Performance Routing with NBAR CCE Application Recognition

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. Performance Routing (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.

Prerequisites for PfR with NBAR CCE Application Recognition

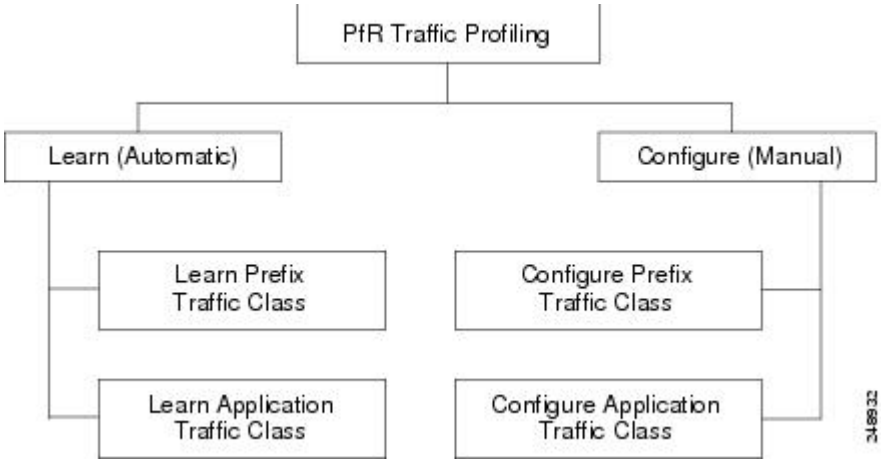
Cisco Express Forwarding (CEF) must be enabled on all participating devices. No other switching path is supported, even if otherwise supported by Policy-Based Routing (PBR).

Information About PfR with NBAR CCE Application Recognition

Performance Routing Traffic Class Profiling

Before optimizing traffic, Performance Routing (PfR) must determine the traffic classes from the traffic that is 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-class 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. Both the learn mechanism and the configure mechanism for traffic classes are implemented during the PfR profile phase. The overall structure of the PfR traffic class profile process and its components can be seen in the figure below.

Figure 1: PfR Traffic Class Profiling Process



PfR can automatically learn the traffic classes while monitoring the traffic flow through border routers using the embedded NetFlow capability. 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. Within the automatic traffic class learning process, there are three components:

- Automatic learning of prefix-based traffic classes
- Automatic learning of application-based traffic classes
- Using learn lists to categorize both prefix-based and application-based traffic classes

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
- Manually configuring application-based traffic classes

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

More details about each of the traffic class profiling components in the figure above are contained in the "Understanding Performance Routing" module.

PfR Application Mapping Using NBAR

The Performance Routing with NBAR CCE Application Recognition feature introduces the ability to profile an application-based traffic class using NBAR. 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 **traffic-class application nbar** (PfR) command is used 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 can identify 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 to determine if an application that can be identified using NBAR is available for use with Performance Routing.

In addition to the static applications supported by the OER—Application Aware Routing with Static Application Mapping feature, and many applications based on non-UDP and non-TCP protocols, the table below 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 1: 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

Application	Keyword	Protocol	Port
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
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 *QoS: NBAR Configuration Guide*.

How to Configure PfR with NBAR CCE Application Recognition

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.

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. With the Performance Routing with NBAR CCE Application Recognition feature, the ability to use applications identified using NBAR was introduced.

In this task, 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 includes only 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, see the “Displaying and Resetting Information About Traffic Classes Identified Using NBAR” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. **pfr 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} **Example:** `Device(config)# ip prefix-list INCLUDE_10_NET permit 10.0.0.0/8`	Creates an IP prefix list to filter prefixes for learning. • 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	**pfr master** **Example:** `Device(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco routing device as a master controller and to configure the master controller policy and timer settings.
Step 5	**learn** **Example:** `Device(config-pfr-mc)# learn`	Enters PfR Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.
Step 6	**list seq** *number* **refname** *refname* **Example:**	Creates a PfR learn list and enters learn list configuration mode.

	Command or Action	Purpose
	`Device(config-pfr-mc-learn)# list seq 10 refname LEARN_RTP_AUDIO_TC`	• Use the **seq** keyword and *number* argument to specify a sequence number used to determine the order in which learn list criteria are applied. • Use the **refname** keyword and *refname* argument to specify a reference name for the learn list. • The example creates a learn list named LEARN_RTP_AUDIO_TC.
Step 7	**traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] [**filter** *prefix-list-name*] **Example:** `Device(config-pfr-mc-learn-list)# traffic-class application nbar rtp:audio`	Defines a PfR traffic class using an application that can be identified using NBAR. • Use the *nbar-app-name* argument to specify one or more applications identified using NBAR. • The example defines a traffic class as containing RTP-audio traffic.
Step 8	**aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*} **Example:** `Device(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	(Optional) Configures a master controller to aggregate learned prefixes based on traffic flow type. • 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 is 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	**throughput** **Example:** `Device(config-pfr-mc-learn-list)# throughput`	Configures the master controller to learn the top prefixes based on the highest outbound throughput. • 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	**exit** **Example:** `Device(config-pfr-mc-learn-list)# exit`	Exits learn list configuration mode, and returns to PfR Top Talker and Top Delay learning configuration mode.
Step 11	**list seq** *number* **refname** *refname* **Example:** `Device(config-pfr-mc-learn)# list seq 10 refname LEARN_SKYPE_TC`	Creates an PfR learn list and enters learn list configuration mode. • Use the **seq** keyword and *number* argument to specify a sequence number used to determine the order in which learn list criteria are applied. • Use the **refname** keyword and *refname* argument to specify a reference name for the learn list. • The example creates a learn list named LEARN_SKYPE_TC.
Step 12	**traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] [**filter** *prefix-list-name*] **Example:** `Device(config-pfr-mc-learn-list)# traffic-class application nbar skype filter INCLUDE_10_NET`	Defines a PfR traffic class using an application that can be identified using NBAR. • Use the *nbar-app-name* argument to specify one or more applications identified using NBAR. • 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	**aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*} **Example:** `Device(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	(Optional) Configures a master controller to aggregate learned prefixes based on traffic-flow type. • 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 is 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:** `Device(config-pfr-mc-learn-list)# throughput`	Configures the master controller to learn the top prefixes based on the highest outbound throughput. • 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:** `Device(config-pfr-mc-learn-list)# end`	Exits learn list configuration mode, and returns to privileged EXEC mode.

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** (PfR) command. Using a PfR 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, see the “Displaying and Resetting Information About Traffic Classes Identified Using NBAR” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. Repeat Step 3 for more prefix list entries, as required.
5. **pfr-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. • Enter your password if prompted.

	Command or Action	Purpose
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*} **Example:** `Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24`	Creates a prefix list to specify destination prefix-based traffic classes. • 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	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map APPL_NBAR_MAP 10`	Enters PfR map configuration mode to configure a PfR map. • Only one match clause can be configured for each PfR map sequence. • Permit sequences are first defined in an IP prefix list and then applied with the **match traffic-class application nbar** (PfR) command in Step 6. • The example creates a PfR map named APPL_NBAR_MAP.
Step 6	**match traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] **prefix-list** *prefix-list-name* **Example:** `Router(config-pfr-map)# match traffic-class application nbar bittorrent directconnect prefix-list LIST1`	Manually configures one or more applications that can be identified using NBAR as match criteria against a prefix list to create traffic classes using a PfR map. • Use the *nbar-app-name* argument to specify one or more 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	**end** **Example:** `Router(config-pfr-map)# end`	(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Displaying and Resetting 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 a PfR 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.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 Go to the router configured a master controller.

Step 2 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
```

Step 3 **show pfr master traffic-class application nbar** *nbar-app-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 a PfR master controller. The following example shows information about traffic classes consisting of Real-Time Transport Protocol streaming audio (RTP-audio) traffic.

Example:

```
Device# show pfr 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        U        0        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        U        0        0        1        2
            250      200        0        0       30        0
```

Step 4 **show pfr master nbar application**

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

Example:

```
Device# show pfr 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 pfr master defined application**

This command is used to display information about user-defined application definitions used in PfR:

Example:

```
Device# show pfr 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 pfr 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 PfR traffic classes defined by the RTP-Audio application that is identified using NBAR and filtered by the 10.1.1.0/24 prefix:

Example:

```
Device# clear pfr master traffic-class application nbar rtp:audio 10.1.1.0/24
```

Step 7 Go to a border router that is configured as part of the PfR network.

Step 8 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
```

Step 9 **show pfr border routes** {**bgp** | **cce** | **static**}

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

Example:

```
Device# show pfr border routes cce

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

Step 10 **show pfr border defined application**

This command is used to display all user-defined applications monitored by a PfR border router:

Example:

```
Device# show pfr 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 PfR with NBAR CCE Application Recognition

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

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 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 includes only 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
pfr 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
pfr-map STREAM_AUDIO 10
 match learn list LEARN_RTP_AUDIO_TC
 exit
pfr-map REMOTE_AUDIO_VIDEO 20
 match learn list LEARN_SKYPE_TC
 end
```

Example: Manually Selecting Traffic Classes Using NBAR Application Mapping

The following example, starting in global configuration mode, configures a PfR 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
pfr-map PREFIXES 10
 match traffic-class application nbar bittorrent directconnect prefix-list LIST1
 end
```

Feature Information for PfR with NBAR CCE Application Recognition

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2: Feature Information for PfR with NBAR CCE Application Recognition

Feature Name	Releases	Feature Configuration Information
Performance Routing with NBAR/CCE Application Recognition	12.4(20)T Cisco IOS XE Release 3.7S	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. The following commands were introduced or modified by this feature: **application define (PfR)**, **clear pfr master traffic-class application nbar**, **match traffic-class application nbar (PfR)**, **show pfr border routes**, **show pfr master nbar application**, **show pfr master traffic-class application nbar**, **traffic-class application nbar (PfR)**.