个输出队列为例，WRR 可为每个队列配置一个加权值（5、5、10、20、20、10、20、10，加权值表示获取资源的比重）。这样可以保证最低优先级队列至少获得 50Mbps 的带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点；
- DRR(Dificit Round Robin，差额循环队列算法)调度，DRR 和 WRR 类似，不过不是按照时间片，而是按照 byte 数来应用权重；
- WFQ(Weighted Fair Queueing，加权公平队列算法)调度，提供了动态的、公平的排队方式，与 DRR 类似也是按照 byte 数来应用权重；区别在于 DRR 算法如果遇到一个空队列，会立即移到下一个队列进行传输，如果队列错过了它的传输时刻就只能等到下一个时刻才能传输，WFQ 不受这种影响，而且比 DRR 更适合于处理变长数据包；
- SP+WRR 调度，即将一个或多个发送队列配置成 SP，其他队列以 WRR 方式调度；SP 队列间，只有高优先级 SP 队列报文发送完了，才发送下一优先级 SP 队列中的报文；SP 与 WRR 调度队列间，只有所有 SP 队列报文发送完成后，才会处理 WRR 调度队列报文。

- SP+DRR 调度，即将一个或多个发送队列配置成 SP，其他队列以 DRR 方式调度；SP 队列间，只有高优先级 SP 队列报文发送完了，才发送下一优先级 SP 队列中的报文；SP 与 DRR 调度队列间，只有所有 SP 队列报文发送完成后，才会处理 DRR 调度队列报文。
- SP+WFQ 调度，即将一个或多个发送队列配置成 SP，其他队列以 WFQ 方式调度；SP 队列间，只有高优先级 SP 队列报文发送完了，才发送下一优先级 SP 队列中的报文；SP 与 WFQ 调度队列间，只有所有 SP 队列报文发送完成后，才会处理 WFQ 调度队列报文。

## 📌 QoS 组播队列

在一些产品上，端口队列被划分成单播队列和组播队列。单播队列包含 8 个队列，所有知名单播报文都按照优先级进入对应的单播队列转发；组播队列包含 1-8 个队列（依产品而定，某些产品不支持组播队列功能），除了知名单播报文以外的所有报文（如广播报文、组播报文、未知单播报文、镜像报文等）都按照优先级进入对应的组播队列转发。组播队列和单播队列一样，可以配置优先级映射和调度算法，通过配置 Cos-to-Mc-Queue 可以实现优先级到组播队列的映射，组播队列目前支持的调度算法为 SP、WRR、SP+WRR 调度。

## 📌 端口下输出队列调度策略与轮转权重比

输出队列调度策略与轮转权重比是基于全局配置的，在一些产品上，同时支持基于全局与基于端口的配置，端口配置的优先级高于全局配置。全局调度策略与相应的全局轮转权重比，端口调度策略与相应的端口轮转权重比配合生效；如果只配置全局调度策略或者端口调度策略，未配置相应的轮转权重比，则以默认的轮转权重比配合调度策略生效。

## 📌 队列带宽

在一些产品上，允许配置队列的最小保证带宽与最大限制带宽；配置了最小保证带宽的队列可以保证此队列的带宽不小于配置值；配置了最大限制带宽的队列可以限制此队列的带宽不超过配置值，丢弃超过最大限制带宽的报文。在某些产品上单播队列、组播队列的带宽限制是一起配置的；在某些产品上单播队列、组播队列的带宽限制是分开配置的；在某些产品上只支持单播队列的带宽配置。

## 相关配置

### 📌 配置 CoS-to-Queue Map

缺省情况下，CoS 值 0 1 2 3 4 5 6 7 分别映射到队列 1 2 3 4 5 6 7 8。

使用 **priority-queue cos-map** 命令，来配置 CoS 到队列的映射，其中 CoS 的取值范围为 0~7，队列的取值范围为 1~8。

### 📌 配置输出队列调度策略

缺省情况下，全局输出队列的调度策略为 WRR。

使用 **mls qos scheduler** 命令，来配置队列的输出调度策略，可配置的调度策略有 SP、WRR、DRR、WFQ；或者使用 **priority-queue** 命令将调度策略配置为 SP。

### 📌 配置 WRR 输出队列调度策略的轮转权重

缺省情况下，全局队列权重比为 1:1:1:1:1:1:1:1。

使用 **wrr-queue bandwidth** 命令，来配置 WRR 输出队列调度策略的轮转权重，可配置权重范围由产品决定。

权重越大，所获得的输出时间就越多。

#### 配置 DRR 输出队列调度策略的轮转权重

缺省情况下，全局队列权重比为 1:1:1:1:1:1:1:1。

使用 **drr-queue bandwidth** 命令，来配置 DRR 输出队列调度策略的轮转权重，可配置权重范围由产品决定。

权重越大，所能发送的报文 bytes 就越多。

#### 配置 WFQ 输出队列调度策略的轮转权重

缺省情况下，全局队列权重比为 1:1:1:1:1:1:1:1。

使用 **wfq-queue bandwidth** 命令，来配置 WFQ 输出队列调度策略的轮转权重，可配置权重范围由产品决定。

权重越大，所能发送的报文 bytes 就越多。

#### 配置队列带宽

使用 **qos queue** 来配置各个队列的最小保证带宽与最大限制带宽。队列的取值范围为 1~8，最小保证带宽、最大限制带宽的取值范围由产品决定，能支持配置的队列类型由产品决定。

## 2.3.5 拥塞避免

拥塞避免通过监控出端口队列的使用情况，在网络拥塞时，采取主动丢弃报文，调整网络流量的方式来解除网络过载。

### 工作原理

拥塞避免通过有效监控网络流量负载预期拥塞的发生，通过丢弃报文达到避免拥塞的目的，丢弃策略有尾部丢弃（Tail-Drop）、RED（Random Early Detection，早期随机检测）丢弃、WRED（Weighted Random Early Detection，加权随机早期检测）丢弃：

#### 尾部丢弃

传统的丢包策略采用尾部丢弃的方法。尾部丢弃对所有的流量都起作用，它并不能区分不同服务级别。在拥塞发生期间，队列尾部的数据包将被丢弃，直到拥塞解决。

#### RED 与 WRED

运行 TCP 协议的主机会采用降低报文发送速率的方法来响应大量丢包的情况，当拥塞得到解决后，再提高数据包的发送速率。这样一来，尾部丢弃可能会引发 TCP 全局同步（Global Synchronization）——当队列同时丢弃多个 TCP 报文时，造成多个 TCP 连接同时进入拥塞避免和慢启动状态，同时降低并调整流量，而后又会在拥塞减少时出现流量高峰，如此反复，使网络流量忽大忽小，线路流量总在极少和饱满之间波动。当 TCP 同步发生时，连接的带宽不能充分利用，从而造成了带宽的浪费。

为了避免这种情况的发生，可以采用 RED/WRED 的报文丢弃策略，它提供了随机丢弃报文的机制，避免了 TCP 的全局同步现象。使得某个 TCP 连接的报文被丢弃，开始减速发送的时候，其他的 TCP 连接仍然有较高的发送速度。这样，无论什么时候，总有 TCP 连接在进行较快的发送，提高了线路带宽的利用率。

采用 WRED 时，用户可以设定队列的低门阈值与最大丢弃概率。当队列的长度小于低门阈值（取值范围为 1~100）时，不丢弃报文；当队列的长度在低门阈值和高门阈值（固定为 100）之间时，WRED 开始随机丢弃报文（队列的长度越长，丢弃的概率越高，有个最大丢弃概率）；当队列的长度大于高门阈值时，以最大丢弃概率丢弃报文。

RED 与 WRED 的区别是后者引入优先权来区别丢弃策略，RED 作为 WRED 的特例，只有当接口上所有的 CoS 都映射到同一个低限和高限时，这时 WRED 就成为了 RED。

## 相关配置

### 开启 WRED 功能

缺省情况下，报文丢弃策略为尾部丢弃。

使用 **queueing wred** 命令，来开启 WRED 功能。

### 配置低门阈值

缺省情况下，支持 2 组低门阈值时，缺省值为 100，80（阈值组数依产品而定）。

在接口配置模式下，使用 **wrr-queue random-detect min-threshold** 命令，来配置各个队列的 WRED 丢弃的低门阈值，队列的取值范围为 1~8，低门阈值的取值范围为 1~100。

当队列的长度小于低门阈值时，不丢弃报文；当队列的长度在低门阈值和高门阈值之间时，WRED 开始随机丢弃报文。

### 配置最大丢弃概率

缺省情况下，支持 2 组最大丢弃概率时，缺省值为 100，80（阈值组数依产品而定）。

在接口配置模式下，使用 **wrr-queue random-detect probability** 命令，来配置各个队列的 WRED 丢弃的最大丢弃概率，队列的取值范围为 1~8，最大丢弃概率的取值范围为 1~100。

当队列的长度在低门阈值和高门阈值之间时，WRED 开始随机丢弃报文，队列的长度越长，丢弃的概率越高，最大不超过最大丢弃概率；当队列的长度大于高门阈值时，以最大丢弃概率丢弃报文。

### 配置 CoS 与门阈值的映射

缺省情况下，所有的 CoS 都映射到第一组阈值（阈值组数依产品而定）。

在接口配置模式下，使用 **wrr-queue cos-map** 命令，来配置 CoS 到阈值组的映射，CoS 的取值范围为 0~7，阈值组数由产品决定。低门阈值、最大丢弃概率都可以配置多组，通过配置 CoS 到阈值组的映射，可以选择此 CoS 所对应的生效阈值组，比如 CoS 0 映射到第一组阈值，CoS 1 映射到第二组阈值，如果 CoS 0 和 1 的报文都进入队列 1 调度，此时 CoS 0 的报文使用第一组的低门阈值与最大丢弃概率进行处理；CoS 1 的报文使用第二组低门阈值与最大丢弃概率进行处理。

当接口上所有的 CoS 都映射到同一组阈值时，这时启用的 WRED 就成为了 RED。

## 2.4 产品说明



S6000E 系列产品，不支持在 SVI 口上配置 QOS 信任模式。





S6000E 系列产品，逻辑端口组的成员必须在同一张线卡内，加入逻辑端口组的成员必须是物理口或者是 Aggregate Port



S6000E 系列产品，CLASS MAP 所匹配的 ACL 表项中的 DENY 行为表项将被忽略，不会起作用。



S6000E 系列产品，不支持修改 vid 的动作。



S6000E 系列产品，应用在出口时，对于带宽超限部分的报文改写 DSCP 值，但不修改对应的 COS 值。应用在入口时，修改超限的 dscp 值，会改对应的 cos 值。

支持改写带宽超限部分的报文的 CoS 值，改写 CoS 值时同步修改对应的 DSCP 值，设置 none-tos 选项后，改写 CoS 值时不修改对应的 DSCP 值；QoS 匹配 DSCP 时，对 MPLS 报文无效。

配置 set cos 时，不支持 none-tos 选项。

带宽限制指的是实际带宽，包含前导码和帧间隙所占去的负荷。（每个报文所附带的前导码和帧间隙所占的带宽为 20 字节）。

支持最小限速粒度为 8Kbps，根据限速值设置的不同，最终会得到不同的限速粒度，具体的限速值和粒度值的关系大致如下表所示：

限速范围	64Kbps-2Gbps	2Gbps-4Gbps	4Gbps-8Gbps
粒度	8Kbps	16Kbps	32Kbps
限速范围	8Gbps-16Gbps	16Gbps-32Gbps	32Gbps-40Gbps
粒度	64Kbps	128Kbps	256Kbps

对于 Qos 策略限速的第二个参数(突发流量)，在存在突发流量的情况下，若参数值设置过小，会导致实际速率可能过小；若参数值设置过大，会导致实际速率可能过大。用户可根据实际情况，使用如下推荐配置：

1) 配置的限速值小于 1024Kbps 时，建议 burst-size 配置为 1024KByte。

2) 配置的限速值小于 10240Kbps 时，建议 burst-size 配置和限速值相同或使用最大值（各产品可能允许的 burst-size 最大值低于 10240KByte）。

3) 配置的限速值大于 10240Kbps 时，建议 burst-size 配置为该设备允许最大值。

对于 Qos 策略限速的第二个参数，当限速的速率比较大的时候，第二参数也要进行相应的调整，不然限速可能不准确。用户可以使用如下推荐配置：

对于万兆端口或 40G 端口，建议使用 burst-size 为 32 或 32 以上。



S6000E 系列产品，支持 policy map 应用到 out 方向。

当为 Aggregate Port 口应用 police 时，要求 AP 成员口必须满足以下条件时，设置的限制带宽才是 Aggregate Port 所有成员口的共享带宽。

1) 如果是 S6000E\_48GT4XS\_E，要求 Aggregate Port 的成员口必须全部属于该线卡的前 24 个端口或者后 24 个端口。

由于 class map 需要关联 acl，所以 acl 配置的所有限制均适用于 qos，具体请参考 acl 配置指南。

不支持在 SVI 口上应用 Policy Maps。

支持输出方向的 Policy Maps，但不支持 AP 口。

输出方向的 Policy Maps 中不支持重标记报文的 CoS 值。重标记报文的 DSCP 值时，不会同时标记报文的 CoS 值。



目前 output 方向应用在逻辑端口组上未被支持。由于 class map 需要关联 acl ,所以 acl 配置的所有限制均适用于 qos ,具体请参考 acl 配置指南。



VSL 口默认采用 SP+DRR 调度算法，其中队列 7 采用 sp 调度，其他队列权重都是 1，该调度配置不会被用户配置所改变。



端口速率的限制指的是实际带宽，包含前导码和帧间隙所占去的负荷。（每个报文所附带的前导码和帧间隙所占的带宽为 20 字节）。

支持最小限速粒度为 8Kbps，根据限速值设置的不同，最终会得到不同的限速粒度，具体的限速值和粒度值的关系大致如下表所示：

限速范围	64Kbps-2Gbps	2Gbps-4Gbps	4Gbps-8Gbps
粒度	8Kbps	16Kbps	32Kbps
限速范围	8Gbps-16Gbps	16Gbps-32Gbps	32Gbps-40Gbps
粒度	64Kbps	128Kbps	256Kbps

对于端口限速的第二个参数，当限速的速率比较大的时候，第二参数也要进行相应的调整，不然限速可能不准确。用户可以使用如下推荐配置：

对于万兆端口，建议使用 burst-size 为 32 或 32 以上。



当前只能通过 **show run** 来查看 WRED 全局功能是否已经开启。



队列上配置低门阈值和最大丢弃概率称为一组 wred 配置，S6000E 系列产品支持 120 组 wred 配置，不建议用户配置超过上述组数的 wred 配置，多配置的 wred 可能不能正常工作。

当低门阈值为 100%时，表示禁用 WRED 功能。



S6000E 系列产品支持物理口上配置映射关系。

管理员可以通过配置 DSCP-CoS 和 CoS-Threshold 的映射关系来实现 DSCP 与 threshold 的映射

管理员可以通过配置 CoS-Threshold 和 CoS-Queue 的映射关系来实现 Queue 与 threshold 的映射



在 VSU 模式下，管理报文的优先级默认为 7，进入队列 8，不建议更改这个映射关系。

## 2.5 配置详解

配置项	配置建议 & 相关命令	
配置流分类	可选配置。用于创建流分类信息。	
	<b>class-map</b>	创建类
	<b>match access-group</b>	匹配 ACL 规则
	<b>match ip precedence</b>	匹配 IP 报文 PRE 优先级
	<b>match ip dscp</b>	匹配 IP 报文 DSCP 优先级

	<b>policy-map</b>	创建策略
	<b>class</b>	关联类
	<b>police</b>	绑定流的带宽限制与超限后的报文处理行为
	<b>set</b>	绑定修改流的 CoS、DSCP、VID 的行为
	<b>virtual-group</b>	创建/接口加入逻辑端口组
	<b>service-policy</b>	在接口上应用策略
配置报文优先级标记与映射	 可选配置。用于配置接口信任模式、缺省 CoS、各种映射关系。	
	<b>mls qos trust</b>	修改接口的信任模式
	<b>mls qos cos</b>	修改接口缺省 CoS 值
	<b>mls qos map cos-dscp</b>	配置 CoS 到 DSCP 的映射
	<b>mls qos map dscp-cos</b>	配置 DSCP 到 CoS 的映射
	<b>mls qos map ip-precedence-dscp</b>	配置 IP PRE 到 DSCP 的映射
配置端口限速	 可选配置。配置端口的限速。	
	<b>rate-limit</b>	配置端口流量限制
配置拥塞管理	 可选配置。配置 CoS 到队列映射，队列调度策略与轮转权重。	
	<b>priority-queue cos-map</b>	配置 CoS 到队列映射
	<b>priority-queue</b>	配置队列的输出调度策略为 SP
	<b>mls qos scheduler</b>	配置队列的输出调度策略
	<b>wrr-queue bandwidth</b>	配置 WRR 输出队列调度策略的轮转权重
	<b>drr-queue bandwidth</b>	配置 DRR 输出队列调度策略的轮转权重
	<b>wfq-queue bandwidth</b>	配置 WFQ 输出队列调度策略的轮转权重
	<b>qos queue bandwidth</b>	配置队列的最小保证带宽与最大限制带宽
配置拥塞避免	 可选配置。通过设置报文丢弃的方式来避免网络拥塞。	
	<b>queueing wred</b>	开启 WRED 功能
	<b>wrr-queue random-detect min-threshold</b>	配置 WRED 丢弃的低门阈值
	<b>wrr-queue random-detect probability</b>	配置 WRED 丢弃的最大丢弃概率
	<b>wrr-queue cos-map</b>	配置 threshold 到 CoS 的映射

## 2.5.1 配置流分类

### 配置效果

- 创建类，匹配分类规则。
- 创建策略，绑定类与流行为。并关联到接口上。

### 注意事项

- 类与策略的名称不能超过 31 个字符。
- 接口上的配置只支持在 AP 口和以太网口上配置。部分产品支持在 SVI 口上应用策略，即 service-policy 命令。当物理口和 SVI 口都存在策略配置时，物理口的优先级比 SVI 口高。
- 全局配置模式下应用策略，即 service-policy 命令，所有支持配置策略的接口都应用策略。

## 配置方法

### 创建类，匹配规则

- 可选配置。
- 创建类，在类配置模式下，匹配 ACL、IP PRE、DSCP 中的一个。

### 创建策略

- 可选配置。
- 创建策略，在策略配置模式下，绑定类与流行为。

### 创建并将接口加入逻辑端口组

- 可选配置。
- 创建逻辑端口组，将接口加入逻辑端口组。

### 配置接口上应用策略

- 可选配置。
- 将配置好的策略关联到指定的接口或逻辑端口组上。

## 检验方法

- 使用 **show class-map** 命令，可以查看类是否创建成功，规则是否匹配成功。
- 使用 **show policy-map** 命令，可以查看策略是否创建成功，类与流行为是否绑定成功。
- 使用 **show mls qos interface** 命令，可以查看接口上是否关联策略。
- 使用 **show virtual-group** 命令，可以查看逻辑接口组下的接口。
- 使用 **show mls qos virtual-group** 命令，可以查看逻辑接口组上是否关联策略。

## 相关命令

### 创建类

- 【命令格式】 **class-map** *class-map-name*
- 【参数说明】 *class-map-name*：要创建的类的名字，名称不能超过 31 个字符。
- 【命令模式】 全局模式

【使用指导】 -

#### 匹配 ACL

【命令格式】 **match access-group** *access-list-number*

【参数说明】 *access-list-number* : 要匹配的访问控制列表编号。

【命令模式】 类配置模式

【使用指导】 -

#### 匹配 IP 报文的 PRE

【命令格式】 **match ip precedence** *precedence-value... [ precedence-value... ]*

【参数说明】 *precedence -value* : 要匹配的 IP PRE , 取值范围为 0~7。

【命令模式】 类配置模式

【使用指导】 -

#### 匹配 IP 报文的 DSCP

【命令格式】 **match ip dscp** *dscp-value... [ dscp-value... ]*

【参数说明】 *dscp -value* : 要匹配的 DSCP , 取值范围为 0~63。

【命令模式】 类配置模式

【使用指导】 -

#### 创建策略

【命令格式】 **policy-map** *policy-map-name*

【参数说明】 *policy-map-name* : 要创建的策略的名字, 名称不能超过 31 个字符。

【命令模式】 全局模式

【使用指导】 -

#### 关联类

【命令格式】 **class** *class-map-name*

【参数说明】 *class-map-name* : 要关联的类名字。

【命令模式】 策略配置模式

【使用指导】 -

#### 绑定修改流的 CoS、DSCP、VID 的行为

【命令格式】 **set { ip dscp new-dscp | cos new-cos | vid new-vid }**

【参数说明】 **ip dscp new-dscp** : 修改流的 DSCP 值为 new-dscp , 取值范围为 0~63。

**cos new-cos** : 修改流的 CoS 值为 new-cos , 取值范围为 0~7。

**vid new-vid** : 修改流的 VLAN ID 为 new-vid , 取值范围为 1-4094。

【命令模式】 类配置模式

【使用指导】 -

#### 绑定流的带宽限制与超限后的报文处理行为

【命令格式】 **police** *rate-bps burst-byte* [ **exceed-action** { **drop** | **dscp** *new-dscp* | **cos** *new-cos* [ **none-tos** ] } ]

【参数说明】 *rate-bps*：每秒带宽限制量(KBits)，由产品决定取值范围。

*burst-byte*：突发流量限制值(KBytes)，由产品决定取值范围。

**drop**：丢弃带宽超限部分的报文。

**dscp** *new-dscp*：修改带宽超限部分报文的 DSCP 值为 *new-dscp*，取值范围为 0~63。

**cos** *new-cos*：修改带宽超限部分报文的 CoS 值为 *new-cos*，取值范围为 0~7。

**none-tos**：改变报文 CoS 值时，不修改报文的 DSCP 值。

【命令模式】 类配置模式

【使用指导】 -

## 创建逻辑端口组/接口加入逻辑接口组

【命令格式】 **virtual-group** *virtual-group-number*

【参数说明】 *virtual-group-number*：逻辑端口组号，取值范围 1~128。

【命令模式】 全局模式下创建逻辑端口组/接口模式将接口加入逻辑端口组，如果逻辑接口组不存在，则先创建逻辑接口组，再将接口加入。

【使用指导】 -

## 在接口上应用策略

【命令格式】 **service-policy** { **input** | **output** } *policy-map-name*

【参数说明】 **input**：接口的输入方向；

**output**：接口的输出方向；

*policy-map-name*：要应用在接口上的策略名。

【命令模式】 接口模式或全局模式

【使用指导】 -

## 配置举例

### 创建 4 个流分类，分别匹配 ACL、IP PRE、DSCP。

- 【配置方法】
- 创建 ACL 规则
  - 创建 4 个流分类，分别匹配 ACL、DSCP、IP PRE

```
Ruijie# configure terminal
Ruijie(config)# access-list 11 permit host 192.168.23.61
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match access-group 11
Ruijie(config-cmap)# exit
Ruijie(config)# class-map cmap2
Ruijie(config-cmap)# match ip dscp 21
Ruijie(config-cmap)# exit
Ruijie(config)# class-map cmap3
Ruijie(config-cmap)# match ip precedence 5
Ruijie(config-cmap)# exit
```

【检验方法】 ● 检查创建的 ACL 规则、流分类规则是否成功。

```
Ruijie# show access-lists
ip access-list standard 11
10 permit host 192.168.23.61
```

```
Ruijie# show class-map
Class Map cmap1
Match access-group 11
Class Map cmap2
Match ip dscp 21
Class Map cmap3
Match ip precedence 5
```

➤ 创建策略，绑定类与流行为，并关联到接口上。

- 【配置方法】 ● 创建流分类 cmap1，匹配 DSCP 值为 18 的报文；创建 cmap2，匹配 IP PRE 为 7 的报文；
- 创建策略 pmap1，关联 cmap1，绑定其行为为修改流的 CoS 为 6；关联 cmap2，绑定其行为为修改流的 DSCP 为 15，并限制其每秒流量为 10000 KBits，触发流量为每秒 1024 KBits，修改超限流量的 DSCP 值为 7；
  - 将策略 pmap1 应用在接口 gigabitEthernet 0/0 的出口上；
  - 创建虚拟逻辑组 1，并将接口 gigabitEthernet 0/1、gigabitEthernet 0/2 加入，将策略 pmap1 应用在虚拟逻辑组的入口上。

```
Ruijie# configure terminal
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match ip dscp 18
Ruijie(config-cmap)# exit
Ruijie(config)# class-map cmap2
Ruijie(config-cmap)# match ip precedence 7
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map pmap1
Ruijie(config-pmap)# class cmap1
Ruijie(config-pmap-c)# set cos 6
Ruijie(config-pmap-c)# exit
Ruijie(config-cmap)# class cmap2
Ruijie(config-pmap-c)# set ip dscp 15
Ruijie(config-pmap-c)# police 10000 1024 exceed-action dscp 7
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# exit
Ruijie(config)# interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# service-policy output pmap1
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface gigabitEthernet 0/1
```

```

Ruijie(config-if-GigabitEthernet 0/1)# virtual-group 1
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# virtual-group 1
Ruijie(config-if-GigabitEthernet 0/2)# exit
Ruijie(config)# virtual-group 1
Ruijie(config-VirtualGroup)# service-policy input pmap1
Ruijie(config-VirtualGroup)# exit

```

#### 【检验方法】

- 检查流分类规则是否创建成功；
- 检查策略是否创建成功，并成功绑定流与流行为；
- 检查策略是否应用到接口上；
- 检查逻辑接口组是否创建成功，关联上接口，并成功应用上策略。

```
Ruijie# show class-map
```

```

Class Map cmap1
  Match ip dscp 18
Class Map cmap2
  Match ip precedence 7

```

```
Ruijie# show policy-map
```

```

Policy Map pmap1
  Class cmap1
    set cos 6
  Class cmap2
    set ip dscp 15
    police 10000 1024 exceed-action dscp 7

```

```
Ruijie# show mls qos interface gigabitEthernet 0/0
```

```

Interface: GigabitEthernet 0/0
Ratelimit input:
Ratelimit output:
Attached input  policy-map:
Attached output policy-map: pmap1
Default trust: none
Default cos: 0

```

```
Ruijie# show virtual-group 1
```

virtual-group	member
1	Gi0/1 Gi0/2

```
Ruijie# show mls qos virtual-group 1
```

```

Virtual-group: 1
Attached input policy-map: pmap1

```

## 2.5.2 配置报文优先级标记与映射

### 配置效果

---

- 配置接口的信任模式，默认 CoS 值。
- 配置 CoS-to-DSCP、DSCP-to-CoS、IP-PRE-to-DSCP 映射关系。

### 注意事项

---

- 接口上的配置只支持在 AP 口和以太网口上配置。

### 配置方法

---

#### 配置接口的信任模式、默认 CoS 值

- 可选配置。
- 在接口模式下，可配置接口的信任模式与默认 CoS 值。

#### 配置 CoS-to-DSCP、DSCP-to-CoS、IP-PRE-to-DSCP 映射关系

- 可选配置。
- 配置各种映射关系。

### 检验方法

---

- 使用 **show mls qos interface** 命令，可以查看接口的信任模式、默认 CoS 值。
- 使用 **show mls qos maps** 命令，可以查看 CoS-to-DSCP、DSCP-to-CoS、IP-PRE-to-DSCP 映射关系。

### 相关命令

---

#### 配置接口的信任模式

- 【命令格式】 **mls qos trust { cos | ip-precedence | dscp }**
- 【参数说明】 **cos**：配置接口的信任模式为 CoS；  
**ip-precedence**：配置接口的信任模式为 IP PRE；  
**dscp**：配置接口的信任模式为 DSCP。
- 【命令模式】 接口模式
- 【使用指导】 -

#### 配置接口的缺省 CoS 值

- 【命令格式】 **mls qos cos default-cos**



- 【参数说明】 *default-cos* : 所要配置的缺省 CoS 值, 默认值为 0, 取值范围为 0~7。
- 【命令模式】 接口模式
- 【使用指导】 -

#### 配置 CoS-to-DSCP MAP

- 【命令格式】 **mls qos map cos-dscp dscp1...dscp8**
- 【参数说明】 *dscp1...dscp8* : CoS 所映射的 DSCP 值, 缺省 CoS 0~7 分别映射到 DSCP 0 8 16 24 32 40 48 56, DSCP 取值范围为 0~63。
- 【命令模式】 全局模式
- 【使用指导】 -

#### 配置 DSCP-to-CoS MAP

- 【命令格式】 **mls qos map dscp-cos dscp-list to cos**
- 【参数说明】 *dscp-list* : 要映射到 CoS 的 DSCP 列表, 缺省 DSCP 0~7 映射到 CoS 0, DSCP 8~15 映射到 CoS 1, DSCP 16~23 映射到 CoS 2, DSCP 24~31 映射到 CoS 3, DSCP 32~39 映射到 CoS 4, DSCP 40~47 映射到 CoS 5, DSCP 48~55 映射到 CoS 6, DSCP 56~63 映射到 CoS 7, DSCP 取值范围为 0~63。  
*cos* : *dscp-list* 所要映射到的 CoS, 取值范围为 0~7。
- 【命令模式】 全局模式
- 【使用指导】 -

#### 配置 IP-PRE-to-DSCP MAP

- 【命令格式】 **mls qos map ip-prec-dscp dscp1...dscp8**
- 【参数说明】 *dscp1...dscp8* : IP PRE 所映射的 DSCP 值, 缺省 IP PRE 0~7 分别映射到 DSCP 0 8 16 24 32 40 48 56, DSCP 取值范围为 0~63。
- 【命令模式】 全局模式
- 【使用指导】 -

## 配置举例

#### 配置接口的信任模式, 默认 CoS 值。

- 【配置方法】
- 修改接口 gigabitEthernet 0/0 的信任模式为信任 DSCP ;
  - 修改接口 gigabitEthernet 0/1 的默认 CoS 值为 7。

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# mls qos trust dscp
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mls qos cos 7
Ruijie(config-if-GigabitEthernet 0/1)# exit
```

- 【检验方法】
- 检查接口配置, 信任模式与默认 CoS 是否配置成功。

```

Ruijie# show mls qos interface gigabitEthernet 0/0
Interface: GigabitEthernet 0/0
Ratelimit input:
Ratelimit output:
Attached input  policy-map:
Attached output policy-map:
Default trust: dscp
Default cos: 0
Ruijie# show mls qos interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Ratelimit input:
Ratelimit output:
Attached input  policy-map:
Attached output policy-map:
Default trust: none
Default cos: 7

```

#### 配置 CoS-to-DSCP、DSCP-to-CoS、IP-PRE-to-DSCP 映射关系。

- 【配置方法】
- 配置 CoS-to-DSCP 将 CoS 0 1 2 3 4 5 6 7 分别映射到 DSCP 7 14 21 28 35 42 49 56；
  - 配置 DSCP-to-CoS 将 DSCP 0 1 2 3 4 映射到 CoS 4，将 DSCP 11 12 13 14 映射到 CoS 7；
  - 配置 IP-PRE-to-DSCP 将 IP PRE 0 1 2 3 4 5 6 7 分别映射到 DSCP 31 26 21 15 19 45 47 61；

```

Ruijie# configure terminal
Ruijie(config)# mls qos map cos-dscp 7 14 21 28 35 42 49 56
Ruijie(config)# mls qos map dscp-cos 0 1 2 3 4 to 4
Ruijie(config)# mls qos map dscp-cos 11 12 13 14 to 7
Ruijie(config)# mls qos map ip-precedence-dscp 31 26 21 15 19 45 47 61

```

- 【检验方法】
- 检查各映射关系是否配置成功。

```

Ruijie# show mls qos maps cos-dscp
cos dscp
----
0    7
1    14
2    21
3    28
4    35
5    42
6    49
7    56
Ruijie# show mls qos maps dscp-cos
dscp cos      dscp cos      dscp cos      dscp cos

```

```

-----
0 4      1 4      2 4      3 4
4 4      5 0      6 0      7 0
8 1      9 1     10 1     11 7
12 7     13 7     14 7     15 1
16 2     17 2     18 2     19 2
20 2     21 2     22 2     23 2
24 3     25 3     26 3     27 3
28 3     29 3     30 3     31 3
32 4     33 4     34 4     35 4
36 4     37 4     38 4     39 4
40 5     41 5     42 5     43 5
44 5     45 5     46 5     47 5
48 6     49 6     50 6     51 6
52 6     53 6     54 6     55 6
56 7     57 7     58 7     59 7
60 7     61 7     62 7     63 7

Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp
-----
0 31
1 26
2 21
3 15
4 19
5 45
6 47
7 61

```

### 2.5.3 配置端口限速

#### 配置效果

- 配置端口的流量限制。

#### 注意事项

- 支持在以太网口和聚合口上配置。

#### 配置方法

## 配置端口的流量限制

- 可选配置。
- 可以配置端口上允许通过的流量与突发流量的限制值。

## 检验方法

- 使用 **show mls qos rate-limit** 命令，可以查看端口的限速信息

## 相关命令

### 配置端口的流量限制

【命令格式】 **rate-limit { input | output } bps burst-size**

【参数说明】 **input**：接口的输入方向。

**output**：接口的输出方向。

**bps**：每秒钟的带宽限制量(KBits)，取值范围依产品而定。

**burst-size**：突发流量限制值(Kbytes)，取值范围依产品而定。

【命令模式】 接口模式

【使用指导】 -

## 配置举例

### 以典型应用---端口限速+优先级重标记应用为例。

- 【配置方法】
- 对于出口访问 Internet，在端口 G0/24 上配置端口的出口流量限制，带宽限制每秒 102400KBits，突发流量限制每秒 256Kbytes；
  - 对于宿舍楼，在端口 G0/3 上配置端口的入口流量限制，带宽限制每秒 51200KBits，突发流量限制每秒 256Kbytes；
  - 对于教学楼，在端口 G0/1 上配置端口的入口流量限制，带宽限制每秒 30720KBits，突发流量限制每秒 256Kbytes；
  - 对于实验楼，创建类 cmap\_dscp7 匹配 DSCP 优先级 7，创建策略 pmap\_shiyan，关联 cmap\_dscp7，绑定流行为为将速度超过 20M 的报文的 DSCP 值改为 16；将 pmap\_shiyan 应用在接口 G0/2 上，并配置接口信任 DSCP。

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/24
Ruijie(config-if-GigabitEthernet 0/24)# rate-limit output 102400 256
Ruijie(config-if-GigabitEthernet 0/24)# exit
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)# rate-limit input 51200 256
Ruijie(config-if-GigabitEthernet 0/3)# exit
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1# rate-limit input 30720 256
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# class-map cmap_dscp7
Ruijie(config-cmap)# match ip dscp 7
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map pmap_shiyan
Ruijie(config-pmap)# class cmap_dscp7
Ruijie(config-pmap-c)# police 20480 128 exceed-action dscp 16
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2# service-policy input pmap_shiyan
Ruijie(config-if-GigabitEthernet 0/2)# mls qos trust dscp
Ruijie(config-if-GigabitEthernet 0/2)# exit
```

**【检验方法】**

- 检查接口限速配置是否成功;
- 检查类与策略是否创建成功，并成功应用在接口上。

```
Ruijie# show mls qos rate-limit
Interface: GigabitEthernet 0/1
  rate limit input Kbps = 30720 burst = 256
Interface: GigabitEthernet 0/3
  rate limit input Kbps = 51200 burst = 256
Interface: GigabitEthernet 0/24
  rate limit output Kbps = 102400 burst = 256
Ruijie# show class-map cmap_dscp7

Class Map cmap_dscp7
  Match ip dscp 7
Ruijie# show policy-map pmap_shiyan

Policy Map pmap_shiyan
  Class cmap_dscp7
    police 20480 128 exceed-action dscp 16
Ruijie# show mls qos interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map: pmap_shiyan
Attached output policy-map:
Default trust: dscp
Default cos: 0
```

## 2.5.4 配置拥塞管理

### 配置效果

---

- 配置 CoS 到队列映射。
- 配置输出队列调度策略与轮转权重。
- 配置队列的最小保证带宽与最大限制带宽

### 注意事项

---

- 接口上的配置只支持在 AP 口和以太网口上配置。

### 配置方法

---

#### 📌 配置 CoS 到单播、组播队列的映射

- 可选配置。
- 可配置 CoS 到队列的映射；在支持组播队列的产品中，可配置 CoS 到组播队列的映射。

#### 📌 配置单播、组播输出队列的调度策略与轮转权重

- 可选配置。
- 配置输出队列的调度策略，并修改轮转权重；在支持组播队列的产品中，可配置组播队列的调度策略与其轮转权重。

#### 📌 配置队列的最小保证带宽与最大限制带宽

- 可选配置。
- 配置队列的最小保证带宽与最大限制带宽。

### 检验方法

---

- 使用 **show mls qos queueing** 命令，可以查看输出队列信息。
- 使用 **show mls qos scheduler** 命令，可以查看输出队列的调度策略。
- 使用 **show qos bandwidth** 命令，可以查看队列带宽。

### 相关命令

---

#### 📌 配置 CoS-to-Queue MAP

【命令格式】 **priority-queue cos-map** *qid* *cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]

【参数说明】 *qid*：所要映射的队列 ID，取值范围为 1~8。

*cos0~cos7*：所要映射到 *qid* 上的 CoS，缺省 CoS 0~7 分别映射到队列 1~8，取值范围为 0~7。

【命令模式】 全局模式

【使用指导】 -

#### 配置输出队列调度策略为 SP

【命令格式】 **priority-queue**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

#### 配置输出队列调度策略

【命令格式】 **mls qos scheduler { sp | rr | wrr | drr | wfq }**

【参数说明】 **sp**：设置输出队列调度算法为绝对优先级调度；

**rr**：配置输出队列的调度策略为轮转调度

**wrr**：设置输出队列调度算法为带帧数量权重轮转调度；

**drr**：设置输出队列调度算法为带帧长度权重轮转调度；

**wfq**：设置输出队列调度算法为加权公平队列调度。

【命令模式】 全局模式

【使用指导】 -

#### 配置输出队列调度策略轮转权重

【命令格式】 **{ drr-queue | wrr-queue | wfq-queue } bandwidth weight1...weight8**

【参数说明】 **drr-queue**：DRR 输出队列调度策略的轮转权重；

**wrr-queue**：WRR 输出队列调度策略的轮转权重；

**wfq-queue**：WFQ 输出队列调度策略的轮转权重。

*weight1...weight8*：输出队列 1~8 的权重，取值范围依产品而定，取值为 0 表示该队列采用 SP 调度，缺省全局/接口队列权重比皆为 1:1。

【命令模式】 全局模式/接口模式

【使用指导】 -

#### 配置队列的最小保证带宽与最大限制带宽

【命令格式】 **qos queue queue-id bandwidth { minimum | maximum } bandwidth**

【参数说明】 *queue-id*：所要配置的队列 ID，取值范围为 1~8。

**minimum bandwidth**：最小保证带宽 Kbps，取值范围依产品而定，缺省没有配置。

**maximum bandwidth**：最大限制带宽 Kbps，取值范围依产品而定，缺省没有配置。

【命令模式】 接口模式

【使用指导】 -

### 配置举例

#### 配置 CoS 到队列映射，修改调度策略与其轮转权重。

- 【配置方法】
- 配置 CoS 到队列的映射为 CoS 值 0 1 2 3 4 5 6 7 分别映射到队列 1 2 5 5 5 5 7 8；
  - 配置队列的输出调度策略为 DRR，轮转权重为 2:1:1:1:6:6:6:8。

```
Ruijie# configure terminal
Ruijie(config)# priority-queue cos-map 5 2 3 4 5
Ruijie(config)# mls qos scheduler drr
Ruijie(config)# drr-queue bandwidth 2 1 1 1 6 6 6 8
```

- 【检验方法】
- 检测 CoS 到队列是否映射成功，队列输出调度策略与轮转权重是否配置成功。

```
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
  Deficit Round Robin
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0    1
1    2
2    5
3    5
4    5
5    5
6    7
7    8

wrr bandwidth weights:
qid weights
---
1    1
2    1
3    1
4    1
5    1
6    1
7    1
8    1

drr bandwidth weights:
qid weights
---
1    2
2    1
```



```

3 1
4 1
5 6
6 6
7 6
8 8

wfq bandwidth weights:
qid weights
----
1 1
2 1
3 1
4 1
5 1
6 1
7 1
8 1

```

#### 以典型应用——优先级重标记+队列调度应用为例。

- 【配置方法】
- 创建访问各类服务器的 ACL，并创建类匹配这些 ACL。
  - 创建策略，关联各个类，为访问各类服务器的报文重新指定 CoS。并将其关联到研发部和市场部的入口上，配置端口信任 CoS。
  - 配置人事管理部端口的缺省 CoS 为最高优先级 7，优先保障人事部发出的报文。
  - 配置队列的输出调度策略为 WRR，轮转权重为 1:1:1:2:6:1:1:0，即对人事管理部报文实行 SP 调度，对研发部与市场部访问邮件数据库、文件数据库、工资查询数据库的报文按照 6 : 2 : 1 的比例来调度

```

Ruijie# configure terminal
Ruijie(config)# ip access-list extended salary
Ruijie(config-ext-nacl)# permit ip any host 192.168.10.1
Ruijie(config-ext-nacl)# exit
Ruijie(config)# ip access-list extended mail
Ruijie(config-ext-nacl)# permit ip any host 192.168.10.2
Ruijie(config-ext-nacl)# exit
Ruijie(config)# ip access-list extended file
Ruijie(config-ext-nacl)# permit ip any host 192.168.10.3
Ruijie(config-ext-nacl)# exit
Ruijie(config)# class-map salary
Ruijie(config-cmap)# match access-group salary
Ruijie(config-cmap)# exit
Ruijie(config)# class-map mail
Ruijie(config-cmap)# match access-group mail

```

```

Ruijie(config-cmap)# exit
Ruijie(config)# class-map file
Ruijie(config-cmap)# match access-group file
Ruijie(config)# policy-map toserver
Ruijie(config-pmap)# class mail
Ruijie(config-pmap-c)# set cos 4
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# class file
Ruijie(config-pmap-c)# set cos 3
Ruijie(config-pmap-c)# exit
Ruijie(config-pmap)# class salary
Ruijie(config-pmap-c)# set cos 2
Ruijie(config-pmap-c)# end
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# service-policy input toserver
Ruijie(config-if-GigabitEthernet 0/1)# mls qos trust cos
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# service-policy input toserver
Ruijie(config-if-GigabitEthernet 0/2)# mls qos trust cos
Ruijie(config-if-GigabitEthernet 0/2)# exit
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)# mls qos cos 7
Ruijie(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 0
Ruijie(config)#mls qos scheduler wrr

```

**【检验方法】**

- 检查 ACL 是否创建成功，类是否成功关联 ACL；
- 检查策略是否创建成功，类与流行为是否绑定成功，策略是否成功应用在接口上；
- 检查接口默认 CoS 是否配置成功，调度策略与轮转权重是否配置成功。

```

Ruijie# show access-lists

ip access-list extended file
 10 permit ip any host 192.168.10.3

ip access-list extended mail
 10 permit ip any host 192.168.10.2

ip access-list extended salary
 10 permit ip any host 192.168.10.1
Ruijie# show class-map

```

```
Class Map salary
  Match access-group salary
Class Map mail
  Match access-group mail
Class Map file
  Match access-group file
Ruijie# show policy-map

Policy Map toserver
  Class mail
    set cos 4
  Class file
    set cos 3
  Class salary
    set cos 2
Ruijie# show mls qos interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Ratelimit input:
Ratelimit output:
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
Ruijie# show mls qos interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
Ruijie# show mls qos interface gigabitEthernet 0/3
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map:
Attached output policy-map:
Default trust: none
Default cos: 7
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
```

```
Weighted Round Robin
Ruijie# Ruijie#show mls qos queueing
Cos-queue map:
cos qid
----
0    1
1    2
2    3
3    4
4    5
5    6
6    7
7    8

wrr bandwidth weights:
qid weights
----
1    1
2    1
3    1
4    2
5    6
6    1
7    1
8    0

drr bandwidth weights:
qid weights
----
1    1
2    1
3    1
4    1
5    1
6    1
7    1
8    1

wfq bandwidth weights:
qid weights
----
```

1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1

## 2.5.5 配置拥塞避免

### 配置效果

- 配置 WRED 的低门阈值，当队列中报文的长度小于低门阈值时，不丢弃报文。
- 配置最大丢弃概率，当队列中报文的长度在低门阈值和高门阈值之间时，随机丢弃报文，此项配置了丢弃的最大概率。
- 配置 CoS 值与门阈值的映射关系。

### 注意事项

- 接口上的配置只支持在 AP 口和以太网口上配置。

### 配置方法

#### 📌 开启 WRED 功能

- 可选配置。
- 如果需要 WRED 功能，则开启。

#### 📌 配置低门阈值

- 可选配置。
- 如需修改低门阈值，则配置。

#### 📌 配置最大丢弃概率

- 可选配置。
- 如需修改最大丢弃概率，则配置。

#### 📌 配置 CoS 与门阈值的映射

- 可选配置。
- 如需修改 CoS 与门阈值的映射关系，则配置。

## 检验方法

- 使用 **show queueing wred interface** 命令，查看 WRED 配置信息。

## 相关命令

### ✚ 开启 WRED 功能

- 【命令格式】 **queueing wred**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

### ✚ 配置低门阈值

- 【命令格式】 **wrr-queue random-detect min-threshold** *queue\_id* *thr1* [*thr2*]
- 【参数说明】 *queue\_id*：接口队列 ID，取值范围为 1~8。  
*thrN*：支持 2 组低门阈值，取值范围为 1~100。
- 【命令模式】 接口模式
- 【使用指导】 -

### ✚ 配置最大丢弃概率

- 【命令格式】 **wrr-queue random-detect probability** *queue\_id* *prob1* [*prob2*]
- 【参数说明】 *queue\_id*：接口队列 ID，取值范围为 1~8。  
*probN*：支持 2 组最大丢弃概率，取值范围为 1~100。
- 【命令模式】 接口模式
- 【使用指导】 -

## 2.6 监视与维护

### 清除各类信息


-

### 查看运行情况

作用	命令
显示流分类信息	<b>show class-map</b> [ <i>class-map-name</i> ]
显示 QoS 策略信息	<b>show policy-map</b> [ <i>policy-map-name</i> [ <b>class</b> <i>class-map-name</i> ]]
显示接口上应用的策略信息	<b>show policy-map interface</b> <i>interface-id</i>
显示逻辑端口组信息	<b>show virtual-group</b> [ <i>virtual-group-number</i>   <b>summary</b> ]

显示逻辑端口组应用的策略信息	<b>show mls qos virtual-group</b> [ <i>virtual-group-number</i>   <b>policers</b> ]
显示各类映射	<b>show mls qos maps</b> [ <b>cos-dscp</b>   <b>dscp-cos</b>   <b>ip-prec-dscp</b> ]
显示端口速度限制信息	<b>show mls qos rate-limit</b> [ <b>interface</b> <i>interface-id</i> ]
显示 QoS 队列、调度策略轮转权重信息	<b>show mls qos queueing</b>
显示输出队列调度策略信息	<b>show mls qos scheduler</b>
显示 WRED 的配置信息	<b>show queueing wred interface</b> <i>interface-id</i>
显示接口的 QoS 信息	<b>show mls qos interface</b> <i>interface-id</i> [ <b>policers</b> ]
显示队列带宽信息	<b>show qos bandwidth</b> [ <b>interfaces</b> <i>interface-id</i> ]

## 查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 QoS 库的调试开关。	<b>debug qos lib</b> [ <b>event</b>   <b>message</b> ]
打开 QoS 通信服务端的调试开关	<b>debug qos server</b> [ <b>event</b>   <b>message</b> ]
打开 QoS 用户命令处理的调试开关	<b>debug qos mls</b>
打开与 VMSUP 相关配置的调试开关	<b>debug qos vmsup</b>

## 3 MMU

### 3.1 概述

MMU(Memory Management Unit ,缓存管理单元) 指的是对芯片缓存进行合理的分配,从而使得交换设备能更好应对各种突发流量。

网络中存在的不总是平稳的流量,也存在各式各样的突发流量。当网络流量平稳且带宽足够时,所有的数据流都得到了较好的处理;当网络存在突发流量时,即使平均的流量速率不超过带宽,也可能发生数据流丢弃。

数据报文进入交换设备中,在转发之前,都会被存储在交换设备的缓存当中。正常情况下,数据报文在缓存中的驻留时间很短,在微秒级别内就被转发出去;当存在突发流量的情况下,如果突发流量的瞬时速率超过交换设备的处理能力,那么来不及处理的数据报文就在交换设备的缓存中堆积,一旦缓存不足就会发生丢包。此时 MMU 就应运而生,可以通过合理的配置缓存来为不同的业务分配不同的缓存使用量,从而达到优化网络的目的。

### 3.2 典型应用

典型应用	场景描述
基于出口队列的大缓存应用	某企业在网盘业务中,需要有足够大的缓存,来保证业务流量不丢包。

#### 3.2.1 基于出口队列的大缓存应用

##### 应用场景

某企业在网盘业务中,需要有足够大的缓存,来保证业务流量不丢包。

如下图所示:设备 A 与 5 台客户端、35 台业务服务器相连,其中 15 台业务服务器虚拟出 15 台前置服务器。

主要业务流如下:

- 客户端服务器向前置服务器发送请求报文。
- 前置服务器把收到的请求报文发送给业务服务器。
- 业务服务器收到请求报文,会发送应答报文给前置服务器。
- 前置服务器收到应答报文之后,会把报文发送给客户端服务器。
- 客户端收到应答报文表示一个会话创建成功。

该业务模型下,存在多对一的流量传输方式:

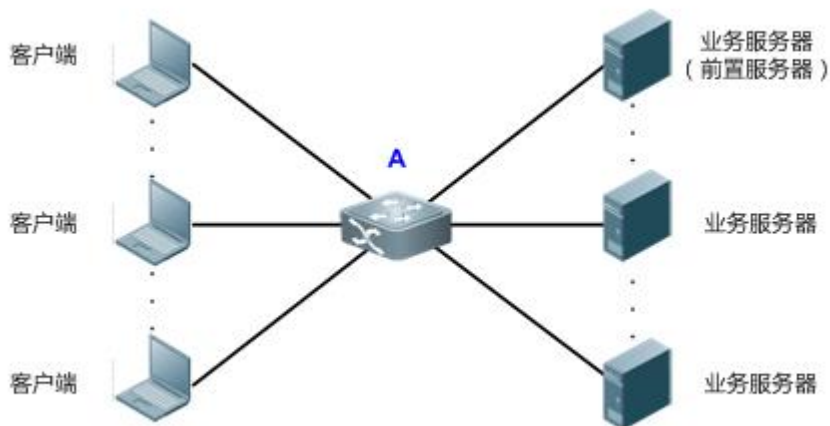
- 多台客户端的请求流量发送给一台前置服务器。
- 多台前置服务器的请求流量发送给一台业务服务器。



- 多台业务服务器的应答流量发送给一台前置服务器。
- 多台前置服务器的应答流量发送给一台客户端。


这些流量基本都是通过设备 A 进行传输，容易造成网络拥塞。通过在设备上配置大缓存，可解决此类问题。

图 3-1



## 功能部属

- 在所有业务口（即连接客户端和服务器的端口）中，把业务所在的队列的共享缓存配置成 100%。
- 在所有业务口中，把不使用的队列的保证缓存配置成最小值。
- 在所有不使用的端口中，把所有队列的保证缓存配置成最小值。

 具体配置可参见配置详解中的配置举例。

## 3.3 功能详解

### 基本概念

#### Cell

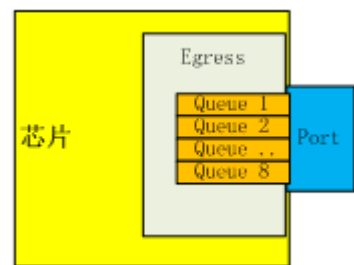
Cell 是缓存的单位，是交换设备存储报文的最小单元。每个 cell 的大小依产品的不同而不同。1 个报文可以使用多个 cell，1 个 cell 只能被 1 个报文使用。

#### 端口组 (Port Group)

物理上属于同一个交换芯片的所有端口称为一个端口组，交换设备的缓存管理都是在端口组内进行管理。如板卡 M18000\_40XS\_CB，该版本有 2 个交换芯片，因此有 2 个端口组，前 20 个端口为 Port Group 1，后 20 个端口为 Port Group 2。

➤ 出口队列

端口出口队列被划分成单播队列和组播队列（队列个数依产品而定）。交换芯片逻辑上分成 Ingress(入方向)和 Egress(出方向)，出口队列处于 Egress 方向。报文从出口出去之前，都要在出口队列进行入队操作。我司有一部分产品是基于出口队列进行缓存管理。



当前总共有 3 种出口队列的模型：

- 出口 8 个单播队列，8 个组播队列。知名单播报文走单播队列，除此之外的报文都走组播队列。
- 出口 8 个单播队列，4 个组播队列。知名单播报文走单播队列，除此之外的报文都走组播队列。
- 出口只有 8 个队列，没有区分单播组播。

功能特性

功能特性	作用
<a href="#">缓存调整</a>	基于队列对缓存进行一定的调整，它是 MMU 的基础。
<a href="#">缓存监控</a>	缓存监控实际上就是对缓存量使用的进行监控，从而有有利于进行缓存调整。
<a href="#">队列统计</a>	对各个队列的收发包进行统计，从而有有利于查看缓存调整的结果。

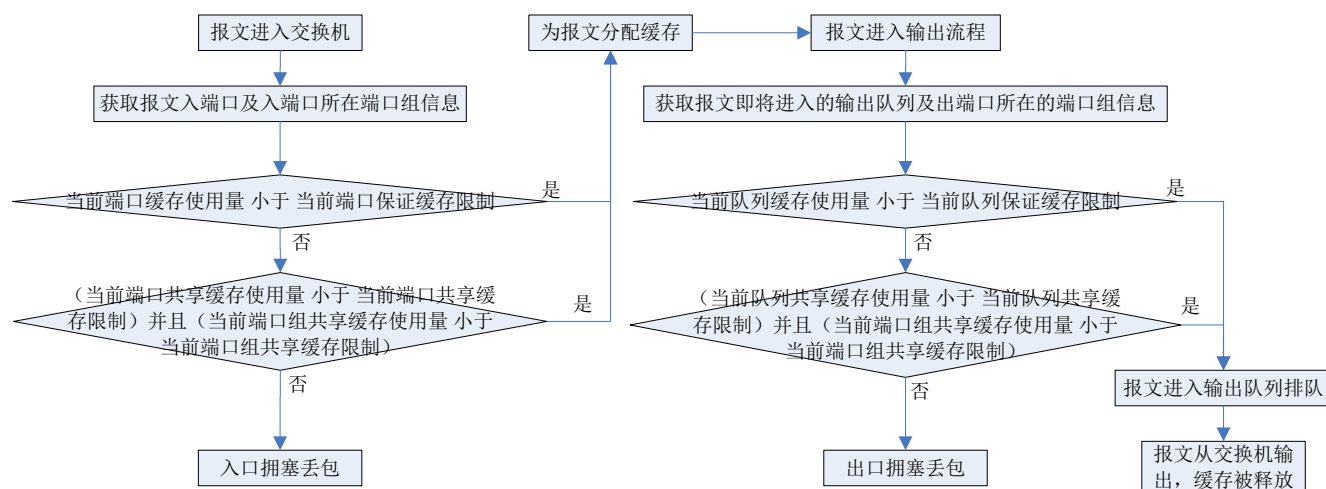
3.3.1 缓存调整

缓存调整通过对队列的缓存进行一定的调整，从而使得各个业务所在队列拥有不同的缓存使用量，从而区分对待各个业务，为不同优先级的业务提供不同的服务。

工作原理

➤ 缓存在硬件的工作机制

在硬件上缓存分输入和输出两个方向进行管理，处理机制如下图所示：



由于在缓存管理时，输入方向都调成最大值从而保证输入方向不丢包，让丢包发生在输出方向。因此输入方向的缓存不开放调整，CLI 仅提供输出方向的缓存调整，包括队列保证缓存和队列共享缓存。缓存调整通过配置队列的保证缓存门限和共享缓存门限来使得各个队列拥有不同的缓存使用量。

## 保证缓存

保证缓存也称之为独享缓存，这部分缓存是基于各个队列进行分配，某个队列的保证缓存只能由该队列使用，其他队列无法使用。每个队列默认都会分配一定量的保证缓存，这部分缓存可以让该队列在平稳流量下正常线速转发报文。

## 缓存模式

缓存模式是一个全局的概念，是基于所有面板口的所有队列调整保证缓存。当前支持配 4 种缓存模式：普通缓存模式，Burst 增强缓存模式（即大缓存模式），QoS 增强缓存模式（即小缓存模式），流控增强缓存模式。

这 4 种缓存模式对应的队列保证缓存具体值依产品而定，几种模式的缓存管理特征及适用场景分别如下：

### 普通缓存模式

该模式兼顾考虑了交换机的突发大流量缓存能力、QoS 调度支持、流控支持三方面因素。对以上三方面的支持比较均衡，没有特别的偏向，因此支持程度都是适中。

#### ● 适用环境：

- 对缓存无特别需求的环境。因为该模式缓存管理较为中庸，兼顾考虑了各方面因素，出问题的概率较小；
- 存在低速口且低速口正常工作不处于休眠状态的环境。所谓低速口是指，端口形态为万兆加千兆的设备上出现协商为百兆的端口，或者端口形态为千兆加百兆的设备上出现协商为十兆的端口；
- 部署 QoS 的环境。可以中等程度支持，表现为 1 个端口输入情况下同时有 5 个端口拥塞才会出现入口丢包进而 QoS 失效；
- 部署流控的环境。可以中低程度支持，表现为 4 个端口同时打 1 个端口才会出现出口丢包进而流控失效；

#### ● 不适用环境：

- 具有特别明显的突发大流量特征的环境不适用，因为该模式下 Burst 缓存能力适中；
- 没有部署流控但又对丢包容忍度较低的环境不适用，因为该模式下考虑对 QoS 中等支持，而 QoS 的特征即丢包；

#### ● 典型应用：

- 园区网环境。主要特征有：环境开放可能随时接入低速终端，对丢包容忍度较高（根据经验值，可以忍受 1%~2% 的丢包率）；

### Burst 增强缓存模式

该模式主要基于普通缓存模式考虑的三方面因素对交换机的突发大流量缓存能力做增强支持,即 Burst 增强。由于 Burst、QoS、流控支持之间存在一定的矛盾互斥关系,因此在 Burst 增强模式下,QoS 和流控支持会适当减弱。Burst 增强模式的缓存配置特征主要是将输出队列缓存限制得比较大,提高单个端口队列及整机的缓存能力,同时也能支持流控及 QoS。

- 适用环境：

- 拓扑稳定,接入到交换机的设备类型固定,交换机上不会随便接入低速网卡终端设备；
- 具有特别明显的突发大流量特征的环境；
- 对丢包容忍度较低的环境,因为单个队列缓存能力配置得尽量大,即使不开流控,也可以通过缓存来减少丢包；
- 部署 QoS 的环境。但只能弱支持,表现为一个端口输入情况下同时有 2 个端口拥塞就会出现入口丢包进而 QoS 失效；
- 部署流控的环境。但只能弱支持,表现为 2 个端口同时打 1 个端口才会出现出口丢包进而流控失效。在该模式下,流控部署一般建议仅接入交换机的上联口开启流控,而下联口不开启流控；

- 不适用环境：

- 存在低速口的环境（低速口的定义参照以上普通缓存模式里的介绍）。因为该模式下缓存放开共享,单个队列的缓存能力更强,如果存在低速口,则会严重影响非低速口的缓存申请造成非低速口丢包严重的问题；
- 组播网络。原因同存在低速口的情况类似,非组播出口可能受到严重影响；

- 典型应用：

- 广播电视台的非线性编辑网络,配合流控使用（上联口开流控即可）。主要特征有：拓扑稳定,具有特别明显的突发大流量特征,对丢包容忍度很低,没有部署 QoS；
- 广播电视台的 IPQAM 推流网络。主要特征有：具有特别明显的突发大流量特征,对丢包容忍度较低；
- 网络同传环境。主要特征有：接入到交换机的设备类型稳定,没有部署 QoS,对带宽利用率要求较高（缓存放开共享可以提高带宽利用率）；
- 视频监控网络。主要特征有：接入到交换机的设备类型稳定,对丢包容忍度较低；

### QoS 增强模式

该模式主要基于普通缓存模式考虑的三方面因素对 QoS 做增强支持。由于 Burst、QoS、流控支持之间存在一定的矛盾互斥关系,因此在 QoS 增强模式下,Burst 缓存能力和流控支持会适当减弱。QoS 增强模式的缓存配置特征主要是将输出队列缓存限制得比较小,使得出口丢包从而达到区分服务的效果。

- 适用环境：

- 对丢包容忍度较高,且存在较多低速口的环境；
- 部署 QoS 的环境。可以做到强支持,表现为每个出口队列都有保证缓存,以及一个端口输入情况下同时有 15 个端口拥塞才会出现入口丢包进而 QoS 失效；
- 部署流控的环境。但只能弱支持,表现为 2 个端口同时打 1 个端口才会出现出口丢包进而流控失效。但又与 Burst 增强模式下的流控弱支持有区别。Burst 增强模式比 QoS 增强模式在输出方向上缓存能力更强,可以更充分的利用交换机自身的缓存能力,而 QoS 增强模式上开流控则更依赖于上一级设备的缓存能力。

- 不适用环境：

- 部署流控的场景一般不建议使用；

### 流控增强模式

该模式主要基于普通缓存模式考虑的三方面因素对流控做增强支持。由于 Burst、QoS、流控支持之间存在一定的矛盾互斥关系,因此在流控增强模式下,Burst 缓存能力和 QoS 支持会适当减弱。流控增强模式的缓存配置特征主要是输出方向缓存不限制,输入方向限制得比较小,使得输出还没丢包之前输入方向即触发流控确保流控不丢包。

- 适用环境：

- 设备上大部分端口均开启流控的环境。可以做到流控强支持,主要表现为 15 个端口同时打一个端口才会出现出口丢

包进而流控失效；

- 不适用环境：

除了整台设备专门部署流控的环境外建议都不要使用；

### 3.3.2 缓存监控

缓存监控通过对各个队列的使用量进行监控，从而为优化网络，合理配置缓存提供数据支撑。

#### 工作原理

缓存监控通过轮询的方式，定时读取各个队列的缓存使用量及总缓存的使用情况，实时呈现当前设备的缓存使用情况。

##### ▮ 端口组缓存利用率告警门限

当端口组的缓存利用率超过该门限，会打印 syslog 来提醒用户。

##### ▮ 队列缓存利用率告警门限

当队列的缓存利用率超过该门限，会打印 syslog 来提醒用户。

### 3.3.3 流控水线调整

流控水线即用于触发开启流控的端口产生流控帧的入口缓存阈值水线，流控水线调整就是实现对入口缓存阈值的调整。

端口开启流控后，要使流控生效，产生流控帧，需要保证流量在入口拥塞，且占用的缓存数达到端口的缓存阈值。芯片对缓存的管理包含入口缓存与出口缓存，要使入口拥塞产生流控，需要保证端口的入口缓存阈值小于出口队列的缓存阈值。

### 3.3.4 队列统计

队列统计通过对各个队列的转发及丢包数据进行监控，从而为优化网络，合理配置缓存提供数据支撑。

#### 工作原理

队列通过轮询的方式，定时读取各个队列的转发报文个数/字节数和丢包报文个数/字节数，从而通过这些数据计算队列的各种统计数据。

## 3.4 产品说明



S6000E 默认的 buffer 模式为 burst-enhance 模式

## 3.5 配置详解

配置项	配置建议 & 相关命令	
<a href="#">缓存调整</a>	 可选配置。用于配置缓存。	
	<b>mmu queue-guarantee</b>	配置保证缓存
	<b>mmu buffer-mode</b>	配置缓存模式
<a href="#">缓存监控</a>	 可选配置。用于配置缓存。	
	<b>mmu usage-warn-limit</b>	配置缓存利用率告警门限
<a href="#">流控流水线调整</a>	 可选配置。用于配置流控流水线。	
	<b>mmu fc-threshold</b>	<b>mmu fc-threshold</b>

### 3.5.1 缓存调整

#### 配置效果

- 配置保证缓存，可以让队列独享这部分缓存。
- 配置缓存模式，可以全局配置队列缓存大小。

#### 注意事项

- 接口上的配置只支持在物理口上配置。

#### 配置方法

##### 配置保证缓存

- 可选配置。
- 在接口模式下，使用命令 **mmu queue-guarantee**，为各个队列配置保证缓存，保证缓存的配置范围依照产品的不同而不同。
- 可以使用该命令的 **no** 命令或者 **default** 命令来恢复缓存默认值。

【命令格式】 **mmu queue-guarantee output { unicast | multicast } [queue-id1 [queue-id2 [queue-idN]] set value**

【参数说明】 **output**：对出口队列进行缓存管理

**unicast**：对出口单播队列进行缓存管理

**multicast**：对出口组播队列进行缓存管理

**queue-id**：队列号，范围为 1-8

**value**：保证缓存数量，单位为 cell，范围依产品而定。

- 【缺省配置】 缺省情况下，各个队列都分配了一定量的保证缓存，具体指依产品而定。
- 【命令模式】 接口模式
- 【使用指导】 不同的设备，该命令的生效方式不一样，依产品而定。

## 配置缓存模式

- 可选配置。
- 在全局配置模式下，使用命令 **mmu buffer-mode** 配置缓存模式。

【命令格式】 **mmu buffer-mode { normal | burst-enhance | qos-enhance | flowctrl-enhance }**

【参数说明】 **normal**：普通缓存模式

**burst-enhance**：Burst 增强缓存模式

**qos-enhance**：QoS 增强支持缓存模式

**flowctrl-enhance**：流控增强支持缓存模式

【缺省配置】 缺省情况下，缓存模式根据产品本身的定位来定，不同产品默认模式可能不一样。MMU 模式 show run 始终可见。

对于接入或者汇聚交换机，终端比较复杂，normal 模式对 Burst、QoS、流控等有一个比较均衡的考虑，因此默认模式使用 normal 模式。对于数据中心交换机，终端较单纯，低速口可控，对 Burst 要求更大，因此默认采用 Burst 增强模式。

【命令模式】 全局配置模式

【使用指导】 不同的设备，该命令的生效方式不一样，依产品而定。

## 检验方法

- 通过 **show running** 命令查看对应的接口下的 MMU 配置是否成功。

## 配置举例

### 基于出口队列的大缓存配置

- 【配置方法】 ● 配置缓存模式为大缓存，即 Burst 增强。

```
Ruijie# configure terminal
Ruijie(config)#mmu buffer-mode burst-enhance
```

- 【检验方法】 ● 检查创建的保证缓存是否配置成功。

```
Ruijie# show run
Buffer-mode burst-enhance
```

## 3.5.2 缓存监控

### 配置效果

- 配置端口组缓存利用率告警门限，当端口组缓存利用率超过该配置值会打印 log 告警。
- 配置队列缓存利用率告警门限，当队列的缓存利用率超过该配置值会打印 log 告警。

### 注意事项

- 接口上的配置只支持在物理口上配置。

### 配置方法

#### 配置端口组缓存利用率告警门限

- 可选配置。
- 全局配置模式下，使用命令 **mmu usage-warn-limit**，为端口组配置缓存利用率告警门限。
- 可以使用该命令的 **no** 命令或者 **default** 命令来恢复缓存默认值。

【命令格式】 **mmu usage-warn-limit set value**  
【参数说明】 *value*：百分比，1-100。  
【缺省配置】 缺省为 0，表示不告警。  
【命令模式】 全局配置模式  
【使用指导】 1. 该配置对所有端口组生效。

#### 配置队列缓存利用率告警门限

- 可选配置。
- 接口配置模式下，使用命令 **mmu usage-warn-limit { unicast | multicast } [queue-id1 [queue-id2 [queue-idN]] set value**，为各个队列配置缓存利用率告警门限。
- 可以使用该命令的 **no** 命令或者 **default** 命令来恢复缓存默认值。

【命令格式】 **mmu usage-warn-limit { unicast | multicast } [queue-id1 [queue-id2 [queue-idN]] set value**  
【参数说明】 **unicast**：对出口单播队列进行缓存管理  
**multicast**：对出口组播队列进行缓存管理  
*queue-id*：队列号，范围为 1-8  
*value*：百分比，1-100。  
【缺省配置】 缺省为 0，表示不告警。  
【命令模式】 接口配置模式  
【使用指导】



## 检验方法

- 通过 **show running** 命令查看对应的接口下的 MMU 配置是否成功。
- 通过 **show queue-buffer** 查看配置是否成功。

## 配置举例

### 基于端口组配置缓存利用率告警水线

- 【配置方法】 ● 在交换机上配置端口组的缓存利用率告警门限为 80%

```
Ruijie# configure terminal
Ruijie(config)# mmu usage-warn-limit set 80
Ruijie(config)#
```

- 【检验方法】 ● 检查创建的保证缓存是否配置成功。

```
Ruijie# show run
mmu usage-warn-limit set 80
```

### 基于出口队列配置缓存利用率告警水线

- 【配置方法】 ● 在交换机上的端口 1/1 的单播队列 6、8 配置缓存利用率告警门限为 70%

```
Ruijie# configure terminal
Ruijie(config)# int tel/1
Ruijie(config-if)#mmu usage-warn-limit unicast 6 8 set 70
```

- 【检验方法】 ● 检查创建的保证缓存是否配置成功。

```
Ruijie#show queue-buffer interface gigabitEthernet 0/9
```

Dev/slot	Port-group	Total-shared(%)	Guarantee-used(%)	Share-used(%)	Available(%)	Warn-limit(%)
1/-	1	74.5271	0.0822	14.7615	85.1562	NA

```
Interface GigabitEthernet 0/9:
```

Type	Queue	Admin-shared(%)	Total-used(%)	Available(%)	Warn-limit(%)	Peak-usage(%)	Peak-time
Unicast	1	(default)	7.4836	0.0103	NA	7.5041	2015/7/14 20:7:14
Unicast	2	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	3	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	4	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	5	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	6	(default)	0.0000	7.4938	70%	0.0000	NA
Unicast	7	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	8	(default)	0.0000	7.4938	70%	0.0000	NA
Multicast	1	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	2	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	3	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	4	(default)	0.0000	7.4938	NA	0.0000	NA

Multicast	5	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	6	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	7	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	8	(default)	0.0000	7.4938	NA	0.0000	NA

### 3.5.3 流控水线调整

#### 配置效果

- 配置流控水线，可以动态配置各个端口产生流控的入口缓存水线

#### 注意事项

- 只支持在物理口上配置。

#### 配置方法

##### 配置流控水线

- 可选配置。
- 在接口模式下，使用命令 **mmu fc-threshold**，为端口配置流控水线，流控水线的配置范围依照产品的不同而不同。
- 可以使用该命令的 **no** 命令或者 **default** 命令来恢复缓存默认值。

【命令格式】 **mmu fc-threshold set thr%**

【参数说明】 **thr%**：百分比，范围为 1-100

- 【缺省配置】
- 缺省情况下，各个端口都分配了一个产生流控的入口缓存水线，该水线是一个百分比
  - 缺省值依产品及缓存模式而定

【命令模式】 接口模式

【使用指导】 不同的设备，该命令的生效方式不一样，依产品而定。

#### 检验方法

- 通过 **show running** 命令查看对应的接口下的 MMU 配置是否成功。

## 3.6 监视与维护

### 清除各类信息



在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除队列统计值。	<b>clear queue-counter</b>
清除缓存历史峰值	<b>clear queue-buffer peaked</b>

### 查看运行情况

作用	命令
显示面板口缓存使用信息	<b>show queue-buffer interface</b>
显示面板口队列统计信息	<b>show queue-counter interface</b>

### 查看调试信息

-