



Using Performance Routing to Profile the Traffic Classes

First Published: July 11, 2008

Last Updated: July 11, 2008

This module describes how Performance Routing (PfR) profiles the traffic classes. To optimize traffic routing, subsets of the total traffic must be identified, and these traffic subsets are named traffic classes. The PfR master controller can profile traffic classes either by manual configuration on the master controller or by automatic learning on the basis of parameters such as throughput or delay characteristics of traffic on the border routers. Automatic learning requires traffic class parameters to be configured on the master controller.



Note

Performance Routing is an extension of the Optimized Edge Routing (OER) technology and many of the commands and command modes use the OER naming conventions. If you are running Cisco IOS Release 12.4(11)T, 12.2(33)SXH, 12.2(33)SRB or earlier releases, see the [“Using OER to Profile the Traffic Classes”](#) module for configuration information and tasks appropriate to your release.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Using PfR to Profile the Traffic Classes”](#) section on page 47.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007–2009 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Using PfR to Profile the Traffic Classes, page 2](#)
- [Restrictions for Using PfR to Profile the Traffic Classes, page 2](#)
- [Information About Using PfR to Profile the Traffic Classes, page 2](#)
- [How to Configure PfR to Profile the Traffic Classes, page 11](#)
- [Configuration Examples for Using PfR to Profile the Traffic Classes, page 40](#)
- [Where To Go Next, page 45](#)
- [Additional References, page 45](#)
- [Feature Information for Using PfR to Profile the Traffic Classes, page 47](#)

Prerequisites for Using PfR to Profile the Traffic Classes

- Before implementing the PfR profile phase, you need to understand an overview of how PfR works and how to set up PfR network components. See the [“Cisco IOS Optimized Edge Routing Overview”](#) and [“Setting Up OER Network Components”](#) modules for more details.
- Cisco Express Forwarding (CEF) must be enabled on all participating devices. No other switching path is supported, even if otherwise supported by PBR.

Restrictions for Using PfR to Profile the Traffic Classes

If any of the border routers is a Cisco Catalyst 6500 switch or a Cisco 7600 series router, there are some hardware constraints and the master controller will set the monitoring mode to special where only the throughput method of learning is used to profile the traffic classes. If both delay and throughput are configured, the master controller will ignore the delay configuration. For more details about the special monitoring mode, see the [“Measuring the Traffic Class Performance and Link Utilization Using OER”](#) module for more details.

Information About Using PfR to Profile the Traffic Classes

To configure the master controller to profile traffic classes, you should understand the following concepts:

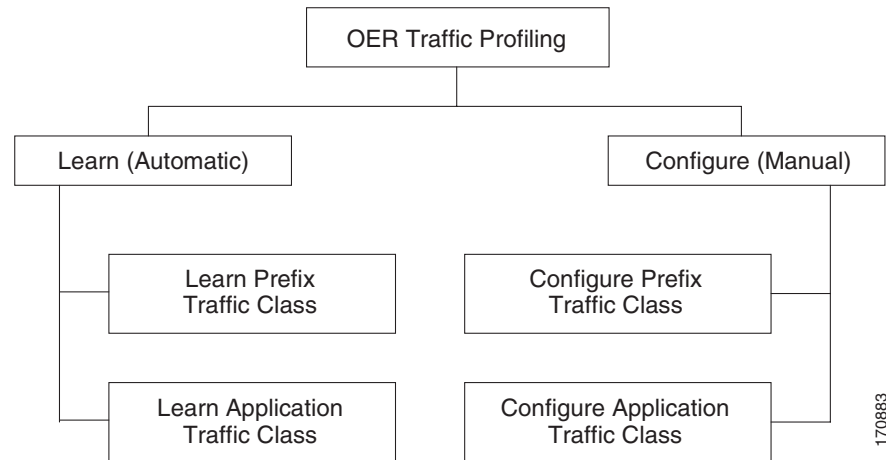
- [PfR Traffic Class Profiling, page 2](#)
- [PfR Automatic Traffic Class Learning, page 3](#)
- [PfR Manual Traffic Class Configuration, page 9](#)

PfR Traffic Class Profiling

Before optimizing traffic, PfR has to determine the traffic classes from the traffic flowing through the border routers. To optimize traffic routing, subsets of the total traffic must be identified, and these traffic subsets are named traffic classes. The list of traffic classes entries is named a Monitored Traffic Class (MTC) list. The entries in the MTC list can be profiled either by automatically learning the traffic

flowing through the device or by manually configuring the traffic classes. Learned and configured traffic classes can both exist in the MTC list at the same time. The PfR profile phase includes both the learn mechanism and the configure mechanism. The overall structure of the PfR traffic class profile process and its component parts can be seen in [Figure 1](#).

Figure 1 PfR Traffic Class Profiling Process



The ultimate objective of this phase is to select a subset of traffic flowing through the network. This subset of traffic—the traffic classes in the MTC list—represents the classes of traffic that need to be routed based on the best performance path available.

More details about each of the components in [Figure 1](#) are contained in the following concepts:

- [PfR Automatic Traffic Class Learning, page 3](#)
- [PfR Manual Traffic Class Configuration, page 9](#)

PfR Automatic Traffic Class Learning

PfR can automatically learn the traffic classes while monitoring the traffic flow through border routers. Although the goal is to optimize a subset of the traffic, you may not know all the exact parameters of this traffic and PfR provides a method to automatically learn the traffic and create traffic classes by populating the MTC list. Several features have been added to PfR since the original release to add functionality to the automatic traffic class learning process.

Within the automatic traffic class learning process there are now three components. One component describes the automatic learning of prefix-based traffic classes, the second component describes automatic learning of application-based traffic classes, and the third component describes the use of learn lists to categorize both prefix-based and application-based traffic classes. These three components are described in the following sections:

- [Prefix Traffic Class Learning Using PfR, page 4](#)
- [Application Traffic Class Learning Using PfR, page 4](#)
- [Learn List Configuration Mode, page 5](#)

Prefix Traffic Class Learning Using PfR

The PfR master controller can be configured, using NetFlow Top Talker functionality, to automatically learn prefixes based on the highest outbound throughput or the highest delay time. Throughput learning measures prefixes that generate the highest outbound traffic volume. Throughput prefixes are sorted from highest to lowest. Delay learning measures prefixes with the highest round-trip response time (RTT) to optimize these highest delay prefixes to try to reduce the RTT for these prefixes. Delay prefixes are sorted from the highest to the lowest delay time.

PfR can automatically learn two types of prefixes:

- outside prefix—An outside prefix is defined as a public IP prefix assigned outside the company. Outside prefixes are received from other networks.
- inside prefix—An inside prefix is defined as a public IP prefix assigned to a company. An inside prefix is a prefix configured within the company network.

In Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, the ability to learn inside prefixes was introduced. Using BGP, PfR can select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. In prior releases, only outside prefixes were supported. Company networks advertise the inside prefixes over the Internet using an Internet service provider (ISP) and receive advertisements for outside prefixes from an ISP.



Note

Although PfR can learn an inside prefix, PfR will not try to control an inside prefix unless there is an exact match in the BGP routing information base (RIB) because PfR does not advertise a new prefix to the Internet.

Automatic prefix learning is configured in OER Top Talker and Top Delay learning configuration mode. The **learn** command is used to enter this mode from PfR master controller configuration mode. When automatic prefix learning is enabled, prefixes and their delay or throughput characteristics are measured on the border routers. Performance measurements for the prefix-based traffic classes are reported to the master controller where the learned prefixes are stored in the MTC list.

Prefixes are learned on the border routers through monitoring the traffic flow using the embedded NetFlow capability. All incoming and outgoing traffic flows are monitored. The top 100 flows are learned by default, but the master controller can be configured to learn up to 2500 flows for each learn cycle. The master controller can control a maximum of 5000 prefixes.

The master controller can be configured to aggregate learned prefixes based on type, BGP or non-BGP (static). Prefixes can be aggregated based on the prefix length. Traffic flows are aggregated using a /24 prefix length by default. Prefix aggregation can be configured to include any subset or superset of the network, from single host route (/32) to a major network address range. For each aggregated prefix, up to five host addresses are selected to use as active probe targets. Prefix aggregation is configured with the **aggregation-type** command in OER Top Talker and Delay learning configuration mode.

Application Traffic Class Learning Using PfR

In the first release of OER, Cisco IOS Release 12.3(8)T, only Layer 3 prefixes could be learned. In subsequent releases, Layer 4 options such as protocol or port numbers were added as filters to the prefix-based traffic class. The protocol and port numbers can be used to identify specific application traffic classes; protocol and port number parameters are monitored only within the context of a prefix and are not sent to the master controller database (MTC list). The prefix that carries the specific traffic

is then monitored by the master controller. In Cisco IOS Release 12.4(9)T, Release 12.2(33)SRB, and later releases, application traffic class learning supports Differentiated Services Code Point (DSCP) values in addition to protocol and port numbers, and these Layer 4 options are entered in the MTC list.

DSCP Value, Port, and Protocol Learning by PfR

In Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, the ability to filter and aggregate application traffic by DSCP value, port number or protocol was introduced. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values. The ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested, was introduced. Information such as protocol, port number, and DSCP value is now sent to the master controller database in addition to the prefix information. The new functionality allows PfR to both actively and passively monitor application traffic. Using new CLI and access lists, PfR can be configured to automatically learn application traffic classes.

Learn List Configuration Mode

In Cisco IOS Release 12.4(15)T, a new configuration mode named learn list was introduced. Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria including prefixes, application definitions, filters, and aggregation parameters for learning traffic classes can be configured. A traffic class is automatically learned by PfR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PfR policies to be applied to each learn list; in previous releases, the traffic classes could not be divided, and an PfR policy was applied to all the learned traffic classes.

New **traffic-class** commands were introduced under learn list mode to simplify the learning of traffic classes. Four types of traffic classes—to be automatically learned—can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name with optional prefix lists to define destination prefixes
- Traffic classes based on a NBAR application mapping name with optional prefix lists to define destination prefixes (introduced in Cisco IOS Release 12.4(20)T)

Only one type of **traffic-class** command can be specified per learn list, and the **throughput** and **delay** commands are also mutually exclusive within a learn list.

Static Application Mapping Using PfR

In Cisco IOS Release 12.4(15)T, the ability to define an application using a keyword was introduced to simplify the configuration of application-based traffic classes. PfR uses well-known applications with fixed ports, and more than one application may be configured at the same time. The list of static applications available for profiling Performance Routing traffic classes is constantly evolving. Use the **traffic-class application ?** command in Cisco IOS Release 12.4(15)T, and later releases, to determine if a static application is available for use with Performance Routing.

[Table 1](#) displays a partial list of static applications that can be configured with Performance Routing. The applications are considered static because they are defined with fixed port and protocols as shown in the table. Configuration is performed on a master controller under learn list configuration mode.

Table 1 **Static Application List**

Application	Keyword	Protocol	Port
CU-SeeMe-Server —CU-SeeMe desktop video conference	cuseeme	TCP UDP	7648 7649 7648 7649 24032
DHCP-Client —Dynamic Host Configuration Protocol client	dhcp (Client)	UDP/TCP	68
DHCP-Server —Dynamic Host Configuration Protocol server	dhcp (Server)	UDP/TCP	67
DNS —Domain Name Server lookup	dns	UDP/TCP	53
FINGER-Server —Finger server	finger	TCP	79
FTP —File Transfer Protocol	ftp	TCP	20, 21
GOPHER-Server —Gopher server	gopher	TCP/UDP	70
HTTP —Hypertext Transfer Protocol, World Wide Web traffic	http	TCP/UDP	80
HTTPSSL-Server —Hypertext Transfer Protocol over TLS/SSL, Secure World Wide Web traffic server	secure-http	TCP	443
IMAP-Server —Internet Message Access Protocol server	imap	TCP/UDP	143 220
SIMAP-Server —Secure Internet Message Access Protocol server	secure-imap	TCP/UDP	585 993 (Preferred)
IRC-Server —Internet Relay Chat server	irc	TCP/UDP	194
SIRC-Server —Secure Internet Relay Chat server	secure-irc	TCP/UDP	994
Kerberos-Server —Kerberos server	kerberos	TCP/UDP	88 749
L2TP-Server —L2F/L2TP tunnel Layer 2 Tunnel Protocol server	l2tp	UDP	1701
LDAP-Server —Lightweight Directory Access Protocol server	ldap	TCP/UDP	389
SLDAP-Server —Secure Lightweight Directory Access Protocol server	secure-ldap	TCP/UDP	636
MSSQL-Server —MS SQL server	mssql	TCP	1443
NETBIOS-Server —NETBIOS server	netbios	UDP TCP	137 138 137 139
NFS-Server —Network File System server	nfs	TCP/UDP	2049
NNTP-Server —Network News Transfer Protocol	nntp	TCP/UDP	119
SNNTP-Server —Network News Transfer Protocol over TLS/SSL	secure-nntp	TCP/UDP	563
NOTES-Server —Lotus Notes server	notes	TCP/UDP	1352
NTP-Server —Network Time Protocol server	ntp	TCP/UDP	123
PCanywhere-Server —Symantec pcANYWHERE	pcany	UDP TCP	22 5632 65301 5631

Table 1 **Static Application List (continued)**

Application	Keyword	Protocol	Port
POP3-Server —Post Office Protocol server	pop3	TCP/UDP	110
SPOP3-Server —Post Office Protocol over TLS/SSL server	secure-pop3	TCP/UDP	123
PPTP-Server —Point-to-Point Tunneling Protocol server	pptp	TCP	17233
SSH —Secured Shell	ssh	TCP	22
SMTP-Server —Simple Mail Transfer Protocol server	smtp	TCP	25
Telnet —Telnet	telnet	TCP	23

The master controller is configured to learn the top prefixes based on highest outbound throughput or delay for the filtered traffic, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored.

For more details on configuring application-based traffic classes using static application mapping, see the [“Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping”](#) section on page 19.

PfR Application Mapping Using NBAR

In Cisco IOS Release 12.4(20)T, the ability to profile an application-based traffic class using NBAR was introduced. Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. PfR uses NBAR to recognize and classify a protocol or application, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored.

The new **traffic-class application nbar** command was introduced under learn list configuration mode to automatically profile traffic classes based on an NBAR application mapping name with an optional prefix list to eliminate or allow specific traffic classes.

NBAR is capable of identifying applications based on the following three types of protocols:

- Non-UDP and Non-TCP IP protocols—For example, Generic Routing Encapsulation (GRE) and Internet Control Message Protocol (ICMP)
- TCP and UDP protocols that use statically assigned port numbers—For example, CU-SeeMe desktop video conference (CU-SeeMe-Server) and Post Office Protocol over TLS/SSL server (SPOP3-Server)
- TCP and UDP protocols that dynamically assign port numbers and require stateful inspection—For example, Real-Time Transport Protocol audio streaming (RTP-Audio) and BitTorrent File Transfer Traffic (BitTorrent)

The list of applications identified using NBAR and available for profiling of Performance Routing traffic classes is constantly evolving. Use the **traffic-class application nbar ?** command in Cisco IOS Release 12.4(20)T, and later releases, to determine if an application that can be identified using NBAR is available for use with Performance Routing. Custom user-defined applications can also be configured to add a new application to the list of supported NBAR applications using a Packet Description Language Module (PDLM). A PDLM uses a mapping of static TCP and UDP port numbers to create a custom application. The application defined by a PDLM file must be recognized on an OER border router and configured on the master controller using the **application define** command.

In addition to the static applications in [Table 1](#), and many applications based on non-UDP and non-TCP protocols, [Table 2](#) displays a partial list of TCP and UDP applications that dynamically assign port numbers. All these applications can be identified using NBAR and used to profile traffic classes for Performance Routing.

Table 2 *NBAR-Supported Application List*

Application	Keyword	Protocol	Port
BitTorrent —File Sharing	bittorrent	TCP	Dynamically assigned or 6881-6889
Citrix ICA —Citrix ICA traffic by application name	citrix	TCP/UDP	Dynamically assigned
Direct Connect —Direct Connect File Transfer Traffic	directconnect	TCP/UDP	411
eDonkey/eMule —eDonkey File Sharing Application Note eMule traffic is also classified as eDonkey traffic in NBAR.	edonkey	TCP	4662
Exchange —MS-RPC for Exchange	exchange	TCP	79
FastTrack —FastTrack	fasttrack	N/A	Dynamically assigned
Gnutella —Gnutella	gnutella	TCP	Dynamically assigned
H.323 —H.323 Teleconferencing Protocol	h323	TCP	Dynamically assigned
KaZaA —KaZaA version 2 Note KaZaA version 1 traffic is classified using FastTrack.	kazaa2	TCP/UDP	Dynamically assigned
MGCP —Media Gateway Control Protocol	mgcp	TCP/UDP	2427 2428 2727
Netshow —Microsoft Netshow	netshow	TCP/UDP	Dynamically assigned
Novadigm —Novadigm Enterprise Desktop Manager (EDM)	novadigm	TCP/UDP	3460-3465
r-commands —rexec, rlogin, rsh	rcmd	TCP	Dynamically assigned
RTCP —Real-Time Control Protocol	rtcp	TCP/UDP	Dynamically assigned
RTP —Real-Time Transport Protocol Payload Classification	rtp	TCP/UDP	Dynamically assigned
RTP-Audio —Real-Time Transport Protocol streaming audio	rtp:audio	TCP/UDP	Dynamically assigned
RTP-Video —Real-Time Transport Protocol streaming video	rtp:video	TCP/UDP	Dynamically assigned
RTSP —Real-Time Streaming Protocol	rtsp	TCP/UDP	Dynamically assigned
SCCP/Skinny —Skinny Client Control Protocol	skinny	TCP	2000 2001 2002
SIP —Session Initiation Protocol	sip	TCP/UDP	5060

Table 2 NBAR-Supported Application List (continued)

Application	Keyword	Protocol	Port
Skype —Peer-to-Peer VoIP Client Software Note Cisco currently supports only Skype Version 1	skype	TCP/UDP	Dynamically assigned
SQL*Net —SQL*NET for Oracle	sqlnet	TCP/UDP	Dynamically assigned
StreamWorks —Stream Works audio and video	streamwork	UDP	Dynamically assigned
SunRCP —Sun Remote Procedure Call	sunrcp	TCP/UDP	Dynamically assigned
TFTP —Trivial File Transfer Protocol	tftp	UDP	Dynamically assigned
VDOLive —VDOLive Streaming Video	vdolive	TCP/UDP	Dynamically assigned
WinMX —WinMX Traffic	winmx	TCP	6699
X Windows —X11, X Windows	xwindows	TCP	6000-6003

For more details about NBAR, see the “[Classifying Network Traffic Using NBAR](#)” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

PfR Manual Traffic Class Configuration

PfR can be manually configured to create traffic classes for monitoring and subsequent optimizing. Automatic learning generally uses a default prefix length of /24 but manual configuration allows exact prefixes to be defined. Within the manual traffic class configuration process there are two components—manually configuring prefix-based traffic classes and manually configuring application-based traffic classes, both of which are described in the following sections:

- [Prefix Traffic Class Configuration Using PfR, page 9](#)
- [Application Traffic Class Configuration Using PfR, page 10](#)

Prefix Traffic Class Configuration Using PfR

A prefix or range of prefixes can be selected for PfR monitoring by configuring an IP prefix list. The IP prefix list is then imported into the MTC list by configuring a match clause in an OER map. An OER map is similar to an IP route map. IP prefix lists are configured with the **ip prefix-list** command and OER maps are configured with the **oer-map** command in global configuration mode.

The prefix list syntax operates in a slightly different way with PfR than in regular routing. The **ge** keyword is not used and the **le** keyword is used by PfR to specify only an inclusive prefix. A prefix list can also be used to specify an exact prefix.

A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, PfR monitors only the exact prefix.

A master controller can monitor and control an inclusive prefix using the **le** keyword and the *le-value* argument set to 32. PfR monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB).



Note Use the inclusive prefix option with caution in a typical PfR deployment because of the potential increase in the amount of prefixes being monitored and recorded.

An IP prefix list with a deny statement can be used to configure the master controller to exclude a prefix or prefix length for learned traffic classes. Deny prefix list sequences should be applied in the lowest OER map sequences for best performance. In Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, the master controller can be configured to tell border routers to filter out uninteresting traffic using an access list.



Note IP prefix lists with deny statements can be applied only to learned traffic classes.

Two types of prefix can be manually configured for PfR monitoring using an IP prefix list:

- outside prefix—An outside prefix is defined as a public IP prefix assigned outside the company. Outside prefixes are received from other networks.
- inside prefix—An inside prefix is defined as a public IP prefix assigned to a company. An inside prefix is a prefix configured within the company network.

In Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, the ability to manually configure inside prefixes was introduced. Using BGP, PfR can be configured to select inside prefixes to support best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. In prior releases, only outside prefixes were supported. Company networks advertise the inside prefixes over the Internet using an Internet service provider (ISP) and receive advertisements for outside prefixes from an ISP.



Note Although an inside prefix can be manually configured for PfR monitoring, PfR will not try to control an inside prefix unless there is an exact match in the BGP routing information base (RIB) because PfR does not advertise a new prefix to the Internet.

Application Traffic Class Configuration Using PfR

In the first release of OER, Cisco IOS Release 12.3(8)T, only Layer 3 prefixes could be manually configured during the OER profile phase. In Cisco IOS Release 12.4(2)T, 12.2(33)SRB, and later releases, support for OER application-aware routing for policy-based routing (PBR) was introduced. Application-aware routing allows the selection of traffic for specific applications based on values in the IP packet header, other than the Layer 3 destination address through a named extended IP access control list (ACL). Only named extended ACLs are supported. The extended ACL is configured with a permit statement and then referenced in an OER map. The protocol and port numbers can be used to identify specific application traffic classes, but protocol and port number parameters are monitored only within the context of a prefix, and are not sent to the MTC list. Only the prefix that carries the specific application traffic is profiled by the master controller. With application-aware routing support, active monitoring of application traffic was supported. Passive monitoring of application traffic was introduced in Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, with application traffic class configuration support of the profiling of DSCP values as well as protocol and port numbers. DSCP values, port numbers, and protocols in addition to prefixes, are all now stored in the MTC list.

In Cisco IOS Release 12.4(15)T, new **match traffic-class** commands were introduced under OER map configuration mode to simplify the configuration of traffic classes. Four types of traffic classes—to be manually configured—can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name and a prefix list to define destination prefixes
- Traffic classes based on NBAR application mapping name and a prefix list to define destination prefixes (introduced in Cisco IOS Release 12.4(20)T)

Only one type of **match traffic-class** command can be specified per OER map.

For a series of well-known applications, static ports have been defined and each application can be defined by entering a keyword. For more details about the mapping of keywords to static applications using PfR, see the [“Static Application Mapping Using PfR” section on page 5](#).

In Cisco IOS Release 12.4(20)T, the ability to profile an application-based traffic class using NBAR was introduced. NBAR is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. PfR uses NBAR to recognize and classify a protocol or application, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored. The new **match traffic-class application nbar** command was introduced to manually configure traffic classes based on an NBAR application mapping name and destination prefixes defined using a mandatory prefix list.

For more details about the mapping of keywords to applications using NBAR, see the [“PfR Application Mapping Using NBAR” section on page 7](#).

How to Configure PfR to Profile the Traffic Classes

A PfR master controller can be configured to automatically learn the traffic classes, or the traffic classes can be manually configured. In Cisco IOS Release 12.4(15)T, the introduction of learn lists allows traffic classes that are automatically learned by PfR to be categorized into separate learn lists to which different PfR policies can be applied. New commands were also introduced to simplify the profiling of traffic classes.

In Cisco IOS Release 12.4(15)T the introduction of learn lists allows traffic classes that are automatically learned by PfR to be categorized into separate learn lists to which different PfR policies can be applied. The ability to learn application traffic classes using a keyword representing a static application is also introduced and new **traffic-class** and **match traffic-class** commands simplify the configuration of traffic classes that PfR can automatically learn, or that can be manually configured.

In Cisco IOS Release 12.4(20)T, the ability to learn application traffic classes using a keyword representing an application that can be recognized using NBAR was introduced. Two new learn list commands, **traffic-class application nbar** and **match traffic-class application nbar**, were introduced.

Automatic Learning

Four types of automatically learned traffic classes can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name with optional prefix lists to define destination prefixes
- Traffic classes based on a NBAR application mapping name with optional prefix lists to define destination prefixes

Only one type of **traffic-class** command can be specified per learn list, and the **throughput** and **delay** commands are also mutually exclusive within a learn list.

Manual Configuration

Four types of manually configured traffic classes can be profiled:

- Traffic classes based on destination prefixes
- Traffic classes representing custom application definitions using access lists
- Traffic classes based on a static application mapping name and a prefix list to define destination prefixes
- Traffic classes based on an NBAR application mapping name and a prefix list to define destination prefixes

Only one type of **match traffic-class** command can be specified per OER map.



Note

If any of the border routers is a Cisco Catalyst 6500 switch and the master controller has set the monitoring mode to special, only the throughput method of learning is used to profile the traffic classes. If both delay and throughput are configured, the master controller will ignore the delay configuration. For more details about the special monitoring mode, see the [“Measuring the Traffic Class Performance and Link Utilization Using OER”](#) module for more details.

Perform any of the following tasks to profile traffic classes:

- [Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes, page 12](#)
- [Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List, page 16](#)
- [Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping, page 19](#)
- [Defining a Learn List to Automatically Learn Traffic Classes Using NBAR Application Mapping, page 24](#)
- [Manually Selecting Traffic Classes Using Static Application Mapping, page 28](#)
- [Manually Selecting Traffic Classes Using NBAR Application Mapping, page 30](#)
- [Manually Selecting Prefix-Based Traffic Classes Using a Prefix List, page 31](#)
- [Manually Selecting Application Traffic Classes Using an Access List, page 33](#)
- [Displaying and Resetting Traffic Class and Learn List Information, page 35](#)
- [Displaying and Resetting Information About Traffic Classes Identified Using NBAR, page 37](#)

Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes

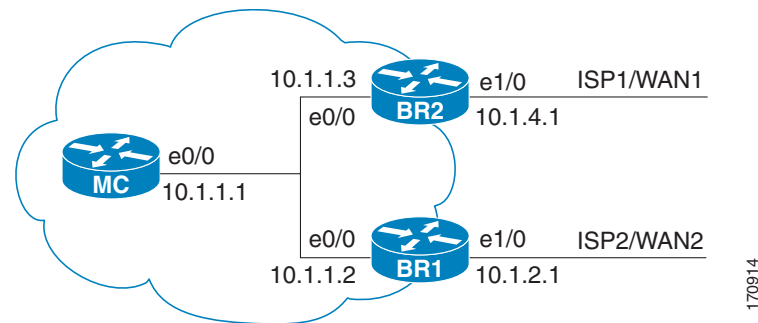
Perform this task at the master controller to define a learn list that will contain traffic classes that are automatically learned based on a prefix list. In Cisco IOS Release 12.4(15)T learn lists were introduced to allow traffic classes to be categorized. Learn lists allow different PfR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and an PfR policy was applied to all the learned traffic classes.

This task is performed on the master controller shown in [Figure 2](#). In this task, a prefix list is created to specify destination addresses and a learn list is defined under OER Top Talker and Top Delay configuration mode. This task configures prefix learning based on the highest outbound throughput.

In this task, the IP prefix list specifies that the prefix 10.1.0.0/16 is to be used as filter when learning the traffic classes. Under learn list mode, the prefix length aggregation is configured as a /24 prefix length. The traffic classes learned by this task will be:

```
10.1.1.0/24
10.1.2.0/24
.
.
.
10.1.255.0/24
```

Figure 2 Network Diagram of PfR Master Controller and Border Routers



Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list-name [seq seq-value] {deny network/length | permit network/length} [le le-value]**
4. Repeat [Step 3](#) for more prefix list entries, as required.
5. **oer master**
6. **learn**
7. **list seq number refname refname**
8. **count number max max-number**
9. **traffic-class prefix-list prefix-list-name**
10. **aggregation-type {bgp | non-bgp | prefix-length prefix-mask}**
11. **throughput**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip prefix-list <i>list-name</i> [seq <i>seq-value</i>] {deny <i>network/length</i> permit <i>network/length</i>} [le <i>le-value</i>]</p> <p>Example: Router(config)# ip prefix-list PREFIXES seq 10 permit 10.1.0.0/16</p>	<p>Creates an IP prefix list.</p> <ul style="list-style-type: none"> An IP prefix list is used under learn list configuration mode to filter IP addresses that are learned. The example creates an IP prefix list named PREFIXES for PfR to profile the prefix, 10.1.0.0/16.
Step 4	Repeat Step 3 for more prefix list entries, as required.	—
Step 5	<p>oer master</p> <p>Example: Router(config)# oer master</p>	<p>Enters OER master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.</p>
Step 6	<p>learn</p> <p>Example: Router(config-oer-mc)# learn</p>	<p>Enters OER Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.</p>
Step 7	<p>list seq <i>number</i> refname <i>refname</i></p> <p>Example: Router(config-oer-mc-learn)# list seq 10 refname LEARN_PREFIXES_TC</p>	<p>Creates an OER learn list and enters learn list configuration mode.</p> <ul style="list-style-type: none"> Use the seq keyword and <i>number</i> argument to specify a sequence number used to determine the order in which learn list criteria is applied. Use the refname keyword and <i>refname</i> argument to specify a reference name for the learn list. The example creates a learn list named LEARN_PREFIXES_TC.

	Command or Action	Purpose
Step 8	<p>count <i>number</i> max <i>max-number</i></p> <p>Example: Router(config-oer-mc-learn-list)# count 40 max 90</p>	<p>Sets the number of traffic classes to be learned during an PfR learn session.</p> <ul style="list-style-type: none"> Use the <i>number</i> argument to specify a number of traffic classes to be learned for the specified learn list during a learn session. Use the max keyword and <i>max-number</i> argument to specify a maximum number of traffic classes to be learned for the specified learn list during all learning sessions. The example specifies 40 traffic classes to be learned per learning session for the learn list named LEARN_PREFIXES_TC, and a maximum of 90 traffic classes in total for this learn list.
Step 9	<p>traffic-class prefix-list <i>prefix-list-name</i> [inside]</p> <p>Example: Router(config-oer-mc-learn-list)# traffic-class prefix-list LEARN_PREFIXES_TC</p>	<p>Defines an PfR traffic class using a prefix list.</p> <ul style="list-style-type: none"> Use the <i>prefix-list-name</i> argument to specify an IP prefix list that contains criteria for defining the traffic classes. Use the inside keyword to specify inside prefixes. The example uses the prefix list named LEARN_PREFIXES_TC to filter the learned traffic classes.
Step 10	<p>aggregation-type {bgp non-bgp prefix-length} <i>prefix-mask</i></p> <p>Example: Router(config-oer-mc-learn-list)# aggregation-type prefix-length 24</p>	<p>(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.</p> <ul style="list-style-type: none"> The bgp keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. The non-bgp keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. The prefix-length keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. If this command is not specified, the default aggregation is performed based on a /24 prefix length. The example configures prefix length aggregation based on a /24 prefix length.

	Command or Action	Purpose
Step 11	<p><code>throughput</code></p> <p>Example: Router(config-oer-mc-learn-list)# <code>throughput</code></p>	<p>Enables prefix learning based on the highest outbound throughput.</p> <ul style="list-style-type: none"> • Prefixes are sorted from the highest to lowest outbound throughput. • The example configures prefix learning based on the highest outbound throughput. <p>Note To configure automatic PfR learning within a learn list you can specify either the delay command or the throughput command, but they are mutually exclusive in learn list configuration mode.</p>
Step 12	<p><code>end</code></p> <p>Example: Router(config-oer-mc-learn-list)# <code>end</code></p>	<p>Exits learn list configuration mode, and returns to privileged EXEC mode.</p>

Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List

Perform this task at the master controller to define a learn list that will contain traffic classes that are automatically learned by PfR using an access list to create customized application traffic classes. Use this task to build application traffic classes where the traffic cannot be defined using standard application port and protocol mapping. If there are some known prefixes that you want to exclude, an optional prefix list can be used to further filter the traffic although this is not shown in this task.

In Cisco IOS Release 12.4(15)T learn lists were introduced to allow traffic classes to be categorized. Learn lists allow different PfR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and an PfR policy was applied to all the traffic classes profiled during one learning session.

In this task, an access list is created that defines custom application traffic classes. Every entry in the access list defines one application. A learn list is then defined, the access list is applied, and an aggregation method is configured. Using the **count** command, 50 traffic classes can be learned during one learning session for the learn list named LEARN_USER_DEFINED_TC, with a maximum specified number of 90 traffic classes for this learn list. The master controller is configured to learn the top prefixes based on highest delay for the filtered traffic and the resulting traffic classes are added to the PfR application database.

To display information about the traffic classes learned by PfR, use the [“Displaying and Resetting Traffic Class and Learn List Information”](#) section on page 35.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list {standard | extended} access-list-name**
4. **[sequence-number] permit udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [dscp dscp-value]**
5. Repeat [Step 4](#) for more access list entries, as required.
6. **exit**
7. **oer master**
8. **learn**
9. **list seq number refname refname**
10. **count number max max-number**
11. **traffic-class access-list access-list-name [filter prefix-list-name]**
12. **aggregation-type {bgp | non-bgp | prefix-length prefix-mask}**
13. **delay**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list {standard extended} access-list-name Example: Router(config)# ip access-list extended USER_DEFINED_TC	Defines an IP access list by name. <ul style="list-style-type: none"> • PfR supports only named access lists. • The example creates an extended IP access list named USER_DEFINED_TC.
Step 4	[sequence-number] permit udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [dscp dscp-value] Example: Router(config-ext-nacl)# permit tcp any any 500	Sets conditions to allow a packet to pass a named IP access list. <ul style="list-style-type: none"> • The example is configured to identify all TCP traffic from any destination or source and from destination port number of 500. This specific TCP traffic is to be optimized. <p>Note Only the syntax applicable to this task is shown. For more details, see the Cisco IOS IP Application Services Command Reference.</p>

	Command or Action	Purpose
Step 5	Repeat Step 4 for more access list entries, as required.	—
Step 6	exit Example: Router(config-ext-nacl)# exit	(Optional) Exits extended access list configuration mode and returns to global configuration mode.
Step 7	oer master Example: Router(config)# oer master	Enters OER master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.
Step 8	learn Example: Router(config-oer-mc)# learn	Enters OER Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.
Step 9	list seq number refname refname Example: Router(config-oer-mc-learn)# list seq 10 refname LEARN_USER_DEFINED_TC	Creates an PFR learn list and enters learn list configuration mode. <ul style="list-style-type: none"> Use the seq keyword and <i>number</i> argument to specify a sequence number used to determine the order in which learn list criteria is applied. Use the refname keyword and <i>refname</i> argument to specify a reference name for the learn list. The example creates a learn list named LEARN_USER_DEFINED_TC.
Step 10	count number max max-number Example: Router(config-oer-mc-learn-list)# count 50 max 90	Sets the number of traffic classes to be learned during an PFR learn session. <ul style="list-style-type: none"> Use the <i>number</i> argument to specify a number of traffic classes to be learned for the specified learn list during a learn session. Use the max keyword and <i>max-number</i> argument to specify a maximum number of traffic classes to be learned for the specified learn list during all learning sessions. The example specifies 50 traffic classes to be learned per learning session for the learn list named LEARN_USER_DEFINED_TC, and a maximum of 90 traffic classes in total for this learn list.
Step 11	traffic-class access-list access-list-name [filter prefix-list-name] Example: Router(config-oer-mc-learn-list)# traffic-class access-list USER_DEFINED_TC	Defines a PFR traffic class using an access list. <ul style="list-style-type: none"> Use the <i>access-list-name</i> argument to specify an access list that contains criteria for defining the traffic classes. The example uses the access list named USER_DEFINED_TC to create the traffic classes.

	Command or Action	Purpose
Step 12	<pre>aggregation-type {bgp non-bgp prefix-length} prefix-mask</pre> <p>Example: <pre>Router(config-oer-mc-learn-list)# aggregation-type prefix-length 24</pre></p>	<p>(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.</p> <ul style="list-style-type: none"> The bgp keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. The non-bgp keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. The prefix-length keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. If this command is not specified, the default aggregation is performed based on a /24 prefix length. The example configures prefix length aggregation based on a /24 prefix length.
Step 13	<pre>delay</pre> <p>Example: <pre>Router(config-oer-mc-learn-list)# delay</pre></p>	<p>Enables prefix learning based on the highest delay time.</p> <ul style="list-style-type: none"> <i>Top Delay</i> prefixes are sorted from the highest to lowest delay time. The example configures prefix learning based on the highest delay. <p>Note To configure automatic PfR learning within a learn list you can specify either the delay command or the throughput command, but they are mutually exclusive in learn list configuration mode.</p>
Step 14	<pre>end</pre> <p>Example: <pre>Router(config-oer-mc-learn-list)# end</pre></p>	<p>Exits learn list configuration mode, and returns to privileged EXEC mode.</p>

Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping

Perform this task at the master controller to define a learn list using static application mapping. Within a learn list, a keyword that represents an application can be used to identify specific application traffic classes. The defined learn list will contain traffic classes to be automatically learned by PfR using the static application mapping. The resulting traffic classes can be filtered by a prefix list, if required.

In Cisco IOS Release 12.4(15)T learn lists were introduced to allow traffic classes to be categorized. Learn lists allow different PfR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and an PfR policy was applied to all the traffic classes profiled during one learning session.

In this example, two learn lists are configured to identify remote login traffic and file transfer traffic. The remote login traffic class is configured using keywords representing Telnet and Secure Shell (SSH) traffic, and the resulting prefixes are aggregated to a prefix length of 24. The file transfer traffic class is

configured using a keyword that represents FTP and is also aggregated to a prefix length of 24. A prefix list is applied to the file transfer traffic class to permit traffic from the 10.0.0.0/8 prefix. The master controller is configured to learn the top prefixes based on highest outbound throughput for the filtered traffic, and the resulting traffic classes are added to the PfR application database.

To display information about the configured learn lists and the traffic classes learned by PfR, use the [“Displaying and Resetting Traffic Class and Learn List Information”](#) section on page 35.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list-name** [seq *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. **oer master**
5. **learn**
6. **list seq number refname refname**
7. **traffic-class application** *application-name* [**filter** *prefix-list-name*]
8. **aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*}
9. **throughput**
10. **exit**
11. **list seq number refname refname**
12. **traffic-class application** *application-name* [**filter** *prefix-list-name*]
13. **aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*}
14. **throughput**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>ip prefix-list <i>list-name</i> [seq <i>seq-value</i>] (deny <i>network/length</i> permit <i>network/length</i>) [le <i>le-value</i>]</p> <p>Example: Router(config)# ip prefix-list INCLUDE_10_NET permit 10.0.0.0/8</p>	<p>Creates an IP prefix list to filter prefixes for learning.</p> <ul style="list-style-type: none"> An IP prefix list is used under learn list configuration mode to filter IP addresses that are learned. The example creates an IP prefix list named INCLUDE_10_NET for PfR to profile the prefix, 10.0.0.0/8.
Step 4	<p>oer master</p> <p>Example: Router(config)# oer master</p>	<p>Enters OER master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.</p>
Step 5	<p>learn</p> <p>Example: Router(config-oer-mc)# learn</p>	<p>Enters OER Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.</p>
Step 6	<p>list seq <i>number</i> refname <i>refname</i></p> <p>Example: Router(config-oer-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC</p>	<p>Creates an PfR learn list and enters learn list configuration mode.</p> <ul style="list-style-type: none"> Use the seq keyword and <i>number</i> argument to specify a sequence number used to determine the order in which learn list criteria is applied. Use the refname keyword and <i>refname</i> argument to specify a reference name for the learn list. The example creates a learn list named LEARN_REMOTE_LOGIN_TC.
Step 7	<p>traffic-class application <i>application-name...</i> [filter <i>prefix-list-name</i>]</p> <p>Example: Router(config-oer-mc-learn-list)# traffic-class application telnet ssh</p>	<p>Defines an PfR traffic class using a pre-defined static application.</p> <ul style="list-style-type: none"> Use the <i>application-name</i> argument to specify one or more keywords that represent pre-defined static applications. The ellipses are used to show that more than one application keyword can be specified. The example defines a traffic class as containing telnet and ssh traffic.

	Command or Action	Purpose
Step 8	<p>aggregation-type {bgp non-bgp prefix-length} <i>prefix-mask</i></p> <p>Example: Router(config-oer-mc-learn-list)# aggregation-type prefix-length 24</p>	<p>(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.</p> <ul style="list-style-type: none"> • The bgp keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. • The non-bgp keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. • The prefix-length keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. • If this command is not specified, the default aggregation is performed based on a /24 prefix length. • The example configures prefix length aggregation based on a /24 prefix length.
Step 9	<p>throughput</p> <p>Example: Router(config-oer-mc-learn-list)# throughput</p>	<p>Configures the master controller to learn the top prefixes based on the highest outbound throughput.</p> <ul style="list-style-type: none"> • When this command is enabled, the master controller will learn the top prefixes across all border routers according to the highest outbound throughput. • The example configures a master controller to learn the top prefixes based on highest outbound throughput for the LEARN_REMOTE_LOGIN_TC traffic class.
Step 10	<p>exit</p> <p>Example: Router(config-oer-mc-learn-list)# exit</p>	<p>Exits learn list configuration mode, and returns to OER Top Talker and Top Delay learning configuration mode.</p>
Step 11	<p>list seq <i>number</i> refname <i>refname</i></p> <p>Example: Router(config-oer-mc-learn)# list seq 20 refname LEARN_FILE_TRANSFER_TC</p>	<p>Creates an PfR learn list and enters learn list configuration mode.</p> <ul style="list-style-type: none"> • Use the seq keyword and <i>number</i> argument to specify a sequence number used to determine the order in which learn list criteria is applied. • Use the refname keyword and <i>refname</i> argument to specify a reference name for the learn list. • The example creates a learn list named LEARN_FILE_TRANSFER_TC.

	Command or Action	Purpose
Step 12	<p>traffic-class application <i>application-name...</i> [filter <i>prefix-list-name</i>]</p> <p>Example: Router(config-oer-mc-learn-list)# traffic-class application ftp filter INCLUDE_10_NET</p>	<p>Defines an PfR traffic class using a pre-defined static application.</p> <ul style="list-style-type: none"> Use the <i>application-name</i> argument to specify one or more keywords that represent pre-defined static applications. The example defines a traffic class as containing FTP traffic filtered by the IP prefix list named INCLUDE_10_NET to include prefixes in the 10.0.0.0/8 subnet.
Step 13	<p>aggregation-type {bgp non-bgp prefix-length} <i>prefix-mask</i></p> <p>Example: Router(config-oer-mc-learn-list)# aggregation-type prefix-length 24</p>	<p>(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.</p> <ul style="list-style-type: none"> The bgp keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. The non-bgp keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. The prefix-length keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. If this command is not specified, the default aggregation is performed based on a /24 prefix length. The example configures prefix length aggregation based on a /24 prefix length.
Step 14	<p>throughput</p> <p>Example: Router(config-oer-mc-learn-list)# throughput</p>	<p>Configures the master controller to learn the top prefixes based on the highest outbound throughput.</p> <ul style="list-style-type: none"> When this command is enabled, the master controller will learn the top prefixes across all border routers according to the highest outbound throughput. The example configures a master controller to learn the top prefixes based on highest outbound throughput for the LEARN_FILE_TRANSFER_TC traffic class. <p>Note To configure automatic PfR learning within a learn list you can specify either the delay command or the throughput command, but they are mutually exclusive in learn list configuration mode.</p>
Step 15	<p>end</p> <p>Example: Router(config-oer-mc-learn-list)# end</p>	<p>Exits learn list configuration mode, and returns to privileged EXEC mode.</p>

Defining a Learn List to Automatically Learn Traffic Classes Using NBAR Application Mapping

Perform this task at the master controller to define a learn list using applications identified using NBAR. Within a learn list, NBAR is used to identify specific application traffic classes. The defined learn list will contain traffic classes to be automatically learned by PfR using NBAR, and an optional prefix list can be used to allow or eliminate certain traffic classes.

In Cisco IOS Release 12.4(15)T, learn lists were introduced to allow traffic classes to be categorized. Learn lists allow different PfR policies to be applied to each learn list; in earlier releases, the traffic classes could not be divided, and a PfR policy was applied to all the traffic classes profiled during one learning session. In Cisco IOS Release 12.4(20)T, the ability to use applications identified using NBAR was introduced.

In this example, a learn list is configured to identify Real-Time Transport Protocol streaming audio (RTP-Audio) traffic. The RTP-Audio traffic is identified using NBAR and the resulting prefixes are aggregated to a prefix length of 24. A second learn list to identify a Skype traffic class is configured using a keyword that represents Skype and is also aggregated to a prefix length of 24. A prefix list is applied to the Skype traffic class to permit traffic from the 10.0.0.0/8 prefix. The master controller is configured to learn the top prefixes based on highest outbound throughput for the filtered traffic, and the resulting traffic classes are added to the PfR application database.

The traffic streams that the learn list profiles for both the RTP-Audio and the Skype applications are:

```
10.1.1.1
10.1.2.1
20.1.1.1
20.1.2.1
```

The traffic classes that are learned for each application are:

```
10.1.1.0/24 rtp-audio
10.1.2.0/24 rtp-audio
20.1.1.0/24 rtp-audio
20.1.2.0/24 rtp-audio

10.1.1.0/24 skype
10.1.2.0/24 skype
```

The difference in traffic classes learned is due to the INCLUDE_10_NET prefix list that only includes Skype application traffic with a destination prefix that matches the prefix 10.0.0.0/8.

To display information about the configured learn lists and the traffic classes learned by PfR, use the [“Displaying and Resetting Information About Traffic Classes Identified Using NBAR”](#) section on page 37.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(20)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]

4. **oer master**
5. **learn**
6. **list seq number refname refname**
7. **traffic-class application nbar nbar-app-name [nbar-app-name...] [filter prefix-list-name]**
8. **aggregation-type {bgp | non-bgp | prefix-length prefix-mask}**
9. **throughput**
10. **exit**
11. **list seq number refname refname**
12. **traffic-class application nbar nbar-app-name [nbar-app-name...] [filter prefix-list-name]**
13. **aggregation-type {bgp | non-bgp | prefix-length prefix-mask}**
14. **throughput**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip prefix-list list-name [seq seq-value] {deny network/length permit network/length} [le le-value] Example: Router(config)# ip prefix-list INCLUDE_10_NET permit 10.0.0.0/8	Creates an IP prefix list to filter prefixes for learning. <ul style="list-style-type: none"> An IP prefix list is used under learn list configuration mode to filter IP addresses that are learned. The example creates an IP prefix list named INCLUDE_10_NET for PfR to profile the prefix, 10.0.0.0/8.
Step 4	oer master Example: Router(config)# oer master	Enters OER master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.
Step 5	learn Example: Router(config-oer-mc)# learn	Enters OER Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.

	Command or Action	Purpose
Step 6	<p>list seq <i>number</i> refname <i>refname</i></p> <p>Example: Router(config-oer-mc-learn)# list seq 10 refname LEARN_RTP_AUDIO_TC</p>	<p>Creates an PfR learn list and enters learn list configuration mode.</p> <ul style="list-style-type: none"> Use the seq keyword and <i>number</i> argument to specify a sequence number used to determine the order in which learn list criteria is applied. Use the refname keyword and <i>refname</i> argument to specify a reference name for the learn list. The example creates a learn list named LEARN_RTP_AUDIO_TC.
Step 7	<p>traffic-class application nbar <i>nbar-app-name</i> [<i>nbar-app-name...</i>] [filter <i>prefix-list-name</i>]</p> <p>Example: Router(config-oer-mc-learn-list)# traffic-class application nbar rtp:audio</p>	<p>Defines an PfR traffic class using an application that can be identified using NBAR.</p> <ul style="list-style-type: none"> Use the <i>nbar-app-name</i> argument to specify one or more keywords that represent applications identified using NBAR. The ellipses are used to show that more than one application keyword can be specified. The example defines a traffic class as containing RTP-Audio traffic.
Step 8	<p>aggregation-type {bgp non-bgp prefix-length <i>prefix-mask</i>}</p> <p>Example: Router(config-oer-mc-learn-list)# aggregation-type prefix-length 24</p>	<p>(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.</p> <ul style="list-style-type: none"> The bgp keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. The non-bgp keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. The prefix-length keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. If this command is not specified, the default aggregation is performed based on a /24 prefix length. The example configures prefix length aggregation based on a /24 prefix length.
Step 9	<p>throughput</p> <p>Example: Router(config-oer-mc-learn-list)# throughput</p>	<p>Configures the master controller to learn the top prefixes based on the highest outbound throughput.</p> <ul style="list-style-type: none"> When this command is enabled, the master controller will learn the top prefixes across all border routers according to the highest outbound throughput. The example configures a master controller to learn the top prefixes based on highest outbound throughput for the LEARN_RTP_AUDIO_TC traffic class.

	Command or Action	Purpose
Step 10	<p>exit</p> <p>Example: Router(config-oer-mc-learn-list)# exit</p>	Exits learn list configuration mode, and returns to OER Top Talker and Top Delay learning configuration mode.
Step 11	<p>list seq number refname refname</p> <p>Example: Router(config-oer-mc-learn)# list seq 10 refname LEARN_SKYPE_TC</p>	<p>Creates an PfR learn list and enters learn list configuration mode.</p> <ul style="list-style-type: none"> Use the seq keyword and <i>number</i> argument to specify a sequence number used to determine the order in which learn list criteria is applied. Use the refname keyword and <i>refname</i> argument to specify a reference name for the learn list. The example creates a learn list named LEARN_SKYPE_TC.
Step 12	<p>traffic-class application nbar nbar-app-name [nbar-app-name...] [filter prefix-list-name]</p> <p>Example: Router(config-oer-mc-learn-list)# traffic-class application nbar skype filter INCLUDE_10_NET</p>	<p>Defines an PfR traffic class using an application that can be identified using NBAR.</p> <ul style="list-style-type: none"> Use the <i>nbar-app-name</i> argument to specify one or more keywords that represent an application identified using NBAR. The ellipses are used to show that more than one application keyword can be specified. The example defines a traffic class as containing Skype traffic identified using NBAR and matching the prefix defined in the prefix list INCLUDE_10_NET.
Step 13	<p>aggregation-type {bgp non-bgp prefix-length prefix-mask}</p> <p>Example: Router(config-oer-mc-learn-list)# aggregation-type prefix-length 24</p>	<p>(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type.</p> <ul style="list-style-type: none"> The bgp keyword configures prefix aggregation based on entries in the BGP routing table. This keyword is used if BGP peering is enabled in the network. The non-bgp keyword configures learned prefix aggregation based on static routes. Entries in the BGP routing table are ignored when this keyword is entered. The prefix-length keyword configures aggregation based on the specified prefix length. The range of values that can be configured for this argument is a prefix mask from 1 to 32. If this command is not specified, the default aggregation is performed based on a /24 prefix length. The example configures prefix length aggregation based on a /24 prefix length.

	Command or Action	Purpose
Step 14	throughput Example: Router(config-oer-mc-learn-list)# throughput	Configures the master controller to learn the top prefixes based on the highest outbound throughput. <ul style="list-style-type: none"> When this command is enabled, the master controller will learn the top prefixes across all border routers according to the highest outbound throughput. The example configures a master controller to learn the top prefixes based on highest outbound throughput for the LEARN_SYKPE_TC traffic class.
Step 15	end Example: Router(config-oer-mc-learn-list)# end	Exits learn list configuration mode, and returns to privileged EXEC mode.

Manually Selecting Traffic Classes Using Static Application Mapping

Perform this task to manually select traffic classes using static application mapping. Use this task when you know the destination prefixes and the applications that you want to select for the traffic classes. In this task, an IP prefix list is created to define the destination prefixes, and static applications are defined using the **match traffic-class application** command. Using an OER map, each prefix is matched with each application to create the traffic classes.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T, or a later release.

SUMMARY STEPS

- enable**
- configure terminal**
- ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
- Repeat [Step 3](#) for more prefix list entries, as required.
- oer-map** *map-name* *sequence-number*
- match traffic-class application** *application-name* **prefix-list** *prefix-list-name*
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip prefix-list <i>list-name</i> [seq <i>seq-value</i>] (deny <i>network/length</i> permit <i>network/length</i>) [le <i>le-value</i>]</p> <p>Example: Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24</p>	<p>Creates a prefix list to specify destination prefix-based traffic classes.</p> <ul style="list-style-type: none"> The example specifies a destination prefix of 10.1.1.0/24 to be used to filter application traffic classes.
Step 4	Repeat Step 3 for more prefix list entries, as required.	—
Step 5	<p>oer-map <i>map-name</i> <i>sequence-number</i></p> <p>Example: Router(config)# oer-map APPLICATION_MAP 10</p>	<p>Enters OER map configuration mode to configure an OER map.</p> <ul style="list-style-type: none"> Only one match clause can be configured for each OER map sequence. Permit sequences are first defined in an IP prefix list and then applied with the match traffic-class command in Step 6. The example creates an OER map named APPLICATION_MAP.
Step 6	<p>match traffic-class <i>application</i> <i>application-name</i> prefix-list <i>prefix-list-name</i></p> <p>Example: Router(config-oer-map)# traffic-class application telnet ssh prefix-list LIST1</p>	<p>Manually configures one or more static applications as match criteria against a prefix list to create traffic classes using an OER map.</p> <ul style="list-style-type: none"> Use the <i>application-name</i> argument to specify one or more keywords that represent pre-defined static applications. The example defines traffic classes as application X with destination prefix Y, where X is Telnet or Secure Shell and Y is a destination address defined in the IP prefix list named LIST1.
Step 7	<p>end</p> <p>Example: Router(config-oer-map)# end</p>	<p>(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.</p>

Manually Selecting Traffic Classes Using NBAR Application Mapping

Perform this task to manually select traffic classes using NBAR application mapping. Use this task when you know the destination prefixes and the NBAR-identified applications that you want to select for the traffic classes. In this task, an IP prefix list is created to define the destination prefixes and the NBAR-identified applications, BitTorrent and Direct Connect, are defined using the **match traffic-class application** command. Using an OER map, each prefix is matched with each application to create the traffic classes.

The traffic classes in this example consist of BitTorrent and Direct Connect traffic identified using NBAR and matched with the destination prefix 10.1.1.0/24 that is specified in a prefix list, LIST1. Only traffic that matches both the BitTorrent and Direct Connect applications and the destination prefix is learned.

To display information about manually configured traffic classes identified using NBAR and learned by PFR, use the [“Displaying and Resetting Information About Traffic Classes Identified Using NBAR” section on page 37](#).

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(20)T, or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. Repeat [Step 3](#) for more prefix list entries, as required.
5. **oer-map** *map-name* *sequence-number*
6. **match traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] **prefix-list** *prefix-list-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>ip prefix-list list-name [seq seq-value] {deny network/length permit network/length} [le le-value]</pre> <p>Example: Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24</p>	<p>Creates a prefix list to specify destination prefix-based traffic classes.</p> <ul style="list-style-type: none"> The example specifies a destination prefix of 10.1.1.0/24 to be used to filter application traffic classes.
Step 4	Repeat Step 3 for more prefix list entries, as required.	—
Step 5	<pre>oer-map map-name sequence-number</pre> <p>Example: Router(config)# oer-map APPL_NBAR_MAP 10</p>	<p>Enters OER map configuration mode to configure an OER map.</p> <ul style="list-style-type: none"> Only one match clause can be configured for each OER map sequence. Permit sequences are first defined in an IP prefix list and then applied with the match traffic-class application nbar command in Step 6. The example creates an OER map named APPL_NBAR_MAP.
Step 6	<pre>match traffic-class application nbar nbar-app-name [nbar-app-name...] prefix-list prefix-list-name</pre> <p>Example: Router(config-oer-map)# match traffic-class application nbar bittorrent directconnect prefix-list LIST1</p>	<p>Manually configures one or more applications that can be identified using NBAR as match criteria against a prefix list to create traffic classes using an OER map.</p> <ul style="list-style-type: none"> Use the <i>application-name</i> argument to specify one or more keywords that represent applications that can be identified using NBAR. The example defines traffic classes as application X with destination prefix Y, where X is BitTorrent or Direct Connect file transfer traffic and Y is a destination address defined in the IP prefix list named LIST1.
Step 7	<pre>end</pre> <p>Example: Router(config-oer-map)# end</p>	<p>(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.</p>

Manually Selecting Prefix-Based Traffic Classes Using a Prefix List

Perform this task on the master controller to manually select traffic classes based only on destination prefixes. Use this task when you know the destination prefixes that you want to select for the traffic classes. An IP prefix list is created to define the destination prefixes and using an OER map, the traffic classes are profiled.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. Repeat [Step 3](#) for more prefix list entries, as required.
5. **oer-map** *map-name* *sequence-number*
6. **match traffic-class prefix-list** *prefix-list-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip prefix-list <i>list-name</i> [seq <i>seq-value</i>] { deny <i>network/length</i> permit <i>network/length</i> } [le <i>le-value</i>] Example: Router(config)# ip prefix-list PREFIX_TC permit 172.16.1.0/24	Creates a prefix list to specify destination prefix-based traffic classes. <ul style="list-style-type: none"> The example creates a prefix list named PREFIX_TC that specifies a destination prefix of 172.16.1.0/24 to be selected for a traffic class.
Step 4	Repeat Step 3 for more prefix list entries, as required.	—
Step 5	oer-map <i>map-name</i> <i>sequence-number</i> Example: Router(config)# oer-map PREFIX_MAP 10	Enters OER map configuration mode to configure an OER map. <ul style="list-style-type: none"> Only one match clause can be configured for each OER map sequence. Permit sequences are first defined in an IP prefix list and then applied with the match traffic-class command in Step 6. The example creates an OER map named PREFIX_MAP.

	Command or Action	Purpose
Step 6	<pre>match traffic-class prefix-list prefix-list-name</pre> <p>Example:</p> <pre>Router(config-oer-map)# match traffic-class prefix-list PREFIX_TC</pre>	<p>Manually configures a prefix list as match criteria used to create traffic classes using an OER map.</p> <ul style="list-style-type: none"> The example defines a traffic class using the destination address defined in the IP prefix list named PREFIX_TC.
Step 7	<pre>end</pre> <p>Example:</p> <pre>Router(config-oer-map)# end</pre>	<p>(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.</p>

Manually Selecting Application Traffic Classes Using an Access List

Perform this task on the master controller to manually select traffic classes using an access list. Each access list entry is a traffic class that must include a destination prefix and may include other optional parameters. This task uses the **match traffic-class access-list** command, which is similar to using the **match ip-address** command in previous releases. In this task, an access list is created and using an OER map, the traffic classes are profiled.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T or a later release.

SUMMARY STEPS

- enable**
- configure terminal**
- ip access-list {standard | extended} access-list-name**
- [sequence-number] permit udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [dscp dscp-value]**
- Repeat [Step 4](#) for more access list entries, as required.
- exit**
- oer-map map-name sequence-number**
- match traffic-class access-list access-list-name**
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip access-list {standard extended} <i>access-list-name</i></p> <p>Example: Router(config)# ip access-list extended ACCESS_TC</p>	<p>Defines an IP access list by name and enters extended named access list configuration mode.</p> <ul style="list-style-type: none"> PfR supports only named access lists. The example creates an extended IP access list named ACCESS_TC.
Step 4	<p>[<i>sequence-number</i>] permit udp <i>source source-wildcard</i> [<i>operator</i> [<i>port</i>]] <i>destination destination-wildcard</i> [<i>operator</i> [<i>port</i>]] [dscp <i>dscp-value</i>]</p> <p>Example: Router(config-ext-nacl)# permit tcp any any 500</p>	<p>Sets conditions to allow a packet to pass a named IP access list.</p> <ul style="list-style-type: none"> The example is configured to identify all TCP traffic from any destination or source and from destination port number of 500. This specific TCP traffic is to be optimized. <p>Note Only the syntax applicable to this task is shown. For more details, see the Cisco IOS IP Application Services Command Reference.</p>
Step 5	Repeat Step 4 for more access list entries, as required.	—
Step 6	<p>exit</p> <p>Example: Router(config-ext-nacl)# exit</p>	<p>(Optional) Exits extended named access list configuration mode and returns to global configuration mode.</p>
Step 7	<p>oer-map <i>map-name</i> <i>sequence-number</i></p> <p>Example: Router(config)# oer-map ACCESS_MAP 10</p>	<p>Enters OER map configuration mode to configure an OER map.</p> <ul style="list-style-type: none"> Only one match clause can be configured for each OER map sequence. Permit sequences are first defined in an IP prefix list and then applied with the match traffic-class command in Step 6. The example creates an OER map named ACCESS_MAP.

	Command or Action	Purpose
Step 8	match traffic-class access-list <i>access-list-name</i> Example: Router(config-oer-map)# match traffic-class access-list ACCESS_TC	Manually configures an access list as match criteria used to create traffic classes using an OER map. <ul style="list-style-type: none"> Each access list entry must contain a destination prefix and may include other optional parameters. The example defines a traffic class using the criteria defined in the access list named ACCESS_TC.
Step 9	end Example: Router(config-oer-map)# end	(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Displaying and Resetting Traffic Class and Learn List Information

Perform this task to display traffic class and learn list information and optionally, to reset some traffic class information. These commands can be entered on a master controller after learn lists are configured and traffic classes are automatically learned, or when traffic classes are manually configured using an OER map. The commands can be entered in any order and all the commands are optional.

Prerequisites

This task requires the master controller to be running Cisco IOS Release 12.4(15)T.

SUMMARY STEPS

- enable**
- show oer master traffic-class** [**access-list** *access-list-name* | **application** *application-name* [*prefix*] | **inside** | **learned** [**delay** | **inside** | **list** *list-name* | **throughput**] | **prefix** *prefix* | **prefix-list** *prefix-list-name*] [**active** | **passive** | **status**] [**detail**]
- show oer master learn list** *list-name*
- clear oer master traffic-class** [**access-list** *access-list-name* | **application** *application-name* [*prefix*] | **inside** | **learned** [**delay** | **inside** | **list** *list-name* | **throughput**] | **prefix** *prefix* | **prefix-list** *prefix-list-name*]

DETAILED STEPS

-
- Step 1** **enable**
- Enables privileged EXEC mode. Enter your password if prompted.
- ```
Router> enable
```
- Step 2**    **show oer master traffic-class** [**access-list** *access-list-name* | **application** *application-name* [*prefix*] | **inside** | **learned** [**delay** | **inside** | **list** *list-name* | **throughput**] | **prefix** *prefix* | **prefix-list** *prefix-list-name*] [**active** | **passive** | **status**] [**detail**]
- This command is used to display information about traffic classes learned or manually configured under PfR learn list configuration mode.
- ```
Router# show oer master traffic-class
```

OER Prefix Statistics:

Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix	Appl_ID		Dscp	Prot	SrcPort	DstPort	SrcPrefix		
	Flags	State					Time	CurrBR	CurrI/F
	PasSDly	PasLDly	PasSUn	PasLUn	PasSLos	PasLLos	EBw	IBw	
	ActSDly	ActLDly	ActSUn	ActLUn	ActSJit	ActPMOS			
10.1.1.0/24			N defa	N	N	N N			
	#		OOPOLICY		32	10.11.1.3	Et1/0		BGP
	N	N	N	N	N	N	N		IBwN
	130	134	0	0	N	N			

Step 3 `show oer master learn list [list-name]`

This command is used to display one or all of the configured PfR learn lists. In this example, the information about two learn lists is displayed.

```
Router# show oer master learn list
```

```
Learn-List LIST1 10
Configuration:
  Application: ftp
  Aggregation-type: bgp
  Learn type: thruput
  Policies assigned: 8 10
Stats:
  Application Count: 0
  Application Learned:
Learn-List LIST2 20
Configuration:
  Application: telnet
  Aggregation-type: prefix-length 24
  Learn type: thruput
  Policies assigned: 5 20
Stats:
  Application Count: 2
  Application Learned:
  Appl Prefix 10.1.5.0/24 telnet
  Appl Prefix 10.1.5.16/28 telnet
```

Step 4 `clear oer master traffic-class [access-list access-list-name | application application-name [prefix] | inside | learned [delay | inside | list list-name | throughput] | prefix prefix | prefix-list prefix-list-name]`

This command is used to clear PfR controlled traffic classes from the master controller database. The following example clears traffic classes defined by the Telnet application and the 10.1.1.0/24 prefix:

```
Router# clear oer master traffic-class application telnet 10.1.1.0/24
```

Displaying and Resetting Information About Traffic Classes Identified Using NBAR

Perform this task to display and reset information about traffic classes identified using NBAR. All the commands in this task are optional and can be entered either after learn lists are configured and traffic classes are automatically learned or after traffic classes are manually configured using an OER map. Most of the commands are entered on a master controller—although some of the commands are entered on a border router—and the following steps indicate on which device you enter each command.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(20)T.

SUMMARY STEPS

1. Go to the master controller device.
2. **enable**
3. **show oer master traffic-class application nbar** *nbar-appl-name* [*prefix*] [**active passive status** | **detail**]
4. **show oer master nbar application**
5. **show oer master defined application**
6. **clear oer master traffic-class application nbar** [*nbar-appl-name* [*prefix*]]
7. Go to a border router configured as part of the OER network.
8. **enable**
9. **show oer border routes** {**bgp** | **cce** | **static**}
10. **show oer border defined application**

DETAILED STEPS

Step 1 Go to the master controller router.

Step 2 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 3 **show oer master traffic-class application nbar** *nbar-appl-name* [*prefix*] [**active passive status** | **detail**]

This command is used to display information about application traffic classes that are identified using NBAR and are monitored and controlled by an OER master controller. The following example shows information about traffic classes consisting of Real-time Transport Protocol streaming audio (RTP-Audio) traffic.

```
Router# show oer master traffic-class application nbar rtp:audio

OER Prefix Statistics:
Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
P - Percentage below threshold, Jit - Jitter (ms),
MOS - Mean Opinion Score
Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
# - Prefix monitor mode is Special, & - Blackholed Prefix
% - Force Next-Hop, ^ - Prefix is denied

DstPrefix      Appl_ID Dscp Prot      SrcPort      DstPort SrcPrefix
Flags          State      Time          CurrBR      CurrI/F Protocol
PasSDly PasLDly PasSUn PasLUn      EBw      IBw
ActSDly ActLDly ActSUn ActLUn ActSJit ActPMOS
-----
10.1.1.0/28      RTP-Audio defa  N          N          N 0.0.0.0/0
                DEFAULT*      461      10.11.1.2  Et1/0      U
                U          0          1          2
                150      130      0          0          15      0

10.1.1.16/28     RTP-Audio defa  N          N          N 0.0.0.0/0
                DEFAULT*      461      10.11.1.2  Et1/0      U
                U          0          1          2
                250      200      0          0          30      0
```

Step 4 show oer master nbar application

This command is used to display information about the status of an application identified using NBAR for each OER border router. The following partial output shows information about the status of applications identified using NBAR at three OER border routers identified by their IP addresses. If the NBAR application is not supported on one or more border routers, then all the traffic classes related to that NBAR application are marked inactive and cannot be optimized using OER.

```
Router# show oer master nbar application

NBAR Appl      10.1.1.4      10.1.1.2      10.1.1.3
-----
aarp            Invalid       Invalid       Invalid
appletalk      Invalid       Invalid       Invalid
arp            Invalid       Invalid       Invalid
bgp            Valid        Valid        Valid
bittorrent     Valid        Valid        Valid
bridge         Invalid       Invalid       Invalid
bstun          Invalid       Invalid       Invalid
cdp            Invalid       Invalid       Invalid
citrix         Invalid       Invalid       Invalid
clns           Valid        Invalid       Invalid
clns_es        Invalid       Invalid       Invalid
clns_is        Invalid       Invalid       Invalid
cmns           Invalid       Invalid       Invalid
compressedtcp  Invalid       Invalid       Invalid
cuseeme        Invalid       Invalid       Invalid
.
.
.
```

Step 5 show oer master defined application

This command is used to display information about user-defined application definitions used in OER. The following partial example output shows information about the user-defined applications configured for use with OER:

```
Router# show oer master defined application
```

```
OER Defined Applications:
```

Name	Appl_ID	Dscp	Prot	SrcPort	DstPort	SrcPrefix
telnet	1	defa	tcp	23-23	1-65535	0.0.0.0/0
telnet	1	defa	tcp	1-65535	23-23	0.0.0.0/0
ftp	2	defa	tcp	21-21	1-65535	0.0.0.0/0
ftp	2	defa	tcp	1-65535	21-21	0.0.0.0/0
cuseeme	4	defa	tcp	7648-7648	1-65535	0.0.0.0/0
cuseeme	4	defa	tcp	7649-7649	1-65535	0.0.0.0/0
cuseeme	4	defa	tcp	1-65535	7648-7648	0.0.0.0/0
cuseeme	4	defa	tcp	1-65535	7649-7649	0.0.0.0/0
dhcp	5	defa	udp	68-68	67-67	0.0.0.0/0
dns	6	defa	tcp	53-53	1-65535	0.0.0.0/0
dns	6	defa	tcp	1-65535	53-53	0.0.0.0/0
dns	6	defa	udp	53-53	1-65535	0.0.0.0/0
dns	6	defa	udp	1-65535	53-53	0.0.0.0/0
finger	7	defa	tcp	79-79	1-65535	0.0.0.0/0
finger	7	defa	tcp	1-65535	79-79	0.0.0.0/0
gopher	8	defa	tcp	70-70	1-65535	0.0.0.0/0
.

Step 6 clear oer master traffic-class application nbar [nbar-appl-name [prefix]]

This command is used to clear PfR controlled traffic classes from the master controller database. The following example clears OER traffic classes defined by the RTP-Audio application that is identified using NBAR and filtered by the 10.1.1.0/24 prefix:

```
Router# clear oer master traffic-class application nbar rtp:audio 10.1.1.0/24
```

Step 7 Go to a border router configured as part of the OER network.

Step 8 enable

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 9 show oer border routes {bgp | cce | static}

This command is used to display information about OER controlled routes of applications identified using NBAR. The following example displays CCE-controlled routes on a border router:

```
Router# show oer border routes cce
```

```
Class-map oer-class-acl-oer_cce#2-stile-telnet, permit, sequence 0, mask 24
  Match clauses:
    ip address (access-list): oer_cce#2
    stile: telnet
  Set clauses:
    ip next-hop 10.1.3.2
    interface Ethernet2/3
  Statistic:
    Packet-matched: 60
```

Step 10 show oer border defined application

This command is used to display all user-defined applications monitored by an OER border router. The following partial example output shows information about the user-defined applications monitored by an OER border router:

```
Router# show oer border defined application
```

```
OER Defined Applications:
```

Name	Appl_ID	Dscp	Prot	SrcPort	DstPort	SrcPrefix
telnet	1	defa	tcp	23-23	1-65535	0.0.0.0/0
telnet	1	defa	tcp	1-65535	23-23	0.0.0.0/0
ftp	2	defa	tcp	21-21	1-65535	0.0.0.0/0
ftp	2	defa	tcp	1-65535	21-21	0.0.0.0/0
cuseeme	4	defa	tcp	7648-7648	1-65535	0.0.0.0/0
cuseeme	4	defa	tcp	7649-7649	1-65535	0.0.0.0/0
dhcp	5	defa	udp	68-68	67-67	0.0.0.0/0
dns	6	defa	tcp	53-53	1-65535	0.0.0.0/0
dns	6	defa	tcp	1-65535	53-53	0.0.0.0/0
dns	6	defa	udp	53-53	1-65535	0.0.0.0/0
dns	6	defa	udp	1-65535	53-53	0.0.0.0/0
finger	7	defa	tcp	79-79	1-65535	0.0.0.0/0
finger	7	defa	tcp	1-65535	79-79	0.0.0.0/0
gopher	8	defa	tcp	70-70	1-65535	0.0.0.0/0
.						
.						
.						

Configuration Examples for Using PfR to Profile the Traffic Classes

The configuration examples in this section show how to use performance routing techniques introduced in Cisco IOS Release 12.4(15)T and later releases, to profile the traffic classes:



Note

If any of the border routers is a Cisco Catalyst 6500 switch and the master controller has set the monitoring mode to special, only the throughput method of learning is used to profile the traffic classes. If both delay and throughput are configured, the master controller will ignore the delay configuration. For more details about the special monitoring mode, see the [“Measuring the Traffic Class Performance and Link Utilization Using OER”](#) module for more details.

- [Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes: Example, page 41](#)
- [Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List: Example, page 41](#)
- [Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping: Example, page 42](#)
- [Defining a Learn List to Automatically Learn Traffic Classes Using NBAR Application Mapping: Example, page 43](#)
- [Manually Selecting Traffic Classes Using Static Application Mapping: Example, page 44](#)

- [Manually Selecting Traffic Classes Using NBAR Application Mapping: Example, page 44](#)
- [Manually Selecting Prefix-Based Traffic Classes Using a Prefix List: Example, page 44](#)
- [Manually Selecting Application Traffic Classes Using an Access List: Example, page 44](#)

Defining a Learn List for Automatically Learned Prefix-Based Traffic Classes: Example

The following example configured on the master controller, defines a learn list that will contain traffic classes that are automatically learned based only on a prefix list. In this example, there are three branch offices and the goal is to optimize all the traffic going to branch offices A and B using one policy (Policy1), and to optimize traffic going to branch office C using a different policy (Policy2).

Branch A is defined as any prefix that matches 10.1.0.0/16, Branch B is defined as any prefix that matches 10.2.0.0/16, and Branch C is defined as any prefix that matches 10.3.0.0/16.

This task configures prefix learning based on the highest outbound throughput.

```
ip prefix-list BRANCH_A_B permit seq 10 10.1.0.0/16
ip prefix-list BRANCH_A_B permit seq 20 10.2.0.0/16
ip prefix-list BRANCH_C permit seq 30 10.3.0.0/16
oer master
  learn
    list seq 10 refname LEARN_BRANCH_A_B
    traffic-class prefix-list BRANCH_A_B
    throughput
  exit
  learn
    list seq 20 refname LEARN_BRANCH_C
    traffic-class prefix-list BRANCH_C
    throughput
  exit
oer-map POLICY1 10
  match learn list LEARN_BRANCH_A_B
  exit
oer-map POLICY2 10
  match learn list LEARN_BRANCH_C
  exit
end
```

Defining a Learn List for Automatically Learned Application Traffic Classes Using an Access List: Example

The following example creates an access list that defines custom application traffic classes. In this example, the custom application consists of four criteria:

- Any TCP traffic on destination port 500
- Any TCP traffic on ports in the range from 700 to 750
- Any UDP traffic on source port 400
- Any IP packet marked with a DSCP bit of ef

The goal is to optimize same policy POLICY_CUSTOM_APP is to be applied to all the learned traffic classes. This task configures traffic class learning based on the highest outbound throughput.

```

ip access-list extended USER_DEFINED_TC
 permit tcp any any 500
 permit tcp any any range 700 750
 permit udp any eq 400 any
 permit ip any any dscp ef
 exit
oer master
 learn
 list seq 10 refname CUSTOM_APPLICATION_TC
 traffic-class access-list USER_DEFINED_TC
 aggregation-type prefix-length 24
 throughput
 exit
 exit
oer-map POLICY_CUSTOM_APP 10
 match learn list CUSTOM_APPLICATION_TC
 end

```

Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping: Example

The following example defines application traffic classes using static application mapping. In this example, the following two PfR learn lists are defined:

- LEARN_REMOTE_LOGIN_TC—Remote login traffic represented by Telnet and SSH.
- LEARN_FILE_TRANSFER_TC—File transfer traffic represented by FTP and filtered by the 10.0.0.0/8 prefix.

The goal is to optimize the remote login traffic using one policy (POLICY_REMOTE), and to optimize the file transfer traffic using a different policy (POLICY_FILE). This task configures traffic class learning based on the highest delay.

```

ip prefix-list INCLUDE_10_NET 10.0.0.0/8
oer master
 learn
 list seq 10 refname LEARN_REMOTE_LOGIN_TC
 traffic-class application telnet ssh
 aggregation-type prefix-length 24
 delay
 exit
 list seq 20 refname LEARN_FILE_TRANSFER_TC
 traffic-class application ftp filter INCLUDE_10_NET
 aggregation-type prefix-length 24
 delay
 exit
 exit
oer-map POLICY_REMOTE 10
 match learn list LEARN_REMOTE_LOGIN_TC
 exit
oer-map POLICY_FILE 20
 match learn list LEARN_FILE_TRANSFER_TC
 end

```

Defining a Learn List to Automatically Learn Traffic Classes Using NBAR Application Mapping: Example

The following example defines application traffic classes using NBAR application mapping. In this example, the following two PfR learn lists are defined:

- LEARN_RTP_AUDIO_TC—Real-time streaming audio traffic represented by RTP-Audio.
- LEARN_SKYPE_TC—Remote audio and video traffic represented by Skype and the 10.0.0.0/8 prefix.

The goal is to optimize the real-time streaming audio traffic using one policy (STREAM_AUDIO), and to optimize the remote audio and video traffic using a different policy (REMOTE_AUDIO_VIDEO). This task configures traffic class learning based on the highest delay.

The traffic streams that the learn list profiles for both the RTP-Audio and the Skype applications are:

```
10.1.1.1
10.1.2.1
20.1.1.1
20.1.2.1
```

The traffic classes that are learned for each application are:

```
10.1.1.0/24 rtp-audio
10.1.2.0/24 rtp-audio
20.1.1.0/24 rtp-audio
20.1.2.0/24 rtp-audio
```

```
10.1.1.0/24 skype
10.1.2.0/24 skype
```

The difference in traffic classes learned is due to the INCLUDE_10_NET prefix list that only includes Skype application traffic with a destination prefix that matches the prefix 10.0.0.0/8.

```
ip prefix-list INCLUDE_10_NET 10.0.0.0/8
oer master
 learn
  list seq 10 refname LEARN_RTP_AUDIO_TC
  traffic-class application nbar rtp-audio
  aggregation-type prefix-length 24
  delay
  exit
  list seq 20 refname LEARN_SKYPE_TC
  traffic-class application nbar skype filter INCLUDE_10_NET
  aggregation-type prefix-length 24
  delay
  exit
  exit
  exit
oer-map STREAM_AUDIO 10
 match learn list LEARN_RTP_AUDIO_TC
 exit
oer-map REMOTE_AUDIO_VIDEO 20
 match learn list LEARN_SKYPE_TC
 end
```

Manually Selecting Traffic Classes Using Static Application Mapping: Example

The following example starting in global configuration mode, configures an OER map to include application traffic predefined as telnet or Secure Shell and destined to prefixes in the 10.1.1.0/24 network, 10.1.2.0/24 network, and 172.16.1.0/24 network.

```
ip prefix-list LIST1 permit 10.1.1.0/24
ip prefix-list LIST1 permit 10.1.2.0/24
ip prefix-list LIST1 permit 172.16.1.0/24
oer-map PREFIXES 10
  match traffic-class application telnet ssh prefix-list LIST1
end
```

Manually Selecting Traffic Classes Using NBAR Application Mapping: Example

The following example starting in global configuration mode, configures an OER map to include file transfer BitTorrent or Direct Connect application traffic identified using NBAR and matched with the destination prefixes 10.1.1.0/24, 10.1.2.0/24, and 172.16.1.0/24 as specified in the prefix list, LIST1. Only traffic that matches both the BitTorrent and Direct Connect applications and the destination prefix is learned.

```
ip prefix-list LIST1 permit 10.1.1.0/24
ip prefix-list LIST1 permit 10.1.2.0/24
ip prefix-list LIST1 permit 172.16.1.0/24
oer-map PREFIXES 10
  match traffic-class application nbar bittorrent directconnect prefix-list LIST1
end
```

Manually Selecting Prefix-Based Traffic Classes Using a Prefix List: Example

The following example configured on the master controller, manually selects traffic classes based only on destination prefixes. Use this task when you know the destination prefixes that you want to select for the traffic classes. An IP prefix list is created to define the destination prefixes and using an OER map, the traffic classes are profiled.

```
ip prefix-list PREFIX_TC permit 10.1.1.0/24
ip prefix-list PREFIX_TC permit 10.1.2.0/24
ip prefix-list PREFIX_TC permit 172.16.1.0/24
oer-map PREFIX_MAP 10
  match traffic-class prefix-list PREFIX_TC
```

Manually Selecting Application Traffic Classes Using an Access List: Example

The following example configured on the master controller, manually selects traffic classes using an access list. Each access list entry is a traffic class that must include a destination prefix and may include other optional parameters.

```
ip access-list extended ACCESS_TC
  permit tcp any 10.1.1.0 0.0.0.255 eq 500
  permit tcp any 172.17.1.0 0.0.255.255 eq 500
```

```

permit tcp any 172.17.1.0 0.0.255.255 range 700 750
permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800 any any dscp ef
exit
oer-map ACCESS_MAP 10
match traffic-class access-list ACCESS_TC

```

Where To Go Next

This module covered the PFR profile phase for Cisco IOS Releases 12.4(15)T and later releases, and it has assumed that you started with the “[Cisco IOS Optimized Edge Routing Overview](#)” and the “[Setting Up OER Network Components](#)” module. The profile phase is the first phase in the PFR/OER performance loop. To learn more about the other OER phases, read through the other modules in the following list:

- [Measuring the Traffic Class Performance and Link Utilization Using OER](#)
- [Configuring and Applying OER Policies](#)
- [Using OER to Control Traffic Classes and Verify the Route Control Changes](#)

Additional References

The following sections provide references related to using PFR to profile the traffic classes.

Related Documents

Related Topic	Document Title
Cisco OER technology overview	“ Cisco IOS Optimized Edge Routing Overview ” module
Concepts and configuration tasks required to set up OER network components	“ Setting Up OER Network Components ” module
Cisco OER commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	<i>Cisco IOS Optimized Edge Routing Command Reference</i>
IP prefix list commands	<i>Cisco IOS IP Routing Protocols Command Reference</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Using PfR to Profile the Traffic Classes

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(11)T, 12.2(33)SRB, 12.2(33)SXH or a later release, appear in the table.

For information on a feature in this technology that is not documented here, see the “Cisco IOS Optimized Edge Routing Features Roadmap.”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Using PfR to Profile the Traffic Classes

Feature Name	Releases	Feature Configuration Information
Port and Protocol Based Prefix Learning	12.3(11)T 12.2(33)SRB	Port and protocol based prefix learning allows you to configure a master controller to learn prefixes based on the protocol type and TCP or UDP port number. The following sections provide information about this feature: <ul style="list-style-type: none"> • Prefix Traffic Class Learning Using PfR, page 4 • Prefix Traffic Class Configuration Using PfR, page 9 The protocol command was introduced by this feature.
expire command ¹	12.3(14)T 12.2(33)SRB	The expire command is used to set an expiration period for learned prefixes. By default, the master controller removes inactive prefixes from the central policy database as memory is needed. This command allows you to refine this behavior by setting a time or session based limit. The time based limit is configured in minutes. The session based limit is configured for the number of monitor periods (or sessions).

Table 3 Feature Information for Using PfR to Profile the Traffic Classes (continued)

Feature Name	Releases	Feature Configuration Information
OER Application-Aware Routing: PBR	12.4(2)T 12.2(33)SRB	<p>The OER Application-Aware Routing: PBR feature introduces the capability to optimize IP traffic based on the type of application that is carried by the monitored prefix. Independent policy configuration is applied to the subset (application) of traffic.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Application Traffic Class Configuration Using PfR, page 10 <p>The following commands were introduced or modified by this feature: debug oer border pbr, debug oer master prefix, match ip address (OER), show oer master active-probes, and show oer master appl.</p>
OER BGP Inbound Optimization	12.4(9)T 12.2(33)SRB	<p>OER BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. OER uses eBGP advertisements to manipulate the best entrance selection.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Prefix Traffic Class Learning Using PfR, page 4 <p>The following commands were introduced or modified by this feature: clear oer master prefix, downgrade bgp, inside bgp, match ip address (OER), match oer learn, max range receive, maximum utilization receive, show oer master prefix.</p>

Table 3 *Feature Information for Using PfR to Profile the Traffic Classes (continued)*

Feature Name	Releases	Feature Configuration Information
OER DSCP Monitoring	12.4(9)T 12.2(33)SRB	<p>OER DSCP Monitoring introduced automatic learning of traffic classes based on protocol, port numbers, and DSCP value. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values, with the ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested. Layer 4 information such as protocol, port number, and DSCP information is now sent to the master controller database in addition to the Layer 3 prefix information. The new functionality allows OER to both actively and passively monitor application traffic.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Application Traffic Class Learning Using PfR, page 4 • Application Traffic Class Configuration Using PfR, page 10 <p>The following commands were introduced or modified by this feature: show oer border passive applications, show oer border passive cache, show oer border passive learn, show oer master appl, traffic-class aggregation, traffic-class filter, and traffic-class keys.</p>

Table 3 Feature Information for Using PfR to Profile the Traffic Classes (continued)

Feature Name	Releases	Feature Configuration Information
OER - Application Aware Routing with Static Application Mapping	12.4(15)T	<p>The OER - Application Aware Routing with Static Application Mapping feature introduces the ability to configure standard applications using just one keyword. In Cisco IOS Release 12.4(9)T, and prior releases, the definition of application traffic involves some awkward configuration. This feature also introduces a learn list configuration mode that allows Optimized Edge Routing (OER) policies to be applied to traffic classes profiled in a learn list. Different policies can be applied to each learn list. New traffic-class and match traffic-class commands are introduced to simplify the configuration of traffic classes that OER can automatically learn, or that can be manually configured.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Learn List Configuration Mode, page 5 • Static Application Mapping Using PfR, page 5 • Application Traffic Class Configuration Using PfR, page 10 • Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping, page 19 • Manually Selecting Traffic Classes Using Static Application Mapping, page 28 • Displaying and Resetting Traffic Class and Learn List Information, page 35 • Defining a Learn List to Automatically Learn Traffic Classes Using Static Application Mapping: Example, page 42 • Manually Selecting Traffic Classes Using Static Application Mapping: Example, page 44 <p>The following commands were introduced or modified by this feature: clear oer master traffic-class, count, delay (OER), list (OER), match traffic-class access-list, match traffic-class application, match traffic-class prefix-list, show oer border defined application, show oer master defined application, show oer master learn list, show oer master traffic-class, throughput, traffic-class access-list, traffic-class application, traffic-class prefix-list.</p>

Table 3 *Feature Information for Using PfR to Profile the Traffic Classes (continued)*

Feature Name	Releases	Feature Configuration Information
OER Border Router Only Functionality	12.2(33)SXH	<p>In Cisco IOS Release 12.2(33)SXH support for using a Cisco Catalyst 6500 series switch as an OER border router was introduced. Only border router functionality is included in the Cisco IOS Release 12.2(33)SXH images; no master controller configuration is available. The master controller that communicates with the Cisco Catalyst 6500 series switch being used as a border router must be a router running Cisco IOS Release 12.4(6)T or a later release. The OER master controller software has been modified to handle the limited functionality supported by the Cisco Catalyst 6500 border routers. Using the Route Processor (RP), the Catalyst 6500 border routers can capture throughput statistics only for a traffic class compared to the delay, loss, unreachability, and throughput statistics collected by non-Catalyst 6500 border routers. A master controller automatically detects the limited capabilities of the Catalyst 6500 border routers and downgrades other border routers to capture only the throughput statistics for traffic classes. By ignoring other types of statistics, the master controller is presented with a uniform view of the border router functionality.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Restrictions for Using PfR to Profile the Traffic Classes, page 2 <p>The following command was introduced or modified by this feature: show oer border passive cache.</p>

Table 3 Feature Information for Using PfR to Profile the Traffic Classes (continued)

Feature Name	Releases	Feature Configuration Information
Performance Routing with NBAR/CCE Application Recognition	12.4(20)T	<p>The Performance Routing with NBAR/CCE Application Recognition feature introduces the ability to profile an application-based traffic class using Network-Based Application Recognition (NBAR). NBAR is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. PfR uses NBAR to recognize and classify a protocol or application, and the resulting traffic classes are added to the PfR application database to be passively and actively monitored.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PfR Application Mapping Using NBAR, page 7 • Application Traffic Class Configuration Using PfR, page 10 • Defining a Learn List to Automatically Learn Traffic Classes Using NBAR Application Mapping, page 24 • Manually Selecting Traffic Classes Using NBAR Application Mapping, page 30 • Displaying and Resetting Information About Traffic Classes Identified Using NBAR, page 37 • Defining a Learn List to Automatically Learn Traffic Classes Using NBAR Application Mapping: Example, page 43 • Manually Selecting Traffic Classes Using NBAR Application Mapping: Example, page 44 <p>The following commands were introduced or modified by this feature: application define, clear oer master traffic-class application nbar, match traffic-class application nbar, show oer border routes, show oer master nbar application, show oer master traffic-class application nbar, traffic-class application nbar.</p>

1. This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.

