

目 录

第 4 章 基于类的 QoS 配置	4-1
4.1 简介	4-1
4.2 配置基于复杂流分类的流量策略	4-2
4.2.1 建立配置任务	4-2
4.2.2 定义流分类	4-3
4.2.3 定义流行为并配置动作	4-4
4.2.4 定义流量策略并在策略中为类指定行为	4-5
4.2.5 应用流量策略	4-6
4.2.6 配置逆向地址检查	4-6
4.2.7 检查配置结果	4-7
4.3 配置基于简单流分类的优先级映射	4-7
4.3.1 建立配置任务	4-7
4.3.2 定义 Diff-Serv 域并配置流量策略	4-8
4.3.3 将接口加入 Diff-Serv 域	4-10
4.3.4 配置 E-LSP 流分类	4-10
4.3.5 检查配置结果	4-11
4.4 配置逻辑接口的简单流分类功能	4-11
4.4.1 建立配置任务	4-11
4.4.2 配置 Ring-if 的简单流分类功能	4-12
4.4.3 配置三层 Trunk 的简单流分类功能	4-12
4.4.4 配置二层物理接口和二层 Trunk 的简单流分类功能	4-13
4.4.5 检查配置结果	4-13
4.5 配置举例	4-13
4.5.1 基于复杂流分类流量策略配置示例	4-14
4.5.2 基于简单流分类的优先级映射配置示例	4-18
4.6 故障处理	4-20

第4章 基于类的 QoS 配置

基于类的 QoS 是指通过对流量按照某种规则进行分类，并对同种类型的流量关联某种动作，形成某种策略。将该策略应用后实现基于类的流量监管、流量整形、拥塞避免等功能。

下表列出了本章所包含的主要内容。

如果您需要……	请阅读……
了解基于类的 QoS 需要用到的基本技术	简介
在网络的入口处根据报文的某些参数配置基于流分类的流量策略，对不同的业务提供差别服务	配置任务： 配置基于复杂流分类的流量策略 配置举例： 基于复杂流分类流量策略配置示例
将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的优先级传送	配置任务： 配置基于简单流分类的优先级映射 配置举例： 基于简单流分类的优先级映射配置示例
限制逻辑端口成员的报文拥塞，增加对物理端口报文优先级的限制	配置任务： 配置逻辑接口的简单流分类功能
诊断及排除基于类的 QoS 配置的故障	故障处理

4.1 简介

NE80E 路由器支持 Diff-Serv，向用户提供 EF、AF 等标准的转发服务。这些标准的服务是通过一系列配套的流量管理措施，如流分类、流量监管和整形、拥塞避免等来实现的。

NE80E 路由器的 QoS 实现流量策略、流量整形、拥塞避免以及 IP 域与 MPLS 域间的 QoS 参数映射处理。

流量策略包括基于复杂流分类规则的流量策略、基于简单流分类规则的流量策略和路由器内部的流量策略：

- 基于复杂流分类规则的流量策略是指根据流量所属的类对流量实施流量监管、重新标记、包过滤、策略路由和流量采样等。基于复杂流分类规则的流量策略通常在 Diff-Serv 域的边界路由器上配置。

- 基于简单流分类规则的流量策略是指根据报文所携带的标记信息重新设置服务级别、颜色和丢弃优先级。
- 路由器内部的流量策略是为了避免接口板的流量对主控板所造成的冲击，控制接口板发往主控板的流量，保证主控板处于安全稳定的状态。

 说明：

- Diff-Serv 主要是为 BA 数据流提供带宽上的保证，NE80E 路由器采用预先定义好的队列调度机制为 EF、AF 等不同类型的业务分配资源，用户无须进行队列管理方面的设置。
 - 复杂流分类的优先级高于简单流分类的优先级。
-

4.2 配置基于复杂流分类的流量策略

 说明：

- 除了物理接口，NE80E 还支持在多种逻辑接口上实现复杂流分类，包括子接口、ring-if 和 Trunk 接口。
 - 对于 VLANIF 逻辑接口，不能直接应用流量策略；可以通过物理接口/二层 Eth-Trunk 接口+VLAN ID 范围的方式实现流量策略。
-

4.2.1 建立配置任务

1. 应用环境

在网络的入口处，如果要根据报文的 DSCP 值、协议类型、IP 地址、端口号、分片报文的类型以及时间段等参数对不同的业务提供差别服务，需要配置基于流分类的流量策略。

通常是在相对边界的路由器上配置复杂流分类，在相对核心的路由器上配置简单流分类。

2. 前置任务

在配置基于复杂流分类的流量策略之前，需要完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性
- 配置相关接口的 IP 地址

3. 数据准备

在配置基于复杂流分类的流量策略之前，需准备以下数据：

序号	数据
1	流分类的名称
2	匹配规则中的数据：ACL 号、DSCP 值、802.1p 值、TCP flag 值
3	流行为的名称
4	流行为中的数据：承诺信息速率、峰值信息速率、承诺突发尺寸、最大突发尺寸、DSCP 值、IP 优先级值、EXP 值、802.1p 值、下一跳地址或出接口
5	流量策略名
6	应用流量策略的接口类型及编号

4. 配置过程

序号	过程
1	定义流分类
2	定义流行为并配置动作
3	定义流量策略并在策略中为类指定行为
4	应用流量策略
5	配置逆向地址检查
6	检查配置结果

 说明：

- 如果在行为中配置了逆向地址检查，并将这个行为关联到一个策略上，这个策略已经应用到接口上时，那么逆向地址检查这个功能将对接口上符合类中的流生效。
- 如果对接口上所有的流都使能逆向地址检查，只需在接口配置逆向地址检查。

4.2.2 定义流分类

步骤	操作	命令
1	进入系统视图	system-view
2	定义流分类并进入类视图	traffic classifier classifier-name [operator { and or }]
3	定义 ACL 匹配规则	if-match acl acl-number

步骤	操作	命令
	或定义 DSCP 匹配规则	if-match dscp <i>dscp-value</i>
	或定义 TCP Flag 匹配规则	if-match tcp syn-flag <i>tcpflag-value</i>
	或定义 VLAN 报文的 802.1p 匹配规则	if-match 8021p <i>8021p-value</i>
	或定义报文源 MAC 地址的匹配规则	if-match source-mac <i>mac-address</i>
	或定义报文目的 MAC 地址的匹配规则	if-match destination-mac <i>mac-address</i>
	或定义 IP 报文优先级的匹配规则	if-match ip-precedence <i>ip-precedence</i>
	或定义匹配所有数据包的规则	if-match any

4.2.3 定义流行为并配置动作

步骤	操作	命令
1	进入系统视图	system-view
2	定义行为进入流行为视图	traffic behavior <i>behavior-name</i>
3	配置流量监管动作	car <i>cir</i> <i>cir-value</i> [pir <i>pir-value</i>] [cbs <i>cbs-value</i> pbs <i>pbs-value</i>] [green { discard pass } yellow { discard pass } [red { discard pass }]]]
	或重新设置 DSCP 值	remark dscp <i>dscp-value</i>
	或重新设置 IP 优先级值	remark ip-precedence <i>ip-precedence</i>
	或重新设置 MPLS EXP 值	remark mpls-exp <i>mpls-experimental-value</i>
	或重新设置 VLAN 优先级	remark 8021p <i>8021p-value</i>
	或配置报文的服务等级	service-class <i>service-class</i> color <i>color</i>
	或允许报文通过	permit
	或禁止报文通过	deny
	或配置重定向到下一条地址及出接口	redirect ip-nexthop <i>ip-address</i> [interface <i>interface-type</i> <i>interface-number</i>]
	或配置重定向到多下一跳地址及出接口	redirect ipv4-multinhp nhp <i>ip-address</i> interface <i>interface-type</i> <i>interface-number</i> nhp <i>ip-address</i> interface <i>interface-type</i> <i>interface-number</i> [nhp <i>ip-address</i> interface <i>interface-type</i> <i>interface-number</i>] &<1-2>
	或配置重定向到公网目标 LSP	redirect lsp public <i>dest-ipv4-address</i> [<i>nexthop-address</i> interface <i>interface-type</i> <i>interface-number</i> secondary]
	或配置逆向地址检查	ip urpf { strict loose } [allow-default]

请根据具体情况选择步骤 3 中的行为特性。

在上述行为中，过滤动作 **permit** 和 **deny** 的优先级高于其他行为，其他行为的优先级相同。

其中，配置报文的服务等级行为只能在报文的上行方向起作用。主要用来指定报文的服务等级与丢弃优先级，让匹配规则的报文能够直接进入指定服务等级的队列，而不需要根据报文头中的优先级字段查 **BA** 表来确定服务等级。同时也可以不必修改报文的优先级字段达到透传报文的目的。



注意：

- 对于 VLANIF、Ring-if 和 Trunk 等逻辑接口，暂时不支持配置重定向的多下一跳地址及出接口。
- 重定向到公网目标 LSP 只能在 MPLS 网络的 ingress 节点上配置，在其他节点（如 transit，egress）不允许配置。

URPF（Unicast Reverse Path Forwarding）是单播逆向路径转发的简称，其主要功能是防止基于源地址欺骗的网络攻击行为。详细信息请参见《Quidway NetEngine80E 通用交换路由器 操作手册 IP 业务分册》。

- **strict:** URPF 将进行严格检查。即根据报文中的源 IP 地址查 FIB（Forward Information Base）表找到单板号、端口号和 VLAN ID（如果是 VLAN 报文），将它们和这个报文进来的单板号、端口号和 VLAN ID（如果是 VLAN 报文）进行比较。如果相等则通过；如果不相等，则丢弃。
- **loose:** URPF 将进行松散检查。根据报文中的源 IP 地址查 FIB 表，如果找到出接口则通过；如果找不到出接口，则丢弃。

4.2.4 定义流量策略并在策略中为类指定行为

步骤	操作	命令
1	进入系统视图	system-view
2	定义流量策略并进入策略视图	traffic policy <i>policy-name</i>
3	在流量策略中为类指定采用的行为	classifier <i>classifier-name</i> behavior <i>behavior-name</i>

4.2.5 应用流量策略

1. 在三层接口中应用流量策略



注意：

- 可以在 POS、GE 等物理接口或子接口、Ringif、IP-Trunk、Eth-Trunk 等逻辑接口上应用流量策略。
- 对于 VLANIF 逻辑接口，不能直接应用流量策略；可以通过物理接口/二层 Eth-Trunk 接口+VLAN ID 范围的方式实现流量策略。

步骤	操作	命令
1	进入系统视图	system-view
2	进入接口视图	interface <i>interface-type</i> <i>interface-number</i>
3	在接口应用流量策略	traffic-policy <i>policy-name</i> { inbound outbound } [link-layer]

如果指定 **link-layer** 参数，NE80E 将根据报文的二层信息进行复杂流分类。缺省情况下，根据三层、四层信息及其他信息进行复杂流分类。

2. 在二层接口中应用流量策略

步骤	操作	命令
1	进入系统视图	system-view
2	进入接口视图	interface <i>interface-type</i> <i>interface-number</i>
3	将接口转换成二层端口	portswitch
4	在二层端口应用流量策略	traffic-policy <i>policy-name</i> { inbound outbound } vlan { <i>vlan-id1</i> [to <i>vlan-id2</i>] all }

4.2.6 配置逆向地址检查

步骤	操作	命令
1	进入系统视图	system-view
2	进入接口视图	interface <i>interface-type</i> <i>interface-number</i>
3	配置逆向地址检查	ip urpf { strict loose } [allow-default]

在接口视图下配置逆向地址检查，将对这个接口上所有流都使能逆向地址检查功能。

4.2.7 检查配置结果

步骤	操作	命令
1	查看接口的流量信息	display interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]
2	查看流行为的配置信息	display traffic behavior { system-defined user-defined } [<i>behavior-name</i>]
3	查看类的配置信息	display traffic classifier { system-defined user-defined } [<i>classifier-name</i>]
4	查看流策略中所有流分类与流行为的关联信息或特定流分类与流行为的关联信息。	display traffic policy { system-defined user-defined } [<i>policy-name</i> [classifier <i>classifier-name</i>]]

4.3 配置基于简单流分类的优先级映射

4.3.1 建立配置任务

1. 应用环境

通过基于简单流分类的优先级映射的配置，可以将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的优先级传送。

2. 前置任务

在配置基于简单流分类的流量策略之前，需要完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性
- 配置相关接口的 IP 地址

3. 数据准备

在配置基于简单流分类的流量策略之前，需准备以下数据：

序号	数据
1	Diff-Serv 域名
2	上行/下行 VLAN 报文 802.1p 值、服务等级
3	上行/下行 IP 报文的 DSCP 编码值、服务等级
4	根据 EXP 定义上行/下行 MPLS 报文的 EXP 域、服务等级、包标记的颜色
5	根据 LSP 定义上行 MPLS 报文的 EXP 域、服务等级、包标记的颜色

序号	数据
6	使能 Diff-Serv 域的端口编号

4. 配置过程

序号	过程
1	定义 Diff-Serv 域并配置流量策略
2	将接口加入 Diff-Serv 域
3	配置 E-LSP 流分类
4	检查配置结果

4.3.2 定义 Diff-Serv 域并配置流量策略

步骤	操作	命令
1	进入系统视图	system-view
2	定义 DS 域并进入 DS 域视图	diffserv domain <i>ds-domain-name</i>
3	对入方向的 VLAN 报文流量定义流量策略	8021p-inbound <i>8021p-value</i> phb <i>service-class</i> [<i>color</i>]
	或对出方向的 VLAN 报文流量定义流量策略	8021p-outbound <i>service-class</i> <i>color</i> map <i>8021p-value</i>
	或对入方向的 IP 流量定义流量策略	ip-dscp-inbound <i>dscp-value</i> phb <i>service-class</i> [<i>color</i>]
	或对出方向的 IP 流量定义流量策略	ip-dscp-outbound <i>service-class</i> <i>color</i> map <i>dscp-value</i>
	或对入方向的 MPLS 流量定义流量策略	mpls-exp-inbound <i>exp</i> phb <i>service-class</i> [<i>color</i>]
	或对出方向的 MPLS 流量定义流量策略	mpls-exp-outbound <i>service-class</i> <i>color</i> map <i>exp-value</i>

Diff-Serv (Different Service) 域由一组采用相同的服务提供策略和实现了相同 PHB 组集合的相连 Diff-Serv 节点组成。

在网络的核心路由器上,一般直接接受或重定义报文中的服务等级。在 IP 域和 MPLS 域的边界路由器上,也需要将 DSCP 和 EXP 进行映射。

简单流分类能够实现从外部优先级到内部优先级及从内部优先级到外部优先级的映射,但是在同种网络流量之间(如 IP 流量之间或 MPLS 流量之间)不支持映射。

系统缺省的 DSCP 到服务类型映射关系如表 4-1 所示。

表4-1 DSCP 与服务类型之间缺省的映射表

DSCP	Service	Color	DSCP	Service	Color
00	be	green	32	af4	green
01	be	green	33	be	green
02	be	green	34	af4	green
03	be	green	35	be	green
04	be	green	36	af4	yellow
05	be	green	37	be	green
06	be	green	38	af4	red
07	be	green	39	be	green
08	af1	green	40	ef	green
09	be	green	41	be	green
10	af1	green	42	be	green
11	be	green	43	be	green
12	af1	yellow	44	be	green
13	be	green	45	be	green
14	af1	red	46	ef	green
15	be	green	47	be	green
16	af2	green	48	cs6	green
17	be	green	49	be	green
18	af2	green	50	be	green
19	be	green	51	be	green
20	af2	yellow	52	be	green
21	be	green	53	be	green
22	af2	red	54	be	green
23	be	green	55	be	green
24	af3	green	56	cs7	green
25	be	green	57	be	green
26	af3	green	58	be	green
27	be	green	59	be	green
28	af3	yellow	60	be	green
29	be	green	61	be	green
30	af3	red	62	be	green
31	be	green	63	be	green

系统缺省的 EXP 到服务类型映射关系如表 4-2 所示。

表4-2 EXP 与服务类型之间缺省的映射表

EXP	Service	Color	EXP	Service	Color
0	be	green	4	af4	green
1	af1	green	5	ef	green
2	af2	green	6	cs6	green
3	af3	green	7	cs7	green

系统缺省的 802.1p 与服务类型映射关系如表 4-3 所示。

表4-3 802.1p 与服务类型之间缺省的映射表

802.1p	Service	Color	802.1p	Service	Color
0	be	green	4	af4	green
1	af1	green	5	ef	green
2	af2	green	6	cs6	green
3	af3	green	7	cs7	green

4.3.3 将接口加入 Diff-Serv 域

步骤	操作	命令
1	进入系统视图	system-view
2	进入接口视图	interface <i>interface-type</i> <i>interface-number</i>
3	在接口上绑定 DS 域	trust upstream { <i>ds-domain-name</i> default }
	或在接口上使能 802.1p	trust 8021p

trust 8021p 命令只能在以太网子接口下配置。

在接口加入到 Diff-Serv 域后，Diff-Serv 域所定义的流量策略将会自动对出入接口的流量起作用。

4.3.4 配置 E-LSP 流分类

步骤	操作	命令
1	进入系统视图	system-view
2	配置 E-LSP 流分类	mpls-lsp-inbound <i>exp</i> phb <i>service-class</i> [<i>color</i>]

4.3.5 检查配置结果

步骤	操作	命令
1	查看 Diff-Serv 域的名称	display diffserv domain [<i>ds-domain-name</i> all]
2	查看接口的流量信息	display interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]

4.4 配置逻辑接口的简单流分类功能

4.4.1 建立配置任务

1. 应用环境

由于逻辑端口在企业组网中将有更加广阔的应用，为了限制逻辑端口成员的报文拥塞，增加对物理端口报文优先级的限制，逻辑端口也必须支持简单流分类的配置及应用。

2. 前置任务

在配置逻辑端口的简单流分类的功能之前，需要完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性
- 配置相关三层接口的 IP 地址

3. 数据准备

在配置逻辑端口的简单流分类的功能之前，需准备以下数据：

序号	数据
1	Diff-Serv 域名
2	上行/下行 VLAN 报文 802.1p 值、服务等级（可选）
3	上行/下行 IP 报文的 DSCP 编码值、服务等级（可选）
4	根据 EXP 定义上行/下行 MPLS 报文的 EXP 域、服务等级、包标记的颜色（可选）
5	根据 LSP 定义上行 MPLS 报文的 EXP 域、服务等级、包标记的颜色（可选）
6	使能 Diff-Serv 域的端口号

4. 配置过程

序号	过程
1	配置 Ring-if 的简单流分类功能
2	配置三层 Trunk 的简单流分类功能
3	配置二层物理接口和二层 Trunk 的简单流分类功能
4	检查配置结果

4.4.2 配置 Ring-if 的简单流分类功能

步骤	操作	命令
1	进入系统视图	system-view
2	定义 DS 域并进入域视图	diffserv domain { <i>ds-domain-name</i> default }
3	定义简单流分类匹配规则	ip-dscp-inbound <i>dscp-value</i> phb <i>service-class</i> [<i>color</i>]
4	进入 Ring-if 视图	interface ringif <i>interface-number</i>
5	匹配 DS 域	trust upstream { <i>ds-domain-name</i> default }

步骤 5 的目的是将 Ring-if 接口匹配 DS 域，这样从 Ring-if 接口进入的报文会实现简单流分类功能。

步骤 3 可以配置多条匹配规则，也可以不配置。若不配置则按缺省的规则处理。

4.4.3 配置三层 Trunk 的简单流分类功能

步骤	操作	命令
1	进入系统视图	system-view
2	定义 DS 域并进入域视图	diffserv domain <i>ds-domain-name</i>
3	定义简单流分类匹配规则	ip-dscp-inbound <i>dscp-value</i> phb <i>service-class</i> [<i>color</i>]
4	进入 Trunk 视图	interface { eth-trunk ip-trunk } <i>interface-number</i>
5	匹配 DS 域	trust upstream { <i>ds-domain-name</i> default }

步骤 3 可以配置多条匹配规则，也可以不配置。若不配置则按缺省的规则处理。

步骤 5 的目的是将 Trunk 接口匹配 DS 域，这样从 Trunk 接口进入的报文会实现简单流分类功能。

4.4.4 配置二层物理接口和二层 Trunk 的简单流分类功能

步骤	操作	命令
1	进入系统视图	system-view
2	定义 DS 域并进入域视图	diffserv domain <i>ds-domain-name</i>
3	定义简单流分类匹配规则	ip-dscp-inbound <i>dscp-value</i> phb <i>service-class</i> [<i>color</i>]
4	进入 GE 接口视图	interface gigabitethernet <i>interface-number</i>
	或进入 Trunk 接口视图	interface { eth-trunk ip-trunk } <i>interface-number</i>
5	将接口转换成二层端口	portswitch
6	基于二层端口和 VLAN 配置简单流分类	trust upstream { ds-domain-name default } vlan { vlan-id1 [to vlan-id2] } &<1-10>
7	基于二层端口和 VLAN 配置修改 VLAN 优先级	trust 8021p vlan { vlan-id1 [to vlan-id2] } &<1-10>

端口可以基于 VLAN 配置加入不同的 DS 域。

步骤 7 是依赖于步骤 6 使用的。如果只配置了步骤 7，是不会对转发产生任何作用的。如果两个步骤都配置，则只会根据 VAN 优先级进入流量管理队列。

4.4.5 检查配置结果

步骤	操作	命令
1	查看 Diff-Serv 域的名称	display diffserv domain [<i>ds-domain-name</i> all]
2	查看接口的流量信息	display interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]

4.5 配置举例

本章的配置举例包括以下案例。

- [基于复杂流分类流量策略配置示例](#)
- [基于简单流分类的优先级映射配置示例](#)

4.5.1 基于复杂流分类流量策略配置示例

1. 配置需求

如图 4-1 所示，三个本地网用户通过路由器 Router 访问 Internet。限制网段 1.1.1.0 的用户的接入速率为 10Mbit/s，承诺突发流量尺寸为 150000 字节；网段 2.1.1.0 的用户的接入速率为 5Mbit/s，承诺突发流量尺寸为 100000 字节；网段 3.1.1.0 的用户的接入速率为 2Mbit/s，承诺突发流量尺寸为 100000 字节。并分别标记他们的 DSCP 值为 40、26 和 0。

2. 组网图

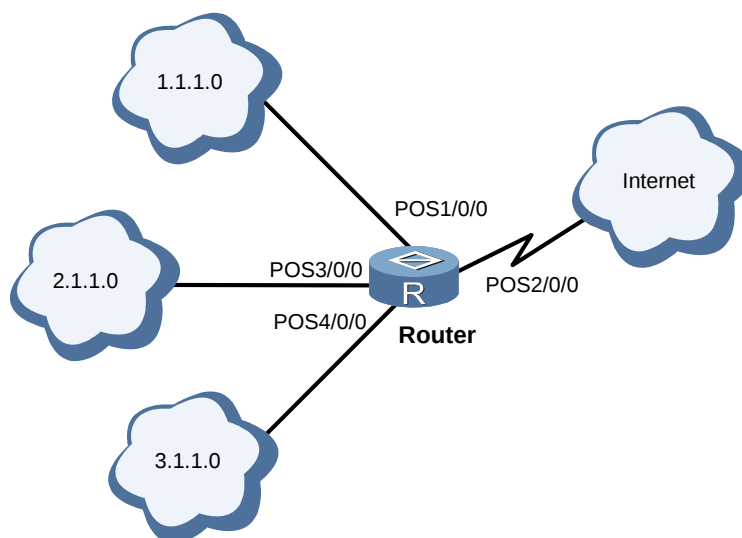


图4-1 流量监管

3. 配置步骤

定义 ACL 规则。

```

[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 1.1.1.0 0.0.0.255
[Router-acl-basic-2001] quit
[Router] acl number 2002
[Router-acl-basic-2002] rule permit source 2.1.1.0 0.0.0.255
[Router-acl-basic-2002] quit
[Router] acl number 2003
[Router-acl-basic-2003] rule permit source 3.1.1.0 0.0.0.255
[Router-acl-basic-2003] quit
    
```

配置流分类，定义基于 ACL 的匹配规则。

```

[Router] traffic classifier a
    
```

```
[Router-classifier-a] if-match acl 2001
[Router-classifier-a] quit
[Router] traffic classifier b
[Router-classifier-b] if-match acl 2002
[Router-classifier-b] quit
[Router] traffic classifier c
[Router-classifier-c] if-match acl 2003
[Router-classifier-c] quit
```

配置完成后，可以通过 **display** 命令查看类的配置信息。

```
[Router] display traffic classifier user-defined
User Defined Classifier Information:
  Classifier: a
    Operator: AND
    Rule(s) : if-match acl 2001
  Classifier: c
    Operator: AND
    Rule(s) : if-match acl 2003
  Classifier: b
    Operator: AND
    Rule(s) : if-match acl 2002
```

定义流行为，并重新设置 DSCP。

```
[Router] traffic behavior e
[Router-behavior-e] car cir 10000 cbs 150000 pbs 0
[Router-behavior-e] remark dscp 40
[Router-behavior-e] quit
[Router] traffic behavior f
[Router-behavior-f] car cir 5000 cbs 100000 pbs 0
[Router-behavior-f] remark dscp 26
[Router-behavior-f] quit
[Router] traffic behavior g
[Router-behavior-g] car cir 2000 cbs 100000 pbs 0
[Router-behavior-g] remark dscp 0
[Router-behavior-g] quit
```

定义流量策略，将流分类与流行为关联。

```
[Router] traffic policy 1
[Router-trafficpolicy-1] classifier a behavior e
[Router-trafficpolicy-1] quit
[Router] traffic policy 2
[Router-trafficpolicy-2] classifier b behavior f
[Router-trafficpolicy-2] quit
[Router] traffic policy 3
```

```
[Router-trafficpolicy-3] classifier c behavior g
[Router-trafficpolicy-3] quit
```

上述配置完成后，使用 **display traffic policy** 命令可以查看流量策略、策略中定义的流分类以及与流分类相关的流行为的配置情况。

```
[Router] display traffic policy user-defined
```

User Defined Traffic Policy Information:

Policy: 3

Classifier: default-class

Behavior: be

-none-

Classifier: c

Behavior: g

Committed Access Rate:

CIR 2000 (Kbps), PIR 0 (Kbps), CBS 100000 (byte), PBS 0 (byte)

Conform Action: pass

Yellow Action: pass

Exceed Action: discard

Marking:

Remark DSCP default

Policy: 2

Classifier: default-class

Behavior: be

-none-

Classifier: b

Behavior: f

Committed Access Rate:

CIR 5000 (Kbps), PIR 0 (Kbps), CBS 100000 (byte), PBS 0 (byte)

Conform Action: pass

Yellow Action: pass

Exceed Action: discard

Marking:

Remark DSCP af31

Policy: 1

Classifier: default-class

Behavior: be

-none-

Classifier: a

Behavior: e

Committed Access Rate:

CIR 10000 (Kbps), PIR 0 (Kbps), CBS 15000 (byte), PBS 0 (byte)

```

        Conform Action: pass
        Yellow Action: pass
        Exceed Action: discard
    Marking:
        Remark DSCP cs5

```

将流量策略应用到接口上。

```

[Router] interface pos 1/0/0
[Router-Pos1/0/0] traffic-policy 1 inbound
[Router-Pos1/0/0] quit
[Router] interface pos 3/0/0
[Router-Pos3/0/0] traffic-policy 2 inbound
[Router-Pos3/0/0] quit
[Router] interface pos 4/0/0
[Router-Pos4/0/0] traffic-policy 3 inbound

```

4. 配置文件

```

#
sysname Router
#
acl number 2001
    rule permit source 1.1.1.0 0.0.0.255
acl number 2002
    rule permit source 2.1.1.0 0.0.0.255
acl number 2003
    rule permit source 3.1.1.0 0.0.0.255
#
traffic classifier a operator and
    if-match acl 2001
traffic classifier c operator and
    if-match acl 2003
traffic classifier b operator and
    if-match acl 2002
#
traffic behavior e
    car cir 10000 cbs 150000 pbs 0 green pass yellow pass red discard
    remark dscp cs5
traffic behavior g
    car cir 2000 cbs 100000 pbs 0 green pass yellow pass red discard
    remark dscp default
traffic behavior f
    car cir 5000 cbs 100000 pbs 0 green pass yellow pass red discard
    remark dscp af31

```

```
#
traffic policy 3
  classifier c behavior g
traffic policy 2
  classifier b behavior f
traffic policy 1
  classifier a behavior e
#
interface Pos1/0/0
  undo shutdown
ip address 1.1.1.1 255.255.255.0
  traffic-policy 1 inbound
#
interface Pos3/0/0
  undo shutdown
ip address 2.1.1.1 255.255.255.0
  traffic-policy 2 inbound
#
interface Pos4/0/0
  undo shutdown
ip address 3.1.1.1 255.255.255.0
  traffic-policy 3 inbound
#
return
```

4.5.2 基于简单流分类的优先级映射配置示例

1. 配置需求

三台路由器之间建立 MPLS 邻居，从 RouterA 上进入的 IP 流量，在 RouterA 至 RouterC 之间走 MPLS 转发。从 RouterC 流出后，又恢复成 IP 流。

要求流量在 RouterA 上，能任意修改成为 MPLS 流量之后的优先级，在 RouterC 上能任意修改恢复 IP 流之后的优先级。

2. 组网图

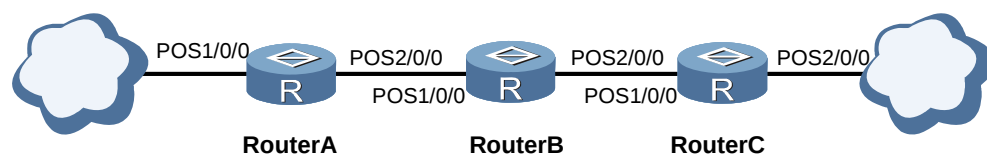


图4-2 从 DSCP 优先级到 MPLS 优先级映射

 说明:

- 在本配置例中,假定已经建立好了三台路由器上的 MPLS 配置,IP 流量从 RouterA 到 RouterC 能进行 MPLS 转发, MPLS 流量出 RouterC 时,能转换成 IP 流。
- 以下的配置,只列出了与 QoS 配置相关的命令。

3. 配置步骤

(1) 配置 RouterA

在 RouterA 的 POS1/0/0 接口上配置 DSCP 到 MPLS 的映射。

```
[RouterA] diffserv domain default
[RouterA-dsdomain-default] ip-dscp-inbound 18 phb af4 green
[RouterA-dsdomain-default] mpls-exp-outbound af4 green map 5
[RouterA-dsdomain-default] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] trust upstream default
[RouterA] interface pos 2/0/0
[RouterA-Pos2/0/0] trust upstream default
```

在 RouterA 的入接口上配置 DSCP 值 AF2 (18) 到路由器内部业务等级 AF4 的转换,在出接口上配置 DSCP 值 AF4 到 MPLS 优先级 5 的映射,从 RouterA 出来的是 EF 流量。

(2) 配置 RouterC

在 RouterC 的 POS1/0/0 接口上配置 MPLS 到 DSCP 的映射。

```
[RouterC] diffserv domain default
[RouterC-dsdomain-default] mpls-exp-inbound 5 phb af3 green
[RouterC-dsdomain-default] ip-dscp-outbound af3 green map 32
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] trust upstream default
[RouterC] interface pos 2/0/0
[RouterC-Pos2/0/0] trust upstream default
```

在 RouterC 的入接口上配置 MPLS 优先级 5 到 DSCP 值 AF3 的映射,在出接口配置 DSCP 值 AF3 到 DSCP 值 AF4 (32) 的转换,RouterC 出来的是 AF4 流量。

配置完成后,从 RouterA 的 POS1/0/0 发送 DSCP 值为 18 (AF2) 的流量,大小为 100M,RouterC 出来的是 DSCP 值为 32 的 AF4 流,流量为 50M。

4. 配置文件

(1) RouterA 的配置文件

#

```

sysname RouterA
#
diffserv domain default
    ip-dscp-inbound 18 phb af4 green
    mpls-exp-outbound af4 green map 5
#
interface Pos1/0/0
    undo shutdown
ip address 2.2.2.1 255.255.255.0
    trust upstream default
#
interface Pos2/0/0
    undo shutdown
ip address 3.3.3.1 255.255.255.0
    trust upstream default
#
return

```

(2) RouterC 的配置文件

```

#
sysname RouterC
#
diffserv domain default
    ip-dscp-outbound af3 green map 32
    mpls-exp-inbound 5 phb af3 green
#
interface Pos1/0/0
    undo shutdown
ip address 4.4.4.1 255.255.255.0
    trust upstream default
#
interface Pos2/0/0
    undo shutdown
ip address 5.5.5.1 255.255.255.0
    trust upstream default
#
return

```

4.6 故障处理

1. 故障现象

配置完成后，路由器 QoS 不能正常运行。

2. 分析

在 QoS 的配置中，除了规则、行为、流量参数配置正确，还要确保配置的出/入方向正确。

3. 处理过程

步骤	操作
1	执行 QoS 的显示命令，查看配置的规则、行为、流量参数等是否正确。
2	执行 display current-configuration 命令查看运行状态及配置的出/入接口是否正确。
3	执行 display device 命令查看接口板状态，正常的状态应该是 Registered。
4	执行 ping 命令，检查物理连接及下层协议是否正常运行。