61200821E1-29.1B
July 2007

ADTRAN®

Configuration Guide

Policy-Based Routing

This Configuration Guide will aid in the setup of policy-based routing (PBR) for ADTRAN Operating System (AOS) products. An overview of PBR general concepts combined with detailed command descriptions for example networks provide step-by-step assistance for configuration. The troubleshooting section outlines proper use of **show** and **debug** commands to verify that PBR has been configured properly on the AOS product(s).

This guide consists of the following sections:

PBR Overview

Policy-based routing (PBR) on an AOS product allows you to implement basic traffic engineering: you can manipulate the path a packet follows based on characteristics of that packet. Routers use PBR to route traffic with the same destination over different paths according to the traffic's priority, source, or size. PBR can also be used to alter a packet's IP header for QoS purposes.

By default, routers forward packets according to their destination address alone. When a packet arrives on an interface, the router matches the destination address in the packet's IP header to an entry in the router's routing table. Unless the routing table changes, the router always routes packets addressed to a particular destination to the same next hop.

To make your network function optimally, however, you may want different types of traffic to travel over different paths, even when that traffic is destined to the same network.

Applications for PBR include enforcing security, reserving a connection for specific traffic, and traffic engineering. These applications are discussed below.

Enforcing Security

You can configure the router to send certain traffic to a security appliance such as an intrusion detection system (IDS) for further processing rather than forwarding it directly over a WAN or Internet connection. An IDS can provide more security than a firewall because it monitors traffic from both external and internal users for suspicious activity.

Your organization's security policies may define certain internal hosts as untrusted. When the router receives traffic from these hosts, the router should forward traffic to the IDS before forwarding it to the Internet or remote site. For other hosts, who are trusted, the router may forward traffic directly over the wide area network (WAN) connection. You could configure a PBR policy that selects traffic from certain hosts and forwards it through the correct interface for that host.

For example, a university might allow faculty, staff, and administrators to access the Internet directly. However, university policies dictate that traffic from subnets used by students and guests must be processed by the IDS before being forwarded to the Internet. This security measure is to deter students and guests from using the university's Internet connection for unauthorized activities. Although traffic from all users may be destined to the same networks, the router will forward traffic based on the host that sends the traffic: either directly to the ISP router or to the IDS.

Reserving a Connection for Specific Traffic

Because some traffic requires special handling, you may want to reserve a particular WAN connection for this traffic. For example, voice over IP (VoIP) traffic requires low delay. Your organization could establish multiple connections to a remote site, reserving a high-speed connection or a connection with fewer hops for VoIP traffic. You would configure a policy that selects VoIP traffic (or other high-priority traffic) and forwards it across the reserved connection.

Traffic Engineering

When your router connects to a site through more than one link, you can configure policies to forward some traffic over one link and other traffic over the other. However, a better practice is to balance the load using a routing protocol or multilink PPP (MLPPP).

You can configure your AOS product to route a packet according to any of the following:

- Standard or extended access control list (ACL) match
- IP precedence
- Differentiated Services (DiffServ) Code Point (DSCP)
- Layer 3 packet length
- Traffic originating from the router

By selecting traffic based on these attributes, you can control the path packets take through different router interfaces and enforce basic traffic engineering.

You configure PBR policies in a route map, which you then apply to an interface. The route map applies to traffic that arrives on the interface. You can apply only one route map to each interface, but you can configure multiple entries for each route map.

Each route map consists of a series of sequenced route map entries. Each route map entry is identified by a name and a sequence number. When you apply the route map to an interface, you apply it as an entire set, which includes all the route map entries with the same name and different sequence numbers. In each route map entry, you enter one or more **match** commands, which select traffic for PBR. You also enter one or more **set** commands, which determine how the selected traffic is routed or modified. When a packet arrives on an interface, the router begins to process the route map associated with the interface. The router processes the entries in order, starting with the entry that has the lowest sequence number. The router stops processing the set of route map entries as soon as it finds a match for a packet. When a match is made the configured **set** commands will be applied to alter the packet or the manner in which it will be routed. Therefore, you should pay attention to the sequence number you assign to a route map entry. For example, if you want to use a route map to route a packet and to mark this packet with a quality of service (QoS) value, you should enter the **set** commands for both these policies in the same route map entry.

Hardware and Software Requirements and Limitations

PBR was introduced in AOS 11.01.00 and is currently available in the following: NetVanta hardware platforms 1335, 3120, 3130, 3305, 3430, 3448, 4305, and 5305.

When using PBR, AOS 14.01.00 or later is recommended due to limitations in previous versions and recent performance enhancements.

To greatly increase router performance when PBR is used, the AOS Fast Forwarding Engine (FFE) needs to be enabled on all interfaces where PBR is applied. To enable FFE on an interface use the **ip ffe** command from interface configuration mode.

For example, the following commands enable FFE on the Ethernet 0/1 interface of an AOS product:

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#ip ffe**

FFE is currently not supported on high-level data link control (HDLC), general routing encapsulation (GRE) tunnel, and demand interface types. Also, FFE does not work in conjunction with the **match length** command discussed in Step 3 of *Configuring PBR in AOS* on page 4. This command can be specified and used; however, router performance will not be optimized anytime traffic matches against the **match length** command in a route map because FFE cannot be utilized.

Configuring PBR in AOS

The following steps are required to implement PBR in AOS:

1. Create an access control list (ACL) to match traffic
2. Create the route map
3. Use **match** commands to specify the traffic
4. Use **set** commands to define the action
5. Apply the policy to an interface

The following sections detail each of the steps listed above with an explanation and the required syntax for configuration.

Step 1: Create an ACL to match traffic

If you wish to select traffic for PBR based on Layer 3 length, IP precedence, or DSCP, you can bypass this step and proceed to step 2.

Using a Standard ACL to Define Traffic

Certain organizational policies may require your router to forward traffic based on its source as well as its destination. For example, certain hosts may be authorized to access the router's connection to a remote site or the Internet directly. However, the organization requires traffic from other hosts to be sent to a security device that will monitor it before forwarding it to its destination.

In this situation, you would configure a policy that selects traffic from unauthorized hosts and forwards it to the security device. Other traffic (from authorized hosts) can use the routes in the router's routing table.

Another application for source-based PBR is to divide network traffic and forward it over several connections to the Internet or the same remote site. However, you should generally use a dynamic routing protocol or MLPPP for this type of load balancing.

You use an ACL to select traffic according to its source. A standard ACL selects the traffic to be routed according to its source only. If you want to route traffic according to both its source and its destination, you must configure an extended ACL.

When you use a standard ACL, the router routes all traffic from a source according to the policy you configure in the route map. You should be certain that the route applies to all traffic.

For example, if you are configuring a policy to forward external traffic from certain sources to a device for further processing, you might not want the router to send local traffic to that device. You can address this issue in one of two ways:

- Configure an extended ACL (instead of a standard ACL) to select traffic from certain hosts. Deny traffic destined to local networks from this ACL.
- If external traffic is normally routed with a default route, you can configure a default policy in the route map. When you enter a **set** command to establish the route map policy, use a command with the **default** keyword. This keyword forces the router to search its routing table before forwarding a packet selected by the route map. If the routing table includes an explicit route to the packet's destination (for example, to a local network), the router uses that route instead of the routing policy specified in the map.

To configure an ACL to route traffic according to its source only, complete these steps:

1. From the Global Configuration mode, create a standard ACL:

   Syntax: **ip access-list standard** <*name*>

2. If necessary, remove a specific source from the list:

   Syntax: **deny [host** <*ip address*> **| hostname** <*name*> **|** <*ip address*> <*wildcard mask*>**]**

3. Permit traffic from the host, network, or range of networks that you want to route using PBR:

   Syntax: **permit [any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>**]**

Use the **host** keyword to select the IP address of a single host. Use the **hostname** keyword to match the hostname of a single host. A dynamic name server (DNS) server must be specified with the **ip name-server** command from Global Configuration mode when using the **hostname** keyword in an ACL. Use the wildcard mask to select an entire network or a range of networks. The IP address you enter is the first address in the range. You can verify the last address in the range by adding the wildcard mask to this address. For example, your local network uses four /24 networks, 10.1.0.0 /24, 10.1.1.0 /24, 10.1.2.0 /24, and 10.1.3.0 /24. Traffic from two of these networks (10.1.0.0 /24 and 10.1.1.0 /24) must be routed to a security device instead of directly over a WAN connection. Enter:

(config-std-nacl)**#permit 10.1.0.0 0.0.1.255**

The **any** keyword selects all traffic.

Using an Extended ACL to Define Traffic

To configure an ACL to route traffic based on its source as well as its destination, complete these steps:

1. From the Global Configuration mode, create an extended ACL:

   Syntax: **ip access-list extended** <*name*>

2. The routing policy may not apply to traffic destined to certain addresses. For example, you could use PBR to forward certain traffic to a device that filters that traffic before allowing it access a remote site.

You might not want to forward local traffic to this device. In this case, you would deny traffic destined to local addresses using this command:

Syntax: **deny ip [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>**] [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>]

For example, exclude all traffic destined to network 192.168.25.0 /24:

(config-ext-nacl)**#deny ip any 192.168.25.0 0.0.0.255**

3. Enter a **permit** statement to select the traffic for PBR. When you enter the command, first specify the address of the host, network, or range of networks for which you want to use PBR to route the traffic. You can then enter the destination address for the route. The destination can be a single host (use the **host** or **hostname** keywords), but you should generally either specify all networks not earlier denied (**any**) or the address for a network or range of networks. Use the wildcard mask to specify a range of addresses.

   Syntax: **permit ip [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>**] [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>**]**

For example, you are configuring PBR on an AOS product that acts as the Internet gateway for a university. The university wants traffic originating from subnets assigned to students to be subjected to additional data security screenings. In this example the student subnets include the second half of networks in the 10.2.0.0 /16 range. Student traffic destined to the Internet will be routed to an IDS device. Other traffic (administrators, faculty, etc) can access the Internet without further processing. Hosts on the student subnets also need access to various servers on the local network (10.2.0.0 /16). Because the local router also receives and routes this traffic, you configure it to route traffic from students destined to local networks using the routes in its routing table. Enter these commands:

(config)**#ip access-list extended students**

(config-ext-nacl)**#deny ip any 10.2.0.0 0.0.255.255**

(config-ext-nacl)**#permit ip 10.2.128.0 0.127.255.255 any**

Notice the order of the ACL arguments. The **deny** statement specifies that any traffic (including the student subnets) attempting to access the 10.2.0.0 /16 subnet should be routed normally (i.e., ignore the route map). The **permit** statement specifies that student subnet traffic going to any destination should be routed differently based on the route map. It is important that the **deny** statement comes first in this example. Otherwise student traffic trying to access various servers on the local network (10.2.0.0 /16) would be mistakenly sent to the IDS.

After you have configured the ACL, it will need to be referenced by name (refer to *Step 3: Use match commands to specify the traffic* on page 8). For this particular example, the ACL name **students** would need to be specified.

Your organization's policies may specify that traffic for certain applications be routed over a different path than that indicated in your router’s routing table. For example, your organization may have a connection that it only wants to use when a File Transfer Protocol (FTP) server transmits files to a server at a remote site, or your organization may want to reserve a connection for real time traffic.

You classify traffic according to its application or protocol by configuring an extended ACL. In this ACL, you specify either the source port of the protocol or the destination port or both. You can also specify particular addresses for the source and destination. Alternatively, you can allow all traffic for that application or all traffic for that application destined to a specific server.

You can also deny traffic for a particular application. For example, you could bar Telnet traffic from a high-cost connection.

Follow these steps to select the traffic for the route map entry:

1. From the Global Configuration mode, create the extended ACL:

   Syntax: **ip access-list extended** <*name*>

2. Use this command to select traffic for the application:

   Syntax: **[permit | deny]** <*protocol*> **[any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>**] [eq** <*port*> **| gt** <*port*> **| lt** <*port*> **| range** <*first port*> <*last port*> **| neq** <*port*>**] [any | host** <*ip address*> **| hostname** <*name*> |<*ip address*> <*wildcard mask*>**] [eq** <*port*> **|**
   gt <*port*> **| lt** <*port*> **| range** <*first port*> <*last port*> **| neq** <*port*>**]**

For the protocol, enter the application's protocol, such as Transmission Control Protocol (TCP) or Universal Datagram Protocol (UDP).

Next, enter the source address and port and then the destination address and port. Use the **any** keyword for the source and destination addresses if you want to allow all traffic for the application. (Use the **any** keyword for the source address, but enter a specific destination address with the **host** keyword, if you want to allow all traffic to a specific server.)

Specify the application by entering the destination port after the destination address. Use the **eq** keyword to select a single port. You can enter either the port's number or the keyword for a well-known port. (Use the **?** help command for a complete list of keywords.) To enter a range of ports, use the **gt**, **lt**, or **range** keywords. The **eq**, **gt**, **lt**, **range**, and **neq** keywords can be used to simplify an ACL by allowing you to specify port numbers that are equal to, greater than, less than, in a specified range, and not equal to, respectively.

Note that you can enter a source port for the application instead of, or in addition to, the destination port.

Step 2: Create the route map

To create a route map entry, enter this command from the Global Configuration mode:

Syntax: **route-map** <*name*> **[permit | deny]** <*sequence number*>

For example, you might enter:

(config)**#route-map PBR permit 10**

(config-route-map)#

Both **permit** and **deny** statements can be used when defining a route map name and sequence number. When the **deny** keyword is specified, it will cause a normal route table look up as opposed to PBR, when the criteria are matched inside the route map.

The **deny** statement generically states that all traffic or objects matching this statement will not use the specified route map. Any **set** commands defined on a **deny** entry are ignored.

When the **permit** keyword is specified, it will apply PBR when the criteria are matched inside the route map.

If no keyword is specified, **permit** is applied by default.

It is possible to apply a normal route table look up when a **permit** keyword is used in these conditions:

- Traffic matches a route map **permit** entry, but no **set ip nexthop** or **set interface** commands are specified.
- Traffic matches a route map **permit** entry, but no **set ip nexthop** or **set interface** commands are valid.
- Traffic matches a route map **permit** entry that specifies an ACL, and the traffic matches a **deny** statement in the ACL.

Step 3: Use match commands to specify the traffic

Use the **match** commands shown in Table 1 to select traffic for the map entry. Read the following sections for explanations of the types of policies you can establish with the various **match** commands.

If you enter more than one **match** command in a particular entry (identified by the sequence number), a packet must match the criteria for all of the **match** commands. If a packet does not match all criteria for the entry, the router attempts to match it to the route map entry with the next sequence number.

If the packet does not match any of the entries, the router will forward it according to a route in its routing table. However, if you do not enter a **match** command in the route map entry, all traffic will match that entry; the router will forward any traffic received on the interface as specified by the **set** command for that entry.

Table 1. AOS Route Map Match Commands

Interface Configuration Mode	Command	Explanation
route-map	**match ip address** <*ACL name*>	Matches traffic based on a standard or extended ACL
	match ip precedence [<*keyword*> | <*value*>]	Matches traffic based on an ip precedence keyword or numerical value (0 to 7)
	match ip dscp [<*AF class*> | <*CS class*> | **default** | **ef** | <*value*>]	Matches traffic based on DiffServ assured forwarding (AF), class selector (CS), default, expedited forwarding (EF), or numerical value (0 to 63)
	match length <*minimum length*> <*maximum length*>	Matches traffic based on Layer 3 length (in bytes)

Implementing PBR According to an ACL

If an ACL is used to define the traffic you wish to use for PBR, the **match ip address** <*ACL name*> command must be used. This command forces the route map to match packets defined in the ACL. *Step 1: Create an ACL to match traffic* on page 4 discusses how to use an ACL depending on your application.

Beginning in AOS 16.01.00, multiple ACLs can be specified separated by a space with one **match ip address** command. This will result in a match if the traffic satisfies the criteria given in any one of the specified ACLs.

As shown in Table 1 on page 9, there are several other ways to match traffic besides with an ACL. The sections below discuss the applications and syntax for use with the various other **match** commands.

Implementing PBR According to Traffic Priority

A packet's IP header includes a type of service (ToS) field that can be marked with various values to request a certain quality of service (QoS) for that packet. The ToS field can include either an IP precedence value or a DSCP.

You can use a route map to route traffic with different ToS values over different paths. In this way, you can reserve a particular connection for high-priority traffic. For example, VoIP applications often mark VoIP packets with a ToS value. You can select these packets by matching the route map to this value.

To select a packet according to the value marked in its ToS field, move to the Route Map Configuration mode.

If your network uses IP precedence, use this command to select traffic:

Syntax: **match ip precedence [critical | flash | flash-override | immediate | internet | network | priority | routine |** <*value*>**]**

You can enter either a value between 0 and 7 or the keyword for the priority. IP precedence 5 (critical) is the highest priority for user traffic; values 6 and 7 are used for Internet control traffic and private network control traffic, respectively. See Table 2 for the value that corresponds to each keyword.

Table 2. IP Precedence Keywords

Value	Priority
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash-override
5	Critical
6	Internet
7	Network

If your network uses DiffServ, you can select traffic according to its per-hop behavior (PHB) setting. In networks that support DiffServ, a PHB defines such settings as the bandwidth allocated to traffic and the traffic dropped first when congestion occurs.

You can select

- the default PHB
- a class selector (CS) PHB
- an assured forwarding (AF) PHB
- the expedited forwarding (EF) PHB

You can also select traffic marked with any DSCP used in your network.

To select traffic that does not have a set DiffServ value, match the entry to the default PHB:

Syntax: **match ip dscp default**

CS PHBs provide backwards compatibility with IP precedence values. To select a CS PHB, enter this command:

Syntax: **match ip dscp [cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7]**

Table 3 displays the DSCP for the CS PHB.

Table 3. Class Selector Per-Hop Behavior

DIffServ Value	DSCP	First 3 bits	IP Precedence
0	000000	000	0
8	001000	001	1
16	010000	010	2
24	011000	011	3
32	100000	100	4
40	101000	101	5
48	110000	110	6
56	111000	111	7

AF divides traffic into classes, which can be assigned varying drop precedences and amounts of bandwidth. Use this command to select an AF PHB used in your network:

Syntax: **match ip dscp [af11 | af12 | af13 | af 21 | af 22 | af23 | af31 | af 32 | af 33 | af 41 | af42 | af43]**

Table 4 displays the DSCP codepoints for the AF PHB.

Table 4. Assured Forwarding Per-Hop Behavior

AF Class	Drop Precedence	DSCP	DiffServ Value
AF1 - least bandwidth			
AF11	low	001010	10
AF12	medium	001100	12
AF13	high	001110	14
AF2 - more bandwidth			
AF21	low	010010	18
AF22	medium	010100	20
AF23	high	010110	22
AF3 - more bandwidth			
AF31	low	011010	26
AF32	medium	011100	28
AF33	high	011110	30
AF4 - more bandwidth			
AF41	low	100010	34
AF42	medium	100100	36
AF43	high	100110	38

You can also select traffic marked for expedited forwarding (DSCP 46), a PHB that is guaranteed low latency and a set amount of bandwidth:

Syntax: **match ip dscp ef**

To select a specific DSCP defined within your network, enter this command:

Syntax: **match ip dscp** <*value*>

Enter a value between 0 and 63.

You can match the entry to more than one ToS value by entering multiple values separated by a space. Any packet that matches one of these values will be selected.

Implementing PBR According to Payload Size

One application for PBR is selecting different routes for interactive and for bulk traffic. For example, you could allow bulk traffic associated with FTP or video streaming applications, which are typically active only temporarily, to use a specific connection reserved for such applications. You could restrict the routine, interactive traffic to a cost-effective connection such as a Frame Relay link.

One way to distinguish bulk traffic from interactive traffic is by packet size. Packets associated with interactive traffic tend to be small. To set the size for packets selected for the route map, enter this command from the Route Map Configuration mode:

Syntax: **match length** *<minimum length> <maximum length>*

Enter lengths in bytes. The length applies to the Layer 3 length, which is the total length of the IP datagram and the IP header. This does not include the Layer 2 packet length.

For example, you could force the router to forward IP packets between 10 and 500 bytes out a specific interface. To select the packets, you would enter:

(config-route-map)**#match length 10 500**

You can enter **0** for the minimum length if you simply want to ensure that the packet does not exceed a specific size. For example, if you knew that packets for interactive traffic in your network were generally smaller than 200 bytes, you could enter this command to select interactive traffic:

(config-route-map)**#match length 0 200**

FFE cannot be utilized when traffic matches this statement in a route map and can result in suboptimal router performance. Refer to ***Hardware and Software Requirements and Limitations*** *on page 3 for more details.*

Step 4: Use set commands to define the action

For each route map entry used for PBR, you must also enter at least one **set** command. This command specifies how selected traffic will be routed or modified.

You can configure the router to forward these packets

- to an adjacent neighbor
- through a specific interface
- to an adjacent neighbor only if the routing table does not include an explicit entry for the packet's destination
- through a specific interface only if the routing table does not include an explicit entry for the packet's destination

You can also configure the router to modify the packet's ToS field for QoS purposes or flag a bit in the packet to prevent fragmentation when traversing through a network.

Use the commands shown in Table 5 on page 14 to configure the policy.

Table 5. AOS Route Map Set Commands

Interface Configuration Mode	Command	Explanation
route-map	**set ip next-hop** <*ip address*> [<*secondary ip address*>]	Forwards traffic to the specified adjacent neighbor's address
	set interface <*interface id*> [<*secondary interface id*>]	Forwards traffic through the specified interface to an implied adjacent neighbor
	set ip default next-hop <*ip address*> [<*secondary ip address*>]	Forwards traffic to the specified adjacent neighbor's address only if a route does not exist for the packet's destination
	set default interface <*interface id*> [<*secondary interface id*>]	Forwards traffic through the specified interface to an implied adjacent neighbor only if a route does not exist for the packet's destination
	set ip pr*ecedence* <*keyword*> | <*value*>	Alters a packet's ip precedence to reflect specified keyword or numerical value (0 to 7)
	set ip dscp [<*AF class*> | <*CS class*> | **default** | **ef** | <*value*>]	Alters a packet's DiffServ to reflect specified assured forwarding (AF), class selector (CS), default, expedited forwarding (EF), or numerical value (0 to 63)
	set ip df	Alters a packet by setting the don't-fragment (DF) bit to prevent fragmentation

Operation of Set Commands

When a router uses typical routing, it can learn more than one route to a destination, which means that it can immediately begin using a backup route if a connection fails. You can also configure backup routes for PBR. Simply specify more than one **set** command or more than one next-hop address or forwarding interface in a single **set** command.

For example, you can specify multiple next-hop addresses with the following **set** command:

(config-route-map)**#set ip next-hop 10.1.1.1 10.2.2.1**

The router first attempts to forward a selected packet to the first address or interface specified. It then tries the second, and so forth.

If multiple routes are specified with **set** commands, the router processes them in the following order: **next-hop**, **interface**, **default next-hop**, and **default interface**. This is the order in which they are displayed when viewing the running configuration of a unit. The router first attempts to route a packet to an adjacent neighbor. If the router does not know how to reach that neighbor or if the forwarding interface for the route to that neighbor is down, the router attempts to route the packet to any secondary specified next-hop address. The router then attempts to route the packet through a specified interface and so forth. If multiple addresses/interfaces are specified for a given route, the first available address/interface will be used. The **set** commands **next-hop** and **default next-hop** require the route to be directly connected.

You can also enter multiple **set** commands.

For example, you could configure two **set** commands in a route map entry that selects traffic with IP precedence 5:

(config-route-map)**#match ip precedence 5**

(config-route-map)**#set interface ppp 1**

(config-route-map)**#set ip next-hop 10.3.3.1**

The first **set** command specifies that the router forward the high-priority traffic through the interface PPP 1. The second command specifies that the router forward the high-priority traffic to an adjacent device with the address 10.3.3.1.

For this example, we will assume the route map is applied to interface Ethernet 0/1 and that the 10.3.3.0 /30 network is applied to the PPP 3 interface.

When a routine packet (IP precedence 0) arrives on interface Ethernet 0/1, the router looks up the entry for network 192.168.64.0 /20 in its routing table and forwards the packet out the appropriate interface specified in the routing table. The router uses the routing table entry because the routine packet does not match the route map entry.

When a mission-critical packet (IP precedence 5) arrives, the router matches the packet to the route map entry. It then routes the packet as indicated in the route map entry. The router first attempts to route the high-priority traffic through interface PPP 3 (the forwarding interface for 10.3.3.1). If this interface is not available or if the route to 10.3.3.1 does not exist, the router forwards the traffic through PPP 1.

If the router cannot find a route for any of the addresses or interfaces specified in the route map entry, it does not drop the packet. Instead, the router forwards the packet according to the matching entry in its routing table. If such an entry does not exist, the router does drop the packet, but if a default route is specified the packet will be forwarded according to it.

If you want your router to drop packets that it cannot forward using a manually-defined, traffic-specific route, you should enter a **set** command for a null interface. For example:

(config-route-map)**#set ip next-hop 10.3.3.1**

(config-route-map)**#set interface ppp 1 null 0**

After trying to route packets to 10.3.3.1 and then through PPP 1, the router drops them.

Packets that do not match criteria in a route map will use the default routing table instead of being dropped. Packets that match an ACL specified in a route map with the **deny** keyword will also use the default routing table instead of being dropped. A **set** command can be used to set the egress interface to **null 0** in order to drop the packets as shown below.

(config-route-map)**#set interface null 0**

The following interface types can be used with the **set interface** command:

ethernet <*slot/port*>

frame-relay <*port.sublink*>

hdlc <*interface id*>

null 0

ppp <*interface id*>

tunnel <*interface id*>

vlan <*interface id*>

All of the interface types specified above, except for **eth**, **vlan**, and **null**, are point-to-point and have an implied next-hop neighbor. The **set interface ethernet** <*slot/port*> command and the **set interface vlan** <*interface id*> command can be used only when DHCP is utilized so the router will forward traffic to the default gateway learned on that particular interface. The **set interface null 0** command should be used to have the router drop traffic.

Configuring Default Routes in a Route Map Entry

You can use route maps to configure default routes that apply to only specific types of traffic. Traffic-specific default routes are particularly useful when you want to apply different policies to external traffic from different sources.

By definition, a routing table can only include one default route. Such a route is usually used for all external traffic. However, your organization may want to route some external traffic differently. For example, if your network provides Internet access to guests, you might want to send such traffic to an IDS device to screen it before allowing it to access the Internet connection.

You can add a default route that applies to most traffic in the routing table. You can then configure a default route in a route map to override the global default. The default route in the route map would only apply to a specific type of traffic (for example, traffic from users that needs additional screening).

The router would still route this traffic as indicated in the routing table when the table includes an explicit route for the traffic's destination (for example, a local network). However, when the table does not contain a route to the destination, the router would forward the specified traffic according to the default route in the route map entry instead of the default route in the routing table.

To configure the traffic-specific default route, you should first create the route map entry and select the traffic. (Refer to *Step 3: Use match commands to specify the traffic* on page 8.) You can then specify the next-hop address or the forwarding interface for the traffic-specific default route:

Syntax: **set ip default next-hop** <*ip address*> **[**<*secondary ip address*>**]**

Syntax: **set default interface** <*interface id*> **[**<*secondary interface id*>**]**

If you enter both commands, the router will first attempt to route traffic to the default next-hop address. If the interface for this neighbor is down, the router will attempt any secondary next-hop addresses. Finally, the router will transmit the packet through the default interface. It is sometimes a good idea to enter only a default interface so that the route will remain valid even if the neighbors' IP addressing changes.

Using a Route Map to Mark Packets with a QoS Value

You can also use the route map to mark selected packets with an IP precedence or DiffServ value. This value requests a particular type of service for the packets in the network to which the packets are being forwarded. Having routers at remote sites mark outbound packets simplifies QoS configuration for the entire network. You do not have to configure complex QoS policies on every WAN router at the central site.

To mark selected packets with an IP precedence value, enter this command from the Route Map Configuration mode:

Syntax: **set ip precedence [critical | flash | flash-override | immediate | internet | network | priority | routine | <*value*>]**

You can enter either a keyword or a value between 0 and 7. (IP precedence value 6 is generally reserved for Internet control traffic, and 7 is reserved for private network control traffic.)

DiffServ values request a specific PHB. If routers in the remote network support DiffServ, they should forward a packet according to the PHB defined for its DiffServ value. It is up to the administrators of that network to define and implement policies for each supported PHB.

The AF PHB divides traffic into four classes, each of which is granted progressively more relative bandwidth. Each class is divided into three subclasses, the first of which is granted to highest drop priority: routers will drop packets in the first subclass last if the network becomes congested.

If the remote network supports AF PHB, you can mark selected packets with the DSCP for an AF subclass. Enter this command:

Syntax: **set ip dscp [af11 | af12 | af13 | af 21 | af 22 | af23 | af31 | af 32 | af 33 | af 41 | af42 | af43]**

You can also set a CS PHB. CS PHBs provide backwards compatibility with IP precedence. Enter this command:

Syntax: **set ip dscp [cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7]**

If you want to remove ToS values from selected packets, you can enter this command:

Syntax: **set ip dscp default**

The EF PHB requests low latency for traffic, as well as a guaranteed amount of bandwidth (set by the administrator of the network into which packets are being forwarded). Enter this command to request EF for selected packets:

Syntax: **set ip dscp ef**

You can also enter a value between 0 and 63 to mark traffic with a DSCP defined in the forwarding network.

The value you set in the route map tags packets for QoS in the remote network, not on the local router. In order to implement QoS functions, such as low latency queuing (LLQ) or class-based weighted fair queuing (CBWFQ), on an AOS router, you must create QoS maps. (A QoS map can also mark packets with an IP precedence or DiffServ value.)

Note also that the remote network must support the type of service requested by the value you set in the route map.

Setting the Don't Fragment Bit

Packets may travel over a path that includes routers with varying maximum transmit units (MTUs). When a router prepares to forward a packet, it checks the packet's size against the MTU of the link that connects to the next-hop router. If the packet exceeds this MTU, the router fragments the packet. Anytime packets are fragmented, they run the risk of loosing their integrity. This risk increases the more times a packet is fragmented.

You can set the don't-fragment bit in a packet's IP header to prevent devices between the local router and the packet's destination from fragmenting the packet. For example, it is important that VoIP packets are not fragmented. This may also apply to certain vendor or application-specific equipment.

You select packets with a route map entry and then set the don't-fragment bit. Define traffic using Step 1 on page 4 or Step 3 on page 8. For example, if a VoIP application marks packets with an IP precedence value of 5, you could select packets with this value for the route map. You could also select packets destined for the application port used by your VoIP equipment with an extended ACL.

To set the don't-fragment bit for selected packets, enter this command from the Route Map Configuration mode:

Syntax: **set ip df**

Setting the don't-fragment bit can cause problems. If a packet is larger than the MTU of a link over which it must pass and the router attempting to forward the packet cannot fragment the packet, the router will drop the packet. Typically, the router will also return an Internet Control Message protocol (ICMP) packet informing the host that sent the packet that the packet was too large. However, some systems have firewalls that prevent routers from sending the ICMP message.

If packets will be traveling through the Internet or other external network with policies you cannot control, setting the don't-fragment bit can cause packets to be dropped. However, if the local router is forwarding packets into a remote network under your organization's control, you can often set the don't-fragment bit without fear. You should be certain that all routers in your organization have compatible MTUs.

Step 5: Apply the policy to an interface

In order to activate a routing policy, you must associate the route map with an Ethernet or WAN interface. The router matches incoming packets to the route map and, if it finds a match, routes them as indicated in the map. Otherwise, the router looks up the forwarding interface for the packet in its routing table as usual.

In other words, the router decides how to route outgoing traffic to the Internet or a remote site according to the route maps applied to the Ethernet interfaces. It decides how to route incoming traffic to the LAN according to the route maps applied to WAN interfaces.

PBR on an AOS router is primarily designed to route traffic over WAN connections in the most cost-effective manner. Therefore, you will usually apply route maps to Ethernet interfaces.

For optimum performance, FFE must be enabled on all interfaces that have a route map applied.

To apply the route map, move to the interface configuration mode and enter this command:

Syntax: **ip policy route-map** <*name*>

The following example applies the route map named **Outbound** and enables FFE to the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#ip policy route-map Outbound**

(config-eth 0/1)**#ip ffe**

Only one route map can be applied to an interface at a time. You can create multiple sequence numbers within the same route map to account for the various scenarios applicable to your network. The sequence numbers within a route map are processed in numerical order and are displayed in this fashion when viewing the running configuration of a unit.

Applying a Route Map to Router Traffic

You can also configure routing policies for traffic generated by the router itself. This can be useful for routing protocols, certain command line interface (CLI) commands, router management traffic, and certain AOS features. The Network Monitor feature added in AOS 13.01.00 requires a route map be applied to the local policy of the router.

Configure a route map as described for applying PBR to network traffic. Then apply the route map to local router traffic with this Global Configuration mode command:

Syntax: **ip local policy route-map** <*mapname*>

PBR Configuration Examples

Example 1 - Routing Traffic to a Security Appliance

You might configure PBR on your router when your network uses a security appliance (such as an IDS) to monitor traffic from untrusted internal hosts.

In this example, a university uses an AOS router to connect to the Internet. The university wants to provide the many resources of the Internet to both its students and its faculty. However, the administration is aware that students, in particular, often pose security risks. Technically savvy students might attempt to hack into servers on the Internet or try to spread viruses.

Therefore, the university has installed an IDS to filter Internet traffic from students and to detect and prevent misuse of the Internet connection. The router should forward all student traffic destined to the Internet to the IDS. After processing the traffic, the IDS will return the traffic to the router to be sent over the Internet.

So that the IDS is not overburdened, the router is allowed to forward traffic from trusted hosts directly to the Internet. The university defines faculty as trusted hosts.

You would configure PBR on the university's AOS router so that the router will distinguish between traffic from faculty and from students and route such traffic differently. (See Figure 1.)

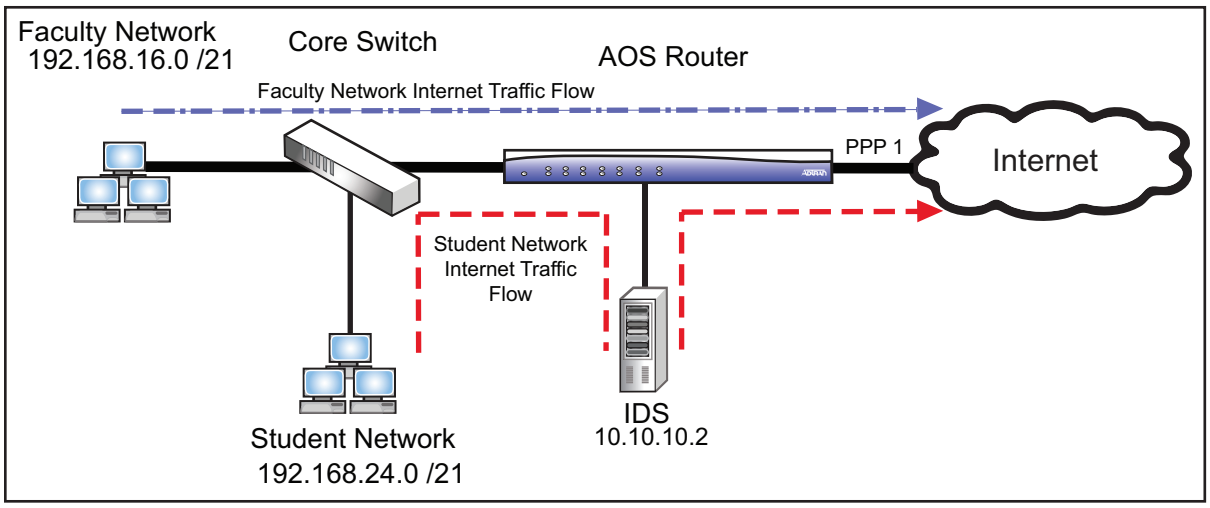

Figure 1. IDS Internet Traffic Filter Example

In this example, students and faculty are assigned to two different subnets within the 192.168.0.0 /16 network that are both accessible via interface Ethernet 0/1. You would need to configure an ACL to select traffic from student subnets for source-based PBR.

The router must send the student traffic to the university's IDS off of interface Ethernet 0/2. You could configure the IDS appliance's IP address (10.10.10.2) as the next-hop address. After the IDS approves the traffic, network address translation (NAT) will occur to change the source IP address of the traffic from the corresponding student's IP address to the public IP address assigned to interface PPP 1. The faculty's network traffic will automatically be NATed to the interface PPP 1 address to go directly out to the Internet instead of being directed to the IDS for approval.

If the router could also reach the IDS through a backup connection, you could specify this backup route by adding a secondary next-hop address or forwarding interface to the **set** command entered for the route map.

In this example, the AOS router uses a default route to forward external traffic. Because you want the router to apply PBR only to external student traffic, you would enter the route map as a default policy. That is, if a packet from a student host has a local destination for which the router has an explicit route in its routing table, the router will not apply PBR to the packet. This allows student hosts to communicate directly with local network servers, which have other security devices protecting them.

You would enter these commands to configure PBR:

(config)**#ip access-list standard students**

(config-std-nacl)**#permit 192.168.24.0 0.0.7.255**

(config-std-nacl)**#exit**

(config)**#route-map Internet 10**

(config-route-map)**#match ip address students**

(config-route-map)**#set default next-hop 10.10.10.2**

(config-route-map)**#exit**

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#ip policy route-map Internet**

(config-eth 0/1)**#ip ffe**

If an IDS is used that does not act as a proxy by changing the source IP address of the packets, and the IDS is placed on a different interface than where the web traffic is originating (like in this example), the reverse path forwarding (RFP) firewall check needs to be disabled on the policy class applied to the interface where the IDS resides. This is done with the following command from Global Configuration mode:

Syntax: **no ip policy-class** <*name*> **rpf-check**

This will prevent the firewall from dropping packets that look like they are spoofed because they are coming in on the wrong interface for the given subnet according to the router's routing table. If the IDS is placed on a DMZ or a non-isolated segment from the Internet, disabling the RFP check can be a security risk. It is highly recommended that the IDS be placed on either the same subnet the traffic is originating from (on the student network for this example) or on another private interface that is isolated from the Internet.

The following firewall related commands are needed if the IDS does not proxy and it is placed on a segment isolated from the Internet:

(config)**#ip access-list standard MATCHALL**

(config-std-nacl)**#permit any**

(config-std-nacl)**#exit**

(config)**#ip firewall**

(config)**#ip policy-class Private**

(config-policy-class)**#allow list MATCHALL self**

(config-policy-class)**#allow list MATCHALL policy IDS**

(config-policy-class)**#nat source list MATCHALL interface ppp 1 overload**

(config-policy-class)**#exit**

(config)**#ip policy-class IDS**

(config-policy-class)**#allow list MATCHALL self**

(config-policy-class)**#nat source list MATCHALL interface ppp 1 overload policy Public**

(config-policy-class)**#exit**

(config)**#no ip policy-class IDS rpf-check**

(config)**#ip policy-class Public**

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#access-policy Private**

(config-eth 0/1)**#interface ethernet 0/2**

(config-eth 0/2)**#access-policy IDS**

(config-eth 0/2)**#interface ppp 1**

(config-ppp 1)**#access-policy Public**

Policy classes, NAT, and other firewall related topics are beyond the scope of this document. For more information about the firewall, please refer to other AOS resources.

Example 2 - Routing Traffic to a Caching Server

Your organization may place a caching server between its AOS router and its Internet Service Provider (ISP). A caching server stores frequently requested web pages to increase performance; hosts can receive the web page directly from the caching server instead of from a remote server.

You can use PBR to forward some of your network's Internet traffic to a caching server. First, decide which types of traffic should be sent to the caching server. For example, you might want to select external traffic from a defined subnet employees use since many of them use the same web sites for work. (See Figure 2.)

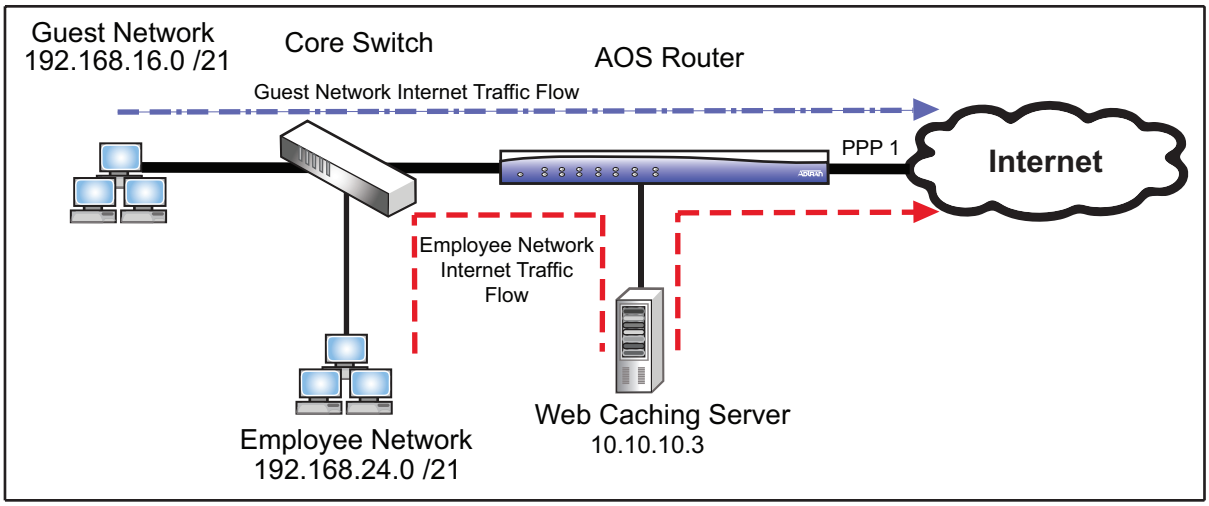

Figure 2. Web Caching PBR Example

Configure an ACL to select the traffic and match the ACL to a route map with commands like those illustrated in *Example 1 - Routing Traffic to a Security Appliance* on page 19. Then specify a route to the caching server (10.10.10.3).

For example, enter:

(config)**#ip access-list standard employee**

(config-std-nacl)**#permit 192.168.24.0 0.0.7.255**

(config-std-nacl)**#exit**

(config)**#route-map Internet 10**

(config-route-map)**#match ip address employee**

(config-route-map)**#set default next-hop 10.10.10.3**
(config-route-map)**#exit**
(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip policy route-map Internet**
(config-eth 0/1)**#ip ffe**

Example 3 - Reserving a Connection for VoIP and Video Traffic

You could use PBR to reserve a connection for VoIP traffic, which requires low latency. You could also reserve a connection for mission-critical traffic.

For example, an organization uses cost-effective Frame Relay connections between its headquarters and branch offices. The branch offices exchange data with servers at the headquarters over these connections.

Employees at the headquarters and at one of the branch offices frequently use VoIP to communicate. When the Frame Relay network is congested, the QoS for this real time traffic is seriously degraded. The organization decides to install a PPP connection between the headquarters and this branch office. You could configure PBR on the headquarters and branch office WAN routers to reserve this connection for the real time traffic. (See Figure 3.)

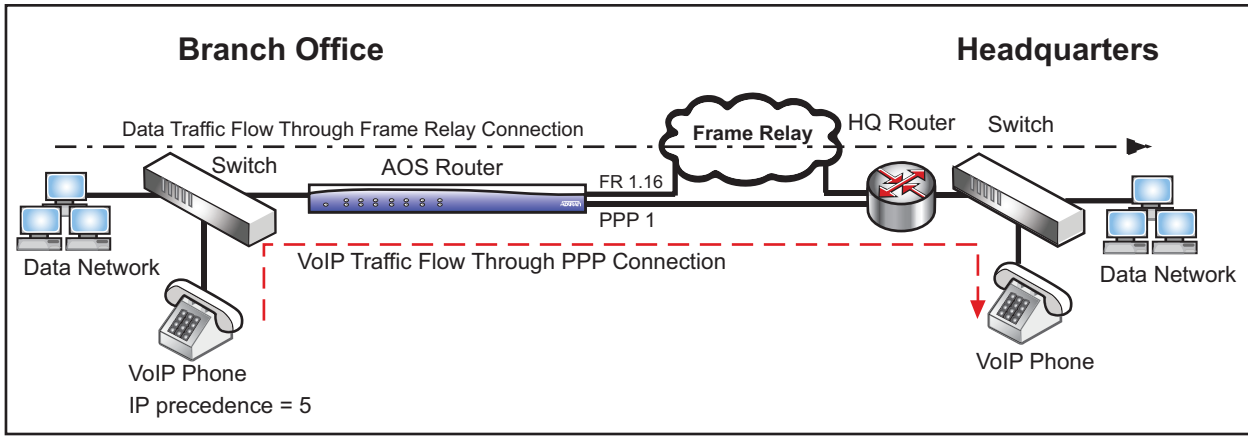

Figure 3. VoIP PBR Example

This example explains how to configure PBR on the branch office router.

If the VoIP and video applications mark real time traffic with a QoS value, you can use this value to select the traffic. Otherwise, you can configure an extended ACL to select traffic destined to UDP Real Time Protocol (RTP) ports. In this example, the applications mark traffic with an IP precedence of 5.

In this example, the routing protocol implemented on the AOS router has selected the Frame Relay connection to route traffic to the headquarters. You can override this selection for real time traffic.

All real time traffic is destined for the headquarters, so it can be routed out the PPP interface that connects to the headquarters.

In this example, the headquarters network uses DiffServ. The branch office router can mark real time packets with the DSCP for the EF PHB. The branch office router can also set the DF bit for the packets so that intervening routers will not fragment them.

Configure the route map as follows:

(config)**#route-map RealTime 10**

(config-route-map)**#match ip precedence 5**

(config-route-map)**#set interface ppp 1**

(config-route-map)**#set ip dscp ef**

(config-route-map)**#set ip df**

(config-route-map)**#exit**

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#ip policy route-map RealTime**

(config-eth 0/1)**#ip ffe**

Example 4 - Reserving a Connection for FTP Traffic

Since FTP traffic can potentially saturate a WAN connection, your organization may want to reserve this traffic to flow over a separate connection to a remote site to prevent other, more time-sensitive traffic from getting dropped.

For example, if a server at a remote branch location periodically uses FTP to backup large files to a server at headquarters, you may want this traffic to be sent over a lower speed Frame Relay connection rather than a more expensive point-to-point connection that is used for time-sensitive traffic for voice and video. (See Figure 4.)

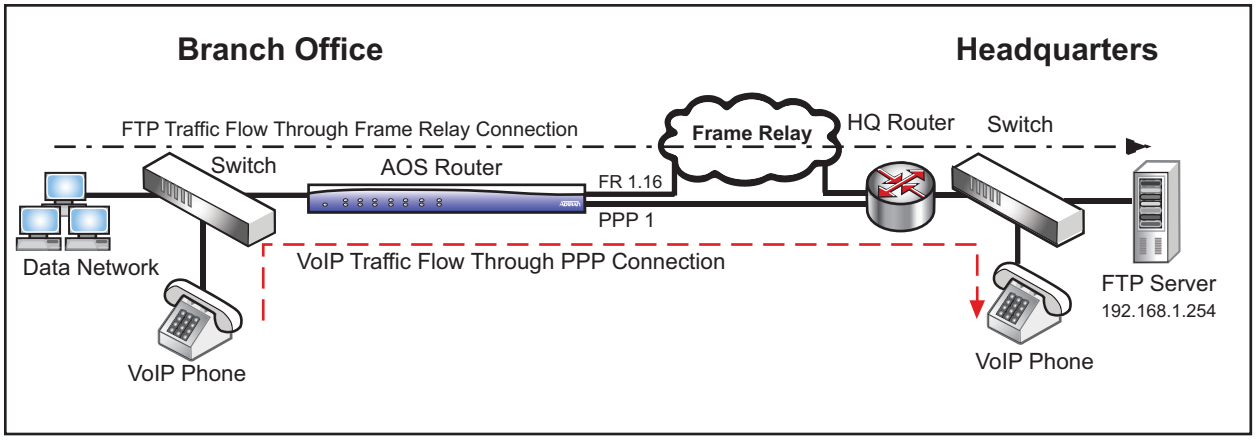

Figure 4. FTP PBR Example

This example assumes that the routing table primarily uses interface PPP 1 to reach headquarters from the remote branch. A lower speed Frame Relay connection also connects the remote branch and headquarters together. The FTP server at headquarters has an IP address of 192.168.1.254.

Configure the remote branch router as follows:

(config)**#ip access-list extended FTP**

(config-ext-nacl)**#permit tcp any host 192.168.1.254 eq ftp**

(config-ext-nacl)**#permit tcp any host 192.168.1.254 eq ftp-data**

(config-ext-nacl)**#exit**

(config)**#route-map LOWSPEED 10**

(config-route-map)**#match ip address FTP**

(config-route-map)**#set interface fr 1.16**

(config-route-map)**#exit**

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#ip policy route-map LOWSPEED**

(config-eth 0/1)**#ip ffe**

The **permit** keyword in the extended ACL above selects traffic for the route map, **tcp** specifies the protocol, **any** indicates that traffic from any host is allowed, **192.168.1.254** gives the address of the FTP server at headquarters, and **eq ftp** and **eq ftp-data** specify the application.

Example 5 - Using PBR to Enforce QoS Across a VPN Connection

PBR can also be used in applications to manipulate the ToS field in packets to ensure their prioritization when encrypted in a virtual private network (VPN) tunnel. In AOS, the VPN engine encrypts packets prior to any QoS handling. As a result, the source and destination address fields within an IP packet are encrypted so they cannot be used to match against within a QoS map. This poses a problem in applications in which voice and data packets are traversing the same VPN tunnel, especially if the voice packets are not natively tagged. Since the PBR engine handles packets prior to the VPN engine, it is possible to use a route map to match based on the source and/or destination fields of the IP packet and then set the ToS bits. The ToS bits are then copied over to the new IP header of the encrypted packet at which point QoS can then effectively prioritize the voice traffic.

For this example, there are employee and executive networks off of interface Ethernet 0/1. The executive network correlates to the 10.10.10.0 /24 subnet, and the employee network correlates to the 10.10.20.0 /24 subnet. Both subnets at this branch office communicate to headquarters through a VPN tunnel. Members of the executive network will receive priority over all other traffic. (See Figure 5 on page 26.)

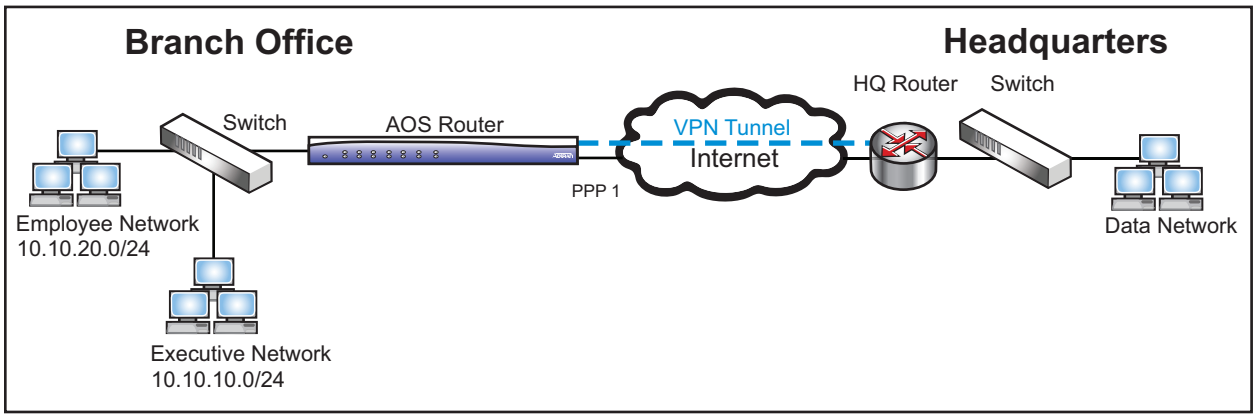

Figure 5. Using PBR to Enforce QoS Over a VPN Example

It is assumed that QoS is applied to the PPP 1 interface of the branch office AOS router, giving packets with a DSCP value of 46 unlimited priority. It is also assumed that the branch office AOS router is appropriately configured for VPN to headquarters and the corresponding crypto map is applied to the PPP 1 interface.

All of the traffic from the remote branch to headquarters is encrypted, preventing the router from distinguishing between executive and employee network packets when the packets hit the QoS engine. PBR can be used to set the ToS bits of packets sourced from the executive network so they will maintain their integrity after encryption, allowing the QoS engine to prioritize them.

The remote branch router must be configured as follows to allow the executive network traffic to be prioritized over a VPN tunnel:

(config)**#ip access-list standard executive**

(config-std-nacl)**#permit 10.10.10.0 0.0.0.255**

(config-ext-nacl)**#exit**

(config)**#route-map PRIORITY 10**

(config-route-map)**#match ip address executive**

(config-route-map)**#set dscp 46**

(config-route-map)**#exit**

(config)**#interface ethernet 0/1**

(config-eth 0/1)**#ip policy route-map PRIORITY**

(config-eth 0/1)**#ip ffe**

PBR Quick Configuration Guide

1. Determine what criteria the router should use for routing packets. The AOS router can route packets based on
   - Standard or extended ACL match
   - IP precedence
   - DiffServ
   - Layer 3 packet length
   - Traffic originating from the router
2. If the router will be routing traffic based on source IP address only, you must configure a standard ACL to select the traffic.
   a. Create the ACL.

      Syntax: **ip access-list standard** <*name*>

   b. Use **permit** statements to specify the hosts, hostnames, networks, or range of networks from which the traffic that is to be routed using PBR will originate. If necessary, first enter a **deny** statement to exclude one or more addresses from a permitted range to which the PBR should not be applied. Use this command to add a statement to the list:

      Syntax: **[deny | permit] [any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>]
3. If the router will be routing traffic according to source and destination IP address or application data, you must create an extended ACL.
   a. Create the ACL.

      Syntax: **ip access-list extended** <*name*>

   b. Use **permit** statements to specify allowed traffic and **deny** statements to exclude traffic.

      Syntax: **[deny | permit] ip [any | host** <*ip address*> **| hostname** <*name*> **|** <*ip address*> <*wildcard mask*>**] [any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>**]**

   For the first address, enter the source of traffic to be routed using PBR. For the second address, enter the traffic's ultimate destination.

   c. If the router should route packets based on application data, the **permit** statement you enter must include the protocol for the application and the source or destination port, or both. Use this command:

      Syntax: **[permit | deny]** <*protocol*> **[any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>**] [eq** <*port*> **| gt** <*port*> **| lt** <*port*> **| range** <*first port*> <*last port*> **| neq** <*port*>**] [any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>**] [eq** <*port*> **| gt** <*port*> **| lt** <*port*> **| range** <*first port*> <*last port*> **| neq** <port>**]**

4. Create a route map entry. From the Global Configuration mode, enter:

   Syntax: **route-map** <*name*> <*permit*> <*sequence number*>

5. Specify the traffic the router should use PBR to route. Use **match** commands to configure the criteria you determined in step 1. If you enter more than one type of **match** command, traffic must match all the criteria. If you do not enter a **match** command, all traffic will match the route map entry.

   a. To route traffic based on source IP address, source and destination address, or application data, specify the ACL you configured in step 2 or step 3.

      Syntax: **match ip address** <*name*>

   b. To route traffic based on IP precedence value, enter this command:

      Syntax: **match ip precedence [critical | flash | flash-override | immediate | internet | network | priority | routine |** <*0-7*>**]**

   Select the value by number or by keyword. Packets should already be marked with the value by devices within your LAN.

   c. To route traffic based on DiffServ value, enter this command:

      Syntax: **match ip dscp [af11 | af12 | af13 | af 21 | af 22 | af23 | af31 | af 32 | af 33 | af 41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef |** <*0-63*>**]**

   You can select default traffic (no DiffServ value set); traffic in a CS PHB, a AF PHB, or the EF PHB; or traffic marked with any DiffServ value defined within your network.

   d. To route traffic based on the payload size (in bytes), enter this command:

      Syntax: **match length** <*minimum length*> <*maximum length*>

   > NOTE *FFE cannot be utilized to increase router performance when packets are matched with the* ***match length*** *command.*

6. Set the next-hop address or the forwarding interface for the PBR:

   a. To set a next-hop address, enter this command:

      Syntax: **set ip [default] next-hop** <*ip address*> <*secondary ip address*>

   If you enter the **default** keyword, the router will only use this PBR to forward a packet when its routing table does not include an explicit route for the packet's destination. You can enter more than one next-hop address in the command to provide a backup route. The router first attempts to route traffic to the first address listed, and then tries the others.

   b. To set a forwarding interface for the PBR, enter this command:

      Syntax: **set [default] interface** <*interface id*> <*secondary interface id*>

You can specify multiple possible forwarding interfaces. Again, the optional **default** keyword forces the router to use its routing table to forward a packet when this table contains an explicit route for the packet's destination.

c. You can enter more than one **set** command. The router will attempt to route traffic as follows:
   - First, to any adjacent next-hop address
   - Then, through any forwarding interface
   - Then, to any default next-hop address
   - Last, through any default forwarding interface

When viewing the running configuration of a unit, the **set** commands will appear in the order of operation.

7. You can configure multiple route map entries with the same name to establish multiple PBRs for traffic arriving on an interface. Repeat the previous steps and reference the same route map name, but change the sequence number. Sequence numbers are processed in numerical order.
8. Apply the route map to LAN interfaces to enable PBR for traffic outbound to the WAN. (This is the typical application.) You can also apply route maps to any logical interface. Move to the Ethernet or logical interface configuration mode and enter this command:

   Syntax: **ip policy route-map** <*name*>

   

   An interface must have an IP address in order for you to assign a route map to it.

9. Enable the AOS FFE to the same interface to which the route map was applied. This will greatly enhance router performance when using PBR. Move to the Ethernet or logical interface configuration mode from the last step and enter this command:

   Syntax: **ip ffe**

   

   *FFE cannot be utilized to increase router performance when packets are matched with the **match length** command.*

Command Summary Table

	Command	Description
Step 1	If using an ACL for **match** criteria (refer to Step 3), create a standard or extended ACL. If using DSCP, IP precedence, or length as the match criteria, proceed to Step 2.	
(Standard ACL)	(config)**#ip access-list standard** <*name*> (config-std-nacl)**#deny [host** <*ip address*> **| hostname** <*name*> **|** <*ip address*> <*wildcard mask*>**]** (config-std-nacl)**#permit [any | host** <*ip address*> **| hostname** <*name*> **|**<*ip address*> <*wildcard mask*>**]** (config-std-nacl)**#exit**	Create a standard ACL if traffic to be routed will be based on source IP address only. Use **deny** to exclude addresses that PBR should not be applied to from the permitted range. Use **permit** to allow traffic from the host, network, or range of networks that you want to route using PBR.
(Extended ACL)	(config)**#ip access-list extended** <*name*> (config-ext-nacl)**#deny ip [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>**] [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>] (config-ext-nacl)**#permit ip [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>**] [any | host** <*ip address*> **| hostname** <*name*>**|** <*ip address*> <*wildcard mask*>**]** (config-ext-nacl)**#exit**	Create an extended ACL if traffic to be routed will be based on source and destination IP addresses or application data. Use **deny** to exclude addresses that PBR should not be applied to from the permitted range. Use **permit** to allow traffic from the host, network/range of networks, or protocol and source/destination ports that you want to route using PBR.
Step 2	(config)**#route-map** <*name*> **[permit | deny]** <*sequence number*>	Create a route map entry.
Step 3	(config-route-map)**#match ip address** <*ACL name*> *or* (config-route-map)**#match ip precedence** [<*keyword*> | <*value*>] *or* (config-route-map)**#match ip dscp** [<*AF class*> | <*CS class*> | **default** | **ef** | <*value*>] *or* (config-route-map)**#match length** <*minimum length*> <*maximum length*>	The **match** commands can be used to specify the traffic the router should use PBR to route. This can be done by referencing the ACL created in Step 1 (if applicable), IP precedence value, DiffServ value, or payload size. If more than one **match** command is issued, traffic must meet all the **match** conditions to be eligible for PBR. Refer to Step 3 on page 8 for more information on **match** commands.

	Command	Description
Step 4	(config-route-map)**#set ip next-hop** <*ip address*> [<*secondary ip address*>] *or* (config-route-map)**#set interface** <*interface id*> [<*secondary interface id*>] *or* (config-route-map)**#set ip default next-hop** <*ip address*> [<*secondary ip address*>] *or* (config-route-map)**#set default interface** <*interface id*> [<*secondary interface id*>] *or* (config-route-map)**#set ip precedence** <*keyword*> | <*value*> *or* (config-route-map)**#set ip dscp** [<*AF class*> | <*CS class*> | **default** | **ef** | <*value*>] *or* (config-route-map)**#set ip df**	Use the **set** commands to define the next hop address or the forwarding interface for the policy-based route. Multiple **set** commands can be used to further define the actions of PBR. Refer to Step 4 on page 13 for more information on **set** commands.
Step 5	Repeat Steps 1 through 4 to establish multiple PBRs.	Establish multiple PBRs for traffic arriving on an interface. Repeat Steps 1 through 4 referencing the same route map name in Step 2, but changing the sequence number. Route map sequence numbers are processed in numerical order
Step 6	(config)**#interface ethernet 0/1** (config-eth 0/1)**#ip policy route-map** <*name*>	Apply the route map to the IP interface closest to the source of the traffic desired for PBR.
Step 7	(config-eth 0/1)**#ip ffe**	Enhance router performance when using PBR by enabling AOS FFE to the same interface the route map was applied to.

Troubleshooting

After configuring PBR, several different commands can be issued from the Enable mode in the CLI to assist in troubleshooting. Table 6 contains the AOS troubleshooting commands that are implemented specifically for PBR.

Table 6. AOS PBR Troubleshooting Commands

Command	Explanation
show ip policy	Displays the interfaces to which route maps are applied
show route-map <*route-map name*>	Displays the applicable route map name, sequence number(s), corresponding match and set clauses, and number of times each clause has been matched
show ip local policy	Displays the applicable route map name, sequence number(s), corresponding match and set clauses, and number of times each clause has been matched for local router originated traffic
clear route-map counters <*name*>	Clears the counters on all or a specified route map
debug ip policy	Displays PBR events with the corresponding source address/interface, destination address/interface, Layer 3 length, and applicable route map

You can view the policies applied to router interfaces with the **show ip policy** command:

Example output:

```
#show ip policy
Interface       Route-map
---------       ---------
local           SOURCE
eth 0/2         SOURCE
```

If **local** appears in the list, the corresponding route map has been applied to traffic generated by the router.

You can view the actual configured policies in the route maps with the **show route-map [**<*name*>**]** command; if you do not specify a map name, all configured route maps will be displayed.

Example output:

```
#show route-map
route-map SOURCE, permit, sequence 10
 Match clauses:
   ip address (access-lists): VOICE
 Set clauses:
   ip dscp 46
   interface: ppp 1
 BGP Filtering matches: 0 routes
 Policy routing matches: 122 packets 8912 bytes
 Redistribution Filtering matches: 0 routes
route-map SOURCE, permit, sequence 20
 Match clauses:
   ip address (access-lists): GUEST
 Set clauses:
   ip next-hop: 10.19.127.50
 BGP Filtering matches: 0 routes
 Policy routing matches: 51 packets 3504 bytes
 Redistribution Filtering matches: 0 routes
route-map LENGTH, permit, sequence 10
 Match clauses:
   length 0 200
 Set clauses:
   interface: frame-relay 1.16
 BGP Filtering matches: 0 routes
 Policy routing matches: 5 packets 128 bytes
 Redistribution Filtering matches: 0 routes
```

The display lists entries in the route maps by sequence number. The entries are further divided into match clauses (which show the criteria the map uses to select packets) and set clauses (which show the next-hop address or forwarding interface for the PBR route). The policy routing matches in packets and in bytes by sequence number can be viewed in this output as well. This is where you can verify that packets are matching the specified criteria.

The **clear route-map counters [**<*name*>**]** command can be issued to clear the policy routing matches on a particular route map. If no map name is specified, the counters will be cleared for all configured route maps.

The **show ip local policy** command displays the policy applied to router traffic (if any). This will show all of the relevant information from the **show route-map** command, but only for the route map applied to the local policy.

Example output:

```
#show ip local policy
Local policy routing is enable, using route-map LENGTH
route-map LENGTH, permit, sequence 10
 Match clauses:
   length 0 200
 Set clauses:
   interface: frame-relay 1.16
 BGP Filtering matches: 0 routes
 Policy routing matches: 133 packets 6575 bytes
 Redistribution Filtering matches: 0 routes
```

The output **Local policy routing is disabled** will be displayed if there is no route map applied to traffic generated by the router.

The **debug ip policy** command can be issued to view PBR events in real time. This output follows the format below:

[time stamp] : route map [map name], item [sequence number], [permit | deny]

[time stamp] : IP: s=[source IP] ([source interface]), d=[destination IP] ([destination interface]), len [Layer 3 length], [PBR information]

As shown above, there are two different messages output for each PBR event. The first message is used to tell which route map name and sequence number was applied to the traffic. The second message lists the source and destination IP addresses, corresponding interfaces used by the router, packet length, and the relevant PBR information.

The PBR information keywords and their explanations are listed below.

The keywords **policy routed via next-hop** will be displayed when the packet was routed according to one of the IP addresses specified with the **set ip next-hop** command.

The keywords **policy routed via default next-hop** will be displayed when the packet was routed according to one of the IP addresses specified with the **set ip default next-hop** command.

The keywords **policy routed via interface** will be displayed when the packet was routed according to one of the interfaces specified with the **set interface** command.

The keywords **policy routed via default interface** will be displayed when the packet was routed according to one of the interfaces specified with the **set default interface** command.

When a packet was routed according to the **set interface** command or **set default interface** command, the egress interface will be indicated in parenthesis after the destination address. If the egress interface shows **null 0**, the packet was dropped by the router.

The keywords **policy routed normally** will be displayed when the packet was routed normally according to the route table. This message will be displayed if a packet matches the conditions of the specified criteria and there are no **set interface**, **set default interface**, **set ip next-hop**, or **set ip default next-hop** commands specified. It will also be displayed if the applicable forwarding interfaces from these **set** commands are not available.

The keywords **(sets used)** will be displayed and appended to one of the PBR information keywords listed above when the **set ip dscp**, **set ip precedence**, or **set ip df** commands have been applied to the packet. It is possible for more than one of these **set** commands to be applied to the packet at a time when this message is displayed.

The keywords **policy reject** will be displayed when traffic matches a route map **deny** entry or traffic matches a route map **permit** entry that specifies an ACL, and the traffic matches a **deny** statement in the ACL. This message will also be displayed if there are multiple **set** commands specified and the criteria do not meet them all.

*Issuing the **debug ip policy** command can be very processor intensive and should be used with caution. The resulting debug output can be very large, depending on the traffic load applicable to PBR.*

Troubleshooting Steps

You can verify that traffic can reach its destination by applying the route map to router traffic with this Global Configuration mode command:

#ip local policy route-map <*name*>

First clear the route map statistics so that you can later verify that the router is matching the traffic to the route map. Enter:

#clear route-map counters

Then send a ping to the desired destination using the extended commands so that the ping matches the criteria specified in the route map.

For example, if traffic was selected to match when the Layer 3 packet size is between 150 and 200 bytes, you could enter this command from the Enable mode:

#ping size 150

*FFE cannot be utilized to increase router performance when packets are matched with the **match length** command.*

You can also select a source address for ping so that you can simulate the traffic for source-based PBR. If the ping is not successful, you should look for misconfigurations in the set clauses. Verify that specified interfaces are up and that the router's routing table includes a route to the next-hop address.

A successful ping does not necessarily mean that traffic used the correct interface.

View the route map by entering **show route-map** and verify that the pings have generated **Policy routing matches**. This is illustrated in *After configuring PBR, several different commands can be issued from the Enable mode in the CLI to assist in troubleshooting. Table 6 contains the AOS troubleshooting commands that are implemented specifically for PBR.* on page 32.

If the router is not matching any packets to the entries, you should verify that the route map has been applied to the correct interface by issuing the **show ip policy** command. Route maps for PBR apply to traffic received on the interface.

You should also look for misconfigurations in the match clauses. One common problem is a misconfigured ACL.

Remember also that if you specify more than one type of criterion in an entry, traffic must match each specification. For example, you enter:

(route-map)**#match length 150 200**

(route-map)**#match ip precedence 5**

This route map entry only selects packets that are both the correct size and have the correct IP precedence value. If a packet only met one of these conditions, the PBR information keywords **policy reject** would be displayed in a **debug ip policy** output assuming there were no other route map sequence numbers the traffic would match.

If you are using source-based PBR only, you can use this **traceroute** command to determine the path the traffic is taking:

Syntax: **traceroute** <*destination ip address*> **source** <*ip address*>

Another common problem that occurs with PBR is that traffic that should be routed normally is being sent over the PBR. In this situation, you consider whether the route map's **set** commands should use the **default** keyword so that it only applies to traffic without another explicit route. Often this is the case when you are using the route map to route and load balance external traffic. You should also check the route map's match clauses for misconfigurations.

If an entry does not include a match clause, it will select all traffic.

