Network-Based Application Recognition and Distributed Network-Based Application Recognition

Figure 1 Feature History

Cisco IOS Release	Modification
12.0(5)XE2	The NBAR feature was introduced. The first implementation of the NBAR feature was available on Cisco 7100 and Cisco 7200 series routers.
12.1(1)E	Subport classification of HTTP traffic by host name for NBAR was introduced.
12.1(2)E	Support for the Citrix, Novadigm, and Printer protocols for NBAR was introduced.
12.1(5)T	This feature was introduced for the Cisco IOS Release 12.1 T train. NBAR became available on Cisco 2600 and 3600 series routers.
12.1(6)E	The dNBAR feature, which introduced NBAR functionality on the Cisco 7500 with a VIP and the Catalyst 6000 family switch with a Flexwan module, was introduced.
12.1(10)EC	NBAR was introduced for Cisco 7100 UBR and Cisco 7200 UBR routers.
12.1(11b)E	The **match protocol rtp** command was introduced on the Cisco IOS Release 12.1 E train.
12.1(12c)E	The **match protocol gnutella** and **match protocol fasttrack** commands were added because Gnutella and FastTrack became available as NBAR-supported protocols.
12.1(13)E	NBAR was released on the Catalyst 6000 family switch without a FlexWAN module.
12.2(2)T	This feature was introduced on Cisco 1700 series routers.
12.2(4)T3	The dNBAR feature introduced NBAR functionality on the Cisco IOS Release 12.2 T train. This feature was introduced for the Cisco 7500 series router with a VIP only.

Figure 1 Feature History (continued)

Cisco IOS Release	Modification
12.2(8)T	The **match protocol rtp** command was introduced, allowing NBAR to classify Real-Time Transport Protocol (RTP) traffic. The Cisco 3700 also became available. The initial release of the Cisco 3700 supported NBAR.
12.2(14)S	NBAR and dNBAR were introduced in Cisco IOS Release 12.2S. The 12.2S version of NBAR includes everything available on the 12.1E and 12.2T implementations of NBAR with the exception of platform support for platforms not supported by 12.2S.

This document provides information for the Network-Based Application Recognition (NBAR) and the Distributed Network-Based Application Recognition (dNBAR) features. This document contains all of the updates made to the NBAR and dNBAR features.

Before proceeding, it is important to note that the dNBAR feature, which introduced NBAR on the Cisco 7500 with a Versatile Interface Processor (VIP) and the Catalyst 6000 family switch with a FlexWAN module, is identical in implementation to NBAR. Therefore, unless otherwise noted, the term NBAR is used throughout this document to describe both the NBAR and dNBAR feature. The term dNBAR is used only when appropriate.

This document includes information on the benefits of NBAR, supported platforms, restrictions, definitions, and new and revised command syntax.

This document includes the following sections:

Feature Overview

The purpose of IP Quality of Service (QoS) is to provide appropriate network resources (bandwidth, delay, jitter and packet loss) to applications. QoS maximizes the return on investments on network infrastructure by ensuring that mission critical applications get the required performance and non-critical applications do not hamper the performance of critical applications.

IP QoS can be deployed by defining classes or categories of applications. These classes are defined by using various classification techniques available in Cisco IOS software. After these classes are defined and attached to an interface, the desired QoS features, such as Marking, Congestion Management, Congestion Avoidance, Link Efficiency mechanisms, or Policing and Shaping can then be applied to the classified traffic to provide the appropriate network resources amongst the defined classes.

Classification, therefore, is an important first-step in configuring QoS in a network infrastructure.

NBAR is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by classifying packets and then applying Quality of Service (QoS) to the classified traffic. Some examples of class-based QoS features that can be used on traffic after the traffic is classified by NBAR include:

- Class-Based Marking (the **set** command)
- Class-Based Weighted Fair Queueing (the **bandwidth** and **queue-limit** commands)
- Low Latency Queueing (the **priority** command)
- Traffic Policing (the **police** command)
- Traffic Shaping (the **shape** command)

Note For an animated example of NBAR being used with other QoS features to solve a network problem, click here.

Note The NBAR feature is used for classifying traffic by protocol. The other class-based QoS features determine how the classified traffic is forwarded and are documented separately from NBAR. Furthermore, NBAR is not the only method of classifying network traffic so that QoS features can be applied to classified traffic.
For information on the class-based features that can be used to forward NBAR-classified traffic, see the individual feature modules for the particular class-based feature as well as the *Cisco IOS Quality of Service Solutions Guide*.
Many of the non-NBAR classification options for QoS are documented in the "Modular Quality of Service Command-Line Interface" section of the *Cisco IOS Quality of Service Solutions Guide*. These commands are configured using the **match** command in class map configuration mode.

NBAR introduces several new classification features that identify applications and protocols from Layer 4 through Layer 7:

- Statically assigned TCP and UDP port numbers
- Non-UDP and non-TCP IP protocols
- Dynamically assigned TCP and UCP port numbers. Classification of such applications requires stateful inspection; that is, the ability to discover the data connections to be classified by parsing the connections where the port assignments are made.
- Sub-port classification or classification based on deep packet inspection; that is. classification by looking deeper into the packet.

NBAR can classify static port protocols. Although access control lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACLs.

NBAR includes a Protocol Discovery feature that provides an easy way to discover application protocols that are transversing an interface. The Protocol Discovery feature discovers any protocol traffic supported by NBAR. Protocol Discovery maintains the following per-protocol statistics for enabled interfaces: total number of input and output packets and bytes, and input and output bit rates. The Protocol Discovery feature captures key statistics associated with each protocol in a network that can be used to define traffic classes and QoS policies for each traffic class.

Benefits

Ability to Identify and Classify Network Traffic by Protocol

Identifying and classifying network traffic is an important first step in implementing QoS. A network administrator can more effectively implement QoS in a networking environment after identifying the amount and the variety of applications and protocols running on a network.

NBAR gives network administrators the ability to see the variety of protocols and the amount of traffic generated by each protocol. After gathering this information, NBAR allows users to implement classes of traffic. These classes of traffic can then be used to provide different levels of service for network traffic, therefore allowing better network management by providing the right level of network resources for network traffic.

NBAR Application Notes

The following section provides information on several topics that could be useful to individuals configuring NBAR in their networks. The following topics are covered in this section:

- Catalyst 6000 Family Switches without FlexWAN Modules Application Notes
- Packet Description Language Module
- Classification of HTTP by URL, Host, or MIME
- Classification of Citrix ICA Traffic by Application Name
- RTP Payload Type Classification
- Classification of Custom Applications
- Classification of Peer-to-Peer File Sharing Applications
- Enhancements after Initial NBAR Release
- Supported Protocols

Catalyst 6000 Family Switches without FlexWAN Modules Application Notes

When NBAR is enabled on a Catalyst 6000 without a FlexWAN module interface, all traffic flows entering or leaving the NBAR-enabled interface will be processed in software on the MSFC2.

The following other restrictions should also be noted when running NBAR:

- NBAR can only be implemented on an MSFC2 with Supervisor Engine 1 or Supervisor Engine 2.

- NBAR Protocol Discovery or QoS service policies using NBAR to match protocols cannot co-exist on an interface that contains Catalyst 6000-specific QoS actions. Refer to the Catalyst 6000 QoS Guide for Catalyst 6000-specific QoS actions (at the time of this publication, the current Catalyst 6000-specific QoS actions were **police** and **trust**, but please refer to the Catalyst 6000 QoS Guide guide for additional information).

The following table provides configuration results when NBAR is added to an interface. The results vary depending on the current configuration of the policy map on the interface.

Table 1 NBAR Behavior Descriptions

Current Policy Map State	Action	Result
At least one service policy with platform-specific QoS action in the policy map is attached to interface.	Enable Protocol Discovery on the interface	Protocol Discovery is rejected.
No service policies on the interface have NBAR or a platform-specific QoS action in policy map.	Enable Protocol Discovery on the interface.	Protocol Discovery is accepted, but the service policy is disabled from the interface.
A service policy on the interface contains **match protocol** NBAR commands.	Enable Protocol Discovery on the interface	Protocol Discovery is accepted.
No policy map is on the interface.	Enable Protocol Discovery on the interface.	The command is accepted. Traffic is processed on the MSFC2 once the command is accepted.
No policy map is on the interface	Disable Protocol Discovery	The command is accepted. Traffic is no longer processed on the MSFC2.
No service policies on the interface have platform-specific QoS actions or **match protocol** NBAR commands.	Disable Protocol Discovery.	Protocol Discovery is disabled. The service policy is removed from the interface. The service policy can be reattached.
At least one service policy on the interface is using the **match protocol** NBAR command.	Disable Protocol Discovery.	Protocol Discovery is disabled.
A service policy with a platform-specific QoS action and Protocol Discovery is enabled on the interface.	Attach service policy to interface,	Reject the service policy. Protocol Discovery and platform-specific QoS actions cannot be enabled in the same policy map.

Current Policy Map State	Action	Result
Protocol Discovery is enabled on an interface and the service policy has a non-platform specific QoS action.	Attach service policy to interface	The policy map is attached. The policy map has to be attached in IOS QoS mode.
No match protocol NBAR commands are in any service policy on the interface and Protocol Discovery is not enabled.	Attach service policy to interface	The policy map is attached in Catalyst 6000 QoS mode.
Protocol Discovery is not enabled on the interface and **match protocol** NBAR commands are in at least one service policy on the interface.	Attach service policy to interface	The service policy is attached in IOS mode and traffic is processed using the MSFC2.
A service policy that has no **match protocol** NBAR commands and no Protocol Discovery needs to be removed from the interface. The interface contains no other service policies which contain **match protocol** NBAR commands or Protocol Discovery.	Detach service policy from interface	The service policy is detached like any other service policy.
A service policy with **match protocol** NBAR commands needs to be detached from the interface. Another service policy attached in the opposite direction does not contain **match protocol** NBAR commands. No Protocol Discovery is enabled on the interface.	Detach service policy with **match protocol** NBAR commands from the interface	The service policy is detached and the other service policy in the opposite direction is also removed. Traffic is no longer processed using the MSFC2.
A service policy contains **match protocol** NBAR command and the policy in the other direction needs **match protocol** NBAR or Protocol Discovery needs to be enabled on the interface.	Detach service policy from interface.	The service policy is detached. Continue to process traffic on the MSFC2 so that **match protocol** can be enabled on the other service policy or Protocol Discovery can be enabled on the interface.

Current Policy Map State	Action	Result
A service policy contains **match protocol** NBAR command. No other service policies are on the interface and Protocol Discovery is not enabled.	Detach service policy from interface	Service policy is detached. Traffic is no longer processed on the MSFC2.

Packet Description Language Module

An external Packet Description Language Module (PDLM) can be loaded at run time to extend the NBAR list of recognized protocols. PDLMs can also be used to enhance an existing protocol recognition capability. PDLMs allow NBAR to recognize new protocols without requiring a new IOS image or a router reload.

New PDLMs will only be released by Cisco and can be loaded from Flash memory. Please contact your local Cisco representative to request additions or changes to the set of protocols classified by NBAR.

To view a list of currently available PDLMs or to download a PDLM, go to the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/pdlm

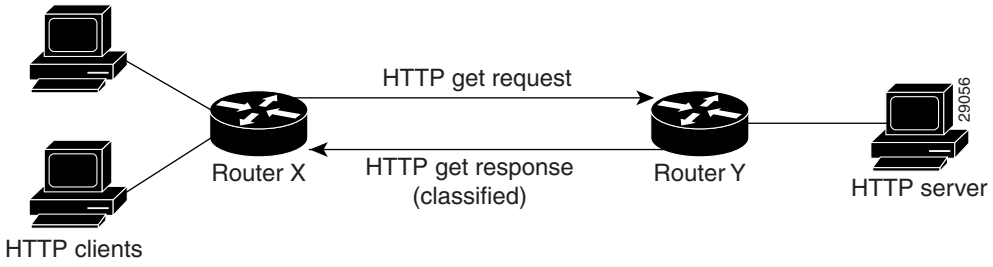
Classification of HTTP by URL, Host, or MIME

NBAR can classify application traffic by looking beyond the TCP/UDP port numbers of a packet. This is subport classification. NBAR looks into the TCP/UDP payload itself and classifies packets on content within the payload such as transaction identifier, message type, or other similar data.

Classification of HTTP by URL, host, or Multipurpose Internet Mail Extension (MIME) type is an example of subport classification. NBAR classifies HTTP traffic by text within the URL or host fields of a request using regular expression matching. HTTP URL matching in NBAR supports GET, PUT, HEAD, POST, DELETE, and TRACE. NBAR uses the UNIX filename specification as the basis for the URL or host specification format. The NBAR engine then converts the specified match string into a regular expression.

NBAR recognizes HTTP packets containing the URL and classifies all packets that are sent to the source of the HTTP request. Figure 2 illustrates a network topology with NBAR in which Router Y is the NBAR-enabled router.

Figure 2 Network Topology with NBAR



When specifying a URL for classification, include only the portion of the URL following the www.hostname.domain in the match statement. For example, for the URL www.cisco.com/latest/whatsnew.html, include only /latest/whatsnew.html.

Host specification is identical to URL specification. NBAR performs a regular expression match on the host field contents inside an HTTP packet and classifies all packets from that host. For example, for the URL www.cisco.com/latest/whatsnew.html, include only www.cisco.com.

For MIME type matching, the MIME type can contain any user-specified text string. A list of the Internet Assigned Numbers Authority (IANA)-supported MIME types can be found at:

ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/media-types

In MIME type matching, NBAR classifies the packet containing the MIME type and all subsequent packets, which are sent to the source of the HTTP request.

NBAR supports URL and host classification in the presence of persistent HTTP. NBAR does not classify packets that are part of a pipelined request. With pipelined requests, multiple requests are pipelined to the server before previous requests are serviced. Pipelined requests are a less commonly used type of persistent HTTP request.

Classification of Citrix ICA Traffic by Application Name

NBAR can classify Citrix Independent Computing Architecture (ICA) traffic and perform subport classification of Citrix traffic based on Citrix published applications. NBAR can monitor Citrix ICA client requests for a published application destined to a Citrix ICA Master browser. After the client requests to the published application, the Citrix ICA Master browser directs the client to the server with the most available memory. The Citrix ICA client then connects to this Citrix ICA server for the application.

NBAR statefully tracks Citrix ICA server client messages and classifies requests for given Citrix application names and traffic. A Citrix application is named when published on a Citrix ICA server. NBAR performs a regular expression match using a user-specified application name string on the contents of the Citrix ICA control packets carrying the published application name. Therefore, users need to specify a regular expression that will result in a match for the published application name if they want to match a specified application. See the **match protocol citrix** command in the "Command Reference" section for additional information.

Citrix ICA clients can be configured in various modes. NBAR cannot distinguish among Citrix applications in all modes of operation. Therefore, network administrators might need to collaborate with Citrix administrators to ensure that NBAR properly classifies Citrix traffic.

A Citrix administrator can configure Citrix to publish Citrix applications individually or as the entire desktop. In the Published Desktop mode of operation, all applications within the published desktop of a client use the same TCP session. Therefore, differentiation among applications is impossible, and NBAR can only be used to classify Citrix applications as aggregates (by looking at port 1494).

The Published Application mode for Citrix ICA clients is recommended when you use NBAR. In Published Application mode, a Citrix administrator can configure a Citrix client in either seamless or non-seamless (windows) modes of operation. In non-seamless mode, each Citrix application uses a separate TCP connection, and NBAR can be used to provide interapplication differentiation based on the name of the published application.

Seamless mode clients can operate in one of two submodes: session sharing or non-session sharing. In seamless session sharing mode, all clients share the same TCP connection, and NBAR cannot differentiate among applications. Seamless sharing mode is enabled by default on some software releases.

In seamless non-session sharing mode, each application for each particular client uses a separate TCP connection. NBAR can provide interapplication differentiation in seamless non-session sharing mode.

Session sharing can be turned off using the following steps:

Step 1 At the command prompt of the Citrix server, open the registry editor by entering the **regedit** command.

Step 2 Create the following registry entry (which overrides session sharing):

```
[HKLM]\SYSTEM\CurrentControlSet\Control\Citrix\WFSHELL\TWI
Value name: "SeamlessFlags", type DWORD, possible values :0 or 1
```

Setting this registry value to 1 overrides session sharing. Note that this flag is SERVER GLOBAL.

Note NBAR operates properly in Citrix ICA secure mode. Pipelined Citrix ICA client requests are not supported.

RTP Payload Type Classification

RTP is a packet format for multimedia data streams. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part. The control part is called Real-time Transport Control Protocol (RTCP). It is important to note that the NBAR RTP Payload Classification feature does not identify RTCP packets, and that RTCP packets run on odd port numbered ports while RTP packets run on even numbered port.

The data part of RTP is a thin protocol providing support for applications with real-time properties such as continuous media (such as audio and video), which includes timing reconstruction, loss detection, and security and content identification. RTP is discussed in RFC 1889 and RFC 1890.

The RTP payload type is the data transported by RTP in a packet, for example audio samples or compressed video data.

NBAR RTP payload classification not only allows one to statefully identify real time audio and video traffic, but it also can differentiate on the basis of audio and video CODECs to provide more granular Quality of Service. The RTP Payload Classification, therefore, looks deep into the RTP header to classify RTP packets.

NBAR RTP Payload Type Classification was first introduced in Cisco IOS Release 12.2(8)T and is also available in Cisco IOS Release 12.1(11b)E.

Classification of Custom Applications

The Custom protocol supports static port-based protocols and applications that are not currently supported in NBAR. This functionality allows mapping of static TCP and UDP port numbers to custom-xx protocol within NBAR. The custom protocol is also available as a PDLM if your version of IOS supports NBAR but not the custom protocol.

10 custom applications can be assigned using NBAR, and each customer application can have up to 16 TCP and 16 UDP ports each mapped to the individual custom protocol. The real-time statistics of each custom protocol can be monitored using Protocol Discovery.

In the following example, a gaming application that runs on tcp port 8877 needs to be classified using NBAR. You can use custom-01 to map TCP port 8877 by entering the following command:

```
Router(config)# ip nbar port-map custom-01 tcp 8877
```

Classification of Peer-to-Peer File Sharing Applications

Gnutella and FastTrack are peer-to-peer file sharing protocols that became classifiable using NBAR in Cisco IOS Release 12.1(12c)E.

The **match protocol gnutella file-transfer** "*regular-expression*" and **match protocol fasttrack file-transfer** "*regular-expression*" commands are used to enable Gnutella and FastTrack classification in a traffic class. The regular-expression variable can be expressed as "*" to indicate that all FastTrack or Gnutella traffic be classified by a traffic class.

In the following example, all FastTrack traffic is classified into class map nbar:

```
class-map match-all nbar
match protocol fasttrack file-transfer "*"
```

Similarly, all Gnutella traffic is classified into class map nbar in this example:

```
class-map match-all nbar
match protocol gnutella file-transfer "*"
```

Wildcard characters in a regular expression can also be used to identify specified Gnutella and FastTrack traffic. These regular expression matches can be used to match based on a filename extension or on a particular string in a filename.

In the following example, all Gnutella files that have the ".mpeg" extension will be classified into class map nbar.

```
class-map match-all nbar
match protocol gnutella file-transfer "*.mpeg"
```

In the following example, only Gnutella traffic that contains the characters "cisco" is classified:

```
class-map match-all nbar
match protocol gnutella file-transfer "*cisco*"
```

The same examples can be used for FastTrack traffic:

```
class-map match-all nbar
match protocol fasttrack file-transfer "*.mpeg"
```

or

```
class-map match-all nbar
match protocol fasttrack file-transfer "*cisco*"
```

Applications that use FastTrack include KaZaA, Grokster, and Morpheus (although newer versions of Morpheus use Gnutella).

Applications that use Gnutella include:

- BearShare
- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- JTella
- LimeWire
- Morpheus
- Mutella
- Phex
- Qtella
- Swapper
- XoloX
- XCache

Enhancements after Initial NBAR Release

The following table provides a brief overview of enhancements made to the NBAR feature after NBAR was initially introduced on the Cisco 7100 and 7200 series routers in Cisco IOS Release 12.0(5)XE2.

Note This list only contains NBAR enhancements that occurred in Cisco IOS Releases 12.0 XE, 12.1 E, and 12.1 T. If you are using NBAR on an Early Deployment train based on one of these releases that contained the enhancement, NBAR is likely available in your release. See your release documentation to ensure NBAR is available in your software release.

Table 2 NBAR Enhancement Descriptions

Enhancement	Description
FastTrack and Gnutella Classification	In Cisco IOS Release 12.1(12c)E, NBAR introduced the ability to classify traffic based on the FastTrack and Gnutella protocols.
RTP Payload Type Classification	In Cisco IOS Release 12.2(8)T, NBAR introduced the ability to classify traffic based on the RTP protocol. This capability also became available on the Cisco IOS Release 12.1(11b)E release in Cisco IOS Release 12.1(11b)E. RTP is the protocol for the transport of real-time data, including audio and video, over the Internet. With the addition of RTP support classification, NBAR can now classify RTP traffic and apply user-configured QoS treatment to RTP traffic.
Availability on Cisco 1700 series routers	NBAR became available for Cisco 1700 series routers in Cisco IOS Release 12.2(2)T.

Enhancement	Description
Availability on Cisco 7100 UBR and Cisco 7200 UBR universal broadband routers	NBAR became available for the Cisco 7100 UBR and Cisco 7200 UBR is Cisco IOS Release 12.1(10)EC.
Availability on Cisco 7500 with VIP and Catalyst 6000 family with a FlexWAN module	The dNBAR feature, which introduced NBAR functionality on the Cisco 7500 with a VIP and the Catalyst 6000 family switch with a FlexWAN module, was initially introduced in Cisco IOS Release 12.1(6)E.
Availability on Cisco IOS Release 12.1 T	NBAR became available for the Cisco IOS Release 12.1 T release train in Cisco IOS Release 12.1(5)T.
Availability on Cisco 2600 and 3600 series routers	NBAR became available for the Cisco 2600 and 3600 series routers in Cisco IOS Release 12.1(5)T.
Support for Citrix, Novadigm, and Printer protocols	In Cisco IOS Release 12.1(2)E, NBAR introduced support for the following protocols: • Support for Citrix, including matching on Citrix application name. • Support for Novadigm and Printer protocols
HTTP traffic matching by hostname.	Beginning in Cisco IOS Release 12.1(1)E, NBAR could perform subport classification of HTTP traffic by host name. You can classify HTTP traffic by web server names. To perform a match on this host name portion of the URL, use the new host match criteria.

Supported Protocols

NBAR is capable of classifying the following three types of protocols:

- Non-UDP and non-TCP IP protocols
- TCP and UDP protocols that use statically assigned port numbers
- TCP and UDP protocols that dynamically assign port numbers and therefore require stateful inspection. This table includes packets that require sub-port classification and classification based on deep packet inspection.

Table 3 Non-UDP and Non-TCP Protocols

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release[1]
EGP	IP	8	Exterior Gateway Protocol	egp	12.0(5)XE2 12.1(1)E 12.1(5)T
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T

Table 3 Non-UDP and Non-TCP Protocols (continued)

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release[1]
GRE	IP	47	Generic Routing Encapsulation	gre	12.0(5)XE2 12.1(1)E 12.1(5)T
ICMP	IP	1	Internet Control Message Protocol	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T
IPINIP	IP	4	IP in IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T
IPSec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T

1. Indicates the Cisco IOS maintenance release that first supported the protocol. This table is updated when a protocol is added to a new Cisco IOS release train.

Table 4 TCP and UDP Static Port Protocols

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release[1]
BGP	TCP/UDP	179	Border Gateway Protocol	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	UDP	24032	Desktop video conferencing	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
DHCP/ BOOTP	UDP	67, 68	Dynamic Host Configuration Protocol/ Bootstrap Protocol	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T
DNS	TCP/UDP	53	Domain Name System	dns	12.0(5)XE2 12.1(1)E 12.1(5)T
Finger	TCP	79	Finger user information protocol	finger	12.0(5)XE2 12.1(1)E 12.1(5)T
Gopher	TCP/UDP	70	Internet Gopher Protocol	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T

Table 4 TCP and UDP Static Port Protocols (continued)

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release[1]
HTTP	TCP	80	Hypertext Transfer Protocol	http	12.0(5)XE2 12.1(1)E 12.1(5)T
HTTPS	TCP	443	Secured HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol	imap	12.0(5)XE2 12.1(1)E 12.1(5)T
IRC	TCP/UDP	194	Internet Relay Chat	irc	12.0(5)XE2 12.1(1)E 12.1(5)T
Kerberos	TCP/UDP	88, 749	Kerberos Network Authentication Service	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T
L2TP	UDP	1701	L2F/L2TP tunnel	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-PPTP	TCP	1723	Microsoft Point-to-Point Tunneling Protocol for VPN	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T
NetBIOS	TCP	137, 139	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
NetBIOS	UDP	137, 138	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
NFS	TCP/UDP	2049	Network File System	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T
NNTP	TCP/UDP	119	Network News Transfer Protocol	nntp	12.0(5)XE2 12.1(1)E 12.1(5)T

Table 4 TCP and UDP Static Port Protocols (continued)

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release[1]
Notes	TCP/UDP	1352	Lotus Notes	notes	12.0(5)XE2 12.1(1)E 12.1(5)T
Novadigm	TCP/UDP	3460-3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T
NTP	TCP/UDP	123	Network Time Protocol	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
POP3	TCP/UDP	110	Post Office Protocol	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
Printer	TCP/UDP	515	Printer	printer	12.1(2)E 12.1(5)T
RIP	UDP	520	Routing Information Protocol	rip	12.0(5)XE2 12.1(1)E 12.1(5)T
RSVP	UDP	1698, 1699	Resource Reservation Protocol	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T
SFTP	TCP	990	Secure FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
SHTTP	TCP	443	Secure HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
SIMAP	TCP/UDP	585, 993	Secure IMAP	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T
SIRC	TCP/UDP	994	Secure IRC	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T
SLDAP	TCP/UDP	636	Secure LDAP	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T

Table 4 TCP and UDP Static Port Protocols (continued)

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release[1]
SMTP	TCP	25	Simple Mail Transfer Protocol	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNNTP	TCP/UDP	563	Secure NNTP	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
SOCKS	TCP	1080	Firewall security protocol	socks	12.0(5)XE2 12.1(1)E 12.1(5)T
SPOP3	TCP/UDP	995	Secure POP3	secure-pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
SSH	TCP	22	Secured Shell	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T
STELNET	TCP	992	Secure Telnet	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
Syslog	UDP	514	System Logging Utility	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T
Telnet	TCP	23	Telnet Protocol	telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
X Windows	TCP	6000-6003	X11, X Windows	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T

1. Indicates the Cisco IOS maintenance release that first supported the protocol. This table is updated when a protocol is added to a new Cisco IOS release train.

Table 5 TCP and UDP Stateful Protocols

Protocol	Type	Description	Syntax	Cisco IOS Release[1]
Citrix ICA	TCP/ UDP	Citrix ICA traffic by application name	citrix citrix app	12.1(2)E 12.1(5)T

Table 5 TCP and UDP Stateful Protocols (continued)

Protocol	Type	Description	Syntax	Cisco IOS Release[1]
FTP	TCP	File Transfer Protocol	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
Exchange	TCP	MS-RPC for Exchange	exchange	12.0(5)XE2 12.1(1)E 12.1(5)T
FastTrack		FastTrack For a list of common FastTrack applications, see the "Classification of Peer-to-Peer File Sharing Applications" section of this document.	fasttrack	12.1(12c)E
Gnutella	TCP	Gnutella For a list of common Gnutella applications, see the "Classification of Peer-to-Peer File Sharing Applications" section of this document.	gnutella	12.1(12c)E
HTTP	TCP	HTTP with URL, MIME, or host classification	http	12.0(5)XE2 12.1(1)E 12.1(5)T (HTTP host classification is not available on the 12.0 XE release train)
Napster	TCP	Napster traffic	napster	12.1(5)T
Netshow	TCP/ UDP	Microsoft Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T
r-commands	TCP	rsh, rlogin, rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T
RealAudio	TCP/ UDP	RealAudio Streaming Protocol	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
RTP	TCP/ UDP	Real-Time Transport Protocol Payload Classification	rtp	12.2(8)T
SQL*NET	TCP/ UDP	SQL*NET for Oracle	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T

Table 5 TCP and UDP Stateful Protocols (continued)

Protocol	Type	Description	Syntax	Cisco IOS Release[1]
StreamWorks	UDP	Xing Technology Stream Works audio and video	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T
SunRPC	TCP/ UDP	Sun Remote Procedure Call	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T
TFTP	UDP	Trivial File Transfer Protocol	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T
VDOLive	TCP/ UDP	VDOLive Streaming Video	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T

1. Indicates the Cisco IOS maintenance release that first supported the protocol. This table is updated when a protocol is added to a new Cisco IOS release train.

Restrictions

The NBAR feature does not support the following:

- NBAR is currently not supported with Stateful Switchover (SSO). This applies to the Catalyst 6500, Cisco 7600 and Cisco 7500.
- More than 24 concurrent URLs, hosts, or MIME type matches
- Matching beyond the first 400 bytes in a packet payload
- Non-IP traffic
- Multicast and other non-CEF switching modes
- Fragmented packets
- Pipelined persistent HTTP requests
- URL/host/MIME classification with secure HTTP
- Asymmetric flows with stateful protocols
- Packets originating from or destined to the router running NBAR

NBAR is not supported on the following logical interfaces:

- Fast EtherChannel
- Interfaces where tunneling or encryption is used
- NBAR was not supported on Dialer interfaces until Cisco IOS Release 12.2(4)T

Note NBAR cannot be used to classify output traffic on a WAN link where tunneling or encryption is used. Therefore, NBAR should be configured on other interfaces on the router (such as a LAN link) to perform input classification before the traffic is switched to the WAN link for output.

Memory Management

NBAR uses approximately 150 bytes of DRAM for each flow that requires stateful inspection. (See Table 5 for a list of stateful protocols supported by NBAR that require stateful inspection.) When NBAR is configured, it allocates 1 MB of DRAM to support up to 5000 concurrent flows. NBAR checks to see if it needs more memory to handle additional concurrent stateful flows. If such a need is detected, NBAR expands its memory usage in increments of 200 Kb to 400 Kb.

Related Features and Technologies

- Access control lists (ACLs)
- Traffic Policing
- Traffic Shaping
- Class-Based Weighted Fair Queueing (CBWFQ)
- Class-Based Marking
- Low Latency Queueing
- Modular Quality of Service Command-Line Interface (Modular QoS CLI)

Related Documents

- *NBAR animation*
- *Quality of Service (QoS) Networking*
- *Quality of Service Solutions Configuration Guide*
- *Quality of Service Solutions Command Reference*
- *Access Control Lists: Overview and Guidelines*

Supported Platforms

The following table lists the platforms that support NBAR and the Cisco IOS releases where support for the platform was introduced:

Table 6 Platform and Initial Cisco IOS Release Support

Platform	Initial Cisco IOS Release Support
Cisco 1700	Cisco IOS Release 12.2(2)T
Cisco 2600	Cisco IOS Release 12.1(5)T
Cisco 3600	Cisco IOS Release 12.1(5)T
Cisco 3700	Cisco IOS Release 12.2(8)T
Cisco 7100	Cisco IOS Release 12.0(5)XE2 Cisco IOS Release 12.1(5)T
Cisco 7100 UBR	Cisco IOS Release 12.1(10)EC
Cisco 7200	Cisco IOS Release 12.0(5)XE2 Cisco IOS Release 12.1(5)T
Cisco 7200 UBR	Cisco IOS Release 12.1(10)EC
Cisco 7500 with VIP	Cisco IOS Release 12.1(6)E Cisco IOS Release 12.2(4)T3
Catalyst 6000 family switch with a FlexWAN module	Cisco IOS Release 12.1(6)E

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Supported Standards, MIBs, and RFCs

Standards

- 0009, *File Transfer Protocol (FTP)*
- 0013, *Domain Names - Concepts and Facilities*
- 0033, *The TFTP Protocol (Revision 2)*
- 0034, *Routing Information Protocol*
- 0053, *Post Office Protocol - Version 3*
- 0056, *RIP Version 2*

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS Release, and to download MIB modules, go to the Cisco MIB web site on cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

- RFC 742, *NAME/FINGER Protocol*
- RFC 759, *Internet Message Protocol*
- RFC 792, *Internet Control Message Protocol*
- RFC 793, *Transmission Control Protocol*
- RFC 821, *Simple Mail Transfer Protocol*
- RFC 827, *Exterior Gateway Protocol*
- RFC 854, *Telnet Protocol Specification*
- RFC 888, *"STUB" Exterior Gateway Protocol*
- RFC 904, *Exterior Gateway Protocol formal specification.*

- RFC 951, *Bootstrap Protocol*
- RFC 959, *File Transfer Protocol*
- RFC 977, *Network News Transfer Protocol*
- RFC 1001, *Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods*
- RFC 1002, *Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications*
- RFC 1057, *RPC: Remote Procedure Call*
- RFC 1094, *NFS: Network File System Protocol Specification*
- RFC 1112, *Host Extensions for IP multicasting*
- RFC 1157, *Simple Network Management Protocol*
- RFC 1282, *BSD Rlogin*
- RFC 1288, *The Finger User Information Protocol*
- RFC 1305, *Network Time Protocol*
- RFC 1350, *The TFTP Protocol (Revision 2)*
- RFC 1436, *The Internet Gopher Protocol*
- RFC 1459, *Internet Relay Chat Protocol*
- RFC 1510, *The Kerberos Network Authentication Service*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 1579, *Firewall-Friendly FTP*
- RFC 1583, *OSPF Version 2*
- RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol*
- RFC 1701, *Generic Routing Encapsulation*
- RFC 1730, *Internet Message Access Protocol - Version 4*
- RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 1777, *Lightweight Directory Access Protocol*
- RFC 1831, *RPC: Remote Procedure Call Protocol Specification Version 2*
- RFC 1889, *A Transport Protocol for Real-Time Applications*
- RFC 1890, *RTP Profile for Audio and Video Conferences with Minimal Control*
- RFC 1928, *SOCKS Protocol Version 5*
- RFC 1939, *Post Office Protocol - Version 3*
- RFC 1945, *Hypertext Transfer Protocol -- HTTP/1.0.*
- RFC 1964, *The Kerberos Version 5 GSS-API Mechanism*
- RFC 2060, *Internet Message Access Protocol - Version 4rev1*
- RFC 2068, *Hypertext Transfer Protocol -- HTTP/1.1*
- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2205, *Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification*
- RFC 2236, *Internet Group Management Protocol, Version 2*

- RFC 2251, *Lightweight Directory Access Protocol (v3)*
- RFC 2252, *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*
- RFC 2253, *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*
- RFC 2326, *Real Time Streaming Protocol (RTSP)*
- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2406, *IP Encapsulating Security Payload*
- RFC 2453, *RIP Version 2*
- RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*

Standards

- 0009, *File Transfer Protocol (FTP)*
- 0013, *Domain Names - Concepts and Facilities*
- 0033, *The TFTP Protocol (Revision 2)*
- 0034, *Routing Information Protocol*
- 0053, *Post Office Protocol - Version 3*
- 0056, *RIP Version 2*

Prerequisites

CEF

You must enable Cisco Express Forwarding (CEF) before you configure NBAR. For more information on CEF, refer to the Cisco IOS Release 12.2 *Cisco IOS Switching Services Configuration Guide*.

Configuration Tasks

The NBAR feature has two components: one component monitors applications traversing a network, and the other that classifies traffic by protocol.

In order to monitor applications traversing a network, Protocol Discovery needs to be enabled.

The ability to classify traffic by protocol using NBAR and then applying QoS to the classified traffic is configured using the Modular QoS CLI.

The Modular QoS CLI is a CLI structure that allows users to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

Modular QoS CLI configuration includes the following three steps:

Step 1 Define a traffic class with the **class-map** command.

Step 2 Create a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).

Step 3 Attach the traffic policy to the interface with the **service-policy** command.

NBAR traffic classification occurs as part of the traffic class configuration.

For additional information on the Modular Quality of Service Command-Line Interface, see the "Configuring the Modular Quality of Service Command-Line Interface" section of the *Cisco IOS Quality of Service Solution Guide* on Cisco.com.

See the following sections for configuration tasks for the NBAR feature. Each task in the list is identified as either optional or required:

- Enabling Protocol Discovery(optional)
- Configuring a Traffic Class (required)
- Configuring a Traffic Policy (required)
- Attaching a Traffic Policy to an Interface (required)

Enabling Protocol Discovery

Use the **ip nbar protocol-discovery** command in order to enable monitoring of applications on a particular interface:

Command	Purpose
`Router(config)# interface interface-name`	Specifies the interface to configure.
`Router(config-if)# ip nbar protocol-discovery`	Enables monitoring by application on a particular interface.

Configuring a Traffic Class

Use the **class-map** configuration command to define a traffic class and the match criteria that will be used to classify network traffic when attached to an interface. When using NBAR to classify traffic, the **match protocol** command will be entered in class map configuration mode.

Command	Purpose
`Router(config)# class-map [match-all | match-any] class-name`	Specifies the user-defined name of the traffic class. The **match-all** option specifies that all match criteria in the class map must be matched. The **match-any** option specifies that one or more match criteria must match.
`Router(config-cmap)# match protocol protocol-name`	Specifies a protocol supported by NBAR as a matching criterion.

Configuring a Traffic Policy

Use the **policy-map** configuration command to specify the QoS policies, such as Traffic Policing, Traffic Shaping, Low Latency Queueing, Class-Based Marking, Class-Based Weighted Fair Queueing or others, to apply to traffic classes defined by a traffic class. A traffic policy does not classify and forward traffic until being attached to an interface.

Command	Purpose
`Router(config)# policy-map policy-name`	User-specified policy map name.
`Router(config-pmap)# class class-name`	Specifies the name of a previously defined class map.
`Router(config-pmap-c)#`	Enter QoS policies in this configuration mode (policy map class).

For additional information on policy map options in the Modular Quality of Service Command-Line Interface, see the *Modular Quality of Service Command-Line Interface* document on Cisco.com.

Attaching a Traffic Policy to an Interface

A traffic policy is not active until it has been attached to an interface. Use the **service-policy** interface configuration command to attach a traffic policy to an interface and to specify the direction in which the policy should be applied (on either packets coming into the interface or packets leaving the interface).

.

Command	Purpose
`Router(config)# interface interface-name`	Specifies the interface to configure.
`Router(config-if)# service-policy output policy-map-name`	Attaches the previously configured traffic policy in the outbound direction of the interface. When this command is entered, all traffic leaving the interface will be classified and forwarded based on the traffic policy configuration.
`Router(config-if)# service-policy input policy-map-name`	Attaches the previously configured traffic policy in the input direction of the interface. When this command is entered, all traffic entering the interface will be classified and forwarded based on the traffic policy configuration.

Use the **no service-policy** [**input** | **output**] *policy-map-name* command to detach a policy map from an interface.

Downloading PDLMs

To extend or enhance the list of protocols recognized by NBAR through a Cisco-provided PDLM, use the **ip nbar pdlm** command after downloading the PDLM:

`Router(config)# ip nbar pdlm pdlm-name`	Specifies the PDLM used to extend or enhance the NBAR list of protocols.

Note To view a list of currently available PDLMs or to download a PDLM, go to the following URL:
http://www.cisco.com/cgi-bin/tablebuild.pl/pdlm

Verifying the Configuration

Use the **show policy-map** [**interface** [*interface-spec* [*input* | *output* [**class** *class-name*]]]] command to display the configuration of a policy map and its associated class maps. Forms of this command are listed in the table below.

Command	Purpose
`Router# show class-map`	Displays all traffic class information.
`Router# show class-map class-name`	Displays the traffic class information of the user-specified traffic class.
`Router# show policy-map`	Displays all configured traffic policies.
`Router# show policy-map policy-map-name`	Displays the user-specified traffic policies.
`Router# show policy-map interface`	Displays statistics and configurations of all input and output policies, which are attached to an interface.
`Router# show policy-map interface-spec`	Displays configuration and statistics of the input and output policies attached to a particular interface.
`Router# show policy-map interface-spec [input]`	Displays configuration and statistics of the input policy attached to an interface.
`Router# show policy-map interface-spec [output]`	Displays configuration statistics of the output policy attached to an interface.
`Router# show policy-map interface-spec [input | output] class class-name`	Displays the configuration and statistics for the class name configured in the policy.

Troubleshooting Tips

- You must enable Cisco Express Forwarding (CEF) on the router prior to configuring the NBAR feature.
- Some error messages use the term “heuristic” to refer to a set of NBAR-supported protocols, and some error message documentation recommends actions to these heuristic protocols.

  RTP is the only currently available heuristic protocol. If the error message or the error message documentation recommends an action to a heuristic protocol, take the recommended action on RTP.

Monitoring and Maintaining NBAR

NBAR can determine which protocols and applications are currently running on a network. NBAR includes the Protocol Discovery feature that provides an easy way of discovering application protocols operating on an interface so that appropriate QoS policies can be developed and applied. With Protocol Discovery, you can discover any protocol traffic supported by NBAR and obtain statistics associated with that protocol. To monitor and maintain the NBAR feature, use the following commands:

Command	Purpose
`Router# show ip nbar port-map [protocol-name]`	Displays the TCP/UDP port numbers used by NBAR to classify a given protocol.
`Router# show ip nbar protocol-discovery`	Displays the statistics for all interfaces on which Protocol Discovery is enabled.

Configuration Examples

This section provides the following configuration examples:

- Configuring a Traffic Policy with NBAR
- Adding a PDLM

Configuring a Traffic Policy with NBAR

In the following example, all SQL*Net traffic leaving fastethernet interface 0/1 is marked with the IP precedence value of 4. In the example, NBAR is used to identify SQL*Net traffic, while the treatment of SQL*Net traffic (in this case, it is forwarded with the IP precedence bit set as 4) is determined by the traffic policy configuration (the **set ip precedence 4** command in policy-map class configuration mode).

```
Router(config)# class-map sqlnettraffic
Router(config-cmap)# match protocol sqlnet

Router(config)# policy-map sqlsetipprec1
Router(config-pmap)# class sqlnettraffic
Router(config-pmap-c)# set ip precedence 4

Router(config)# interface fastethernet 0/1
Router(config-if)# service-policy output sqlsetipprec1
```

Adding a PDLM

In the following example, the FastTrack PDLM, which has already been downloaded to the Flash drive, is added as an NBAR-supported protocol:

```
Router(config)# ip nbar pdlm flash://fasttrack.pdlm
```

Command Reference

This section documents new and enhanced commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **ip nbar pdlm**
- **ip nbar port-map**
- **ip nbar protocol-discovery**
- **match protocol**
- **match protocol citrix**
- **match protocol fasttrack**
- **match protocol gnutella**
- **match protocol http**
- **match protocol rtp**
- **show ip nbar pdlm**
- **show ip nbar port-map**
- **show ip nbar protocol-discovery**

Note In this section, **match protocol citrix**, **match protocol fasttrack**, **match protocol gnutella**, **match protocol http**, and **match protocol rtp** are included while other **match protocol** *protocol-name* commands are not because these commands require additional information than the other **match protocol** *protocol-name* commands for NBAR.

ip nbar pdlm

To extend or enhance the list of protocols recognized by NBAR through a Cisco-provided Packet Description Language Module (PDLM), use the **ip nbar pdlm** configuration command. Use the **no** form of this command to unload a PDLM if it was previously loaded.

ip nbar pdlm *pdlm-name*

no ip nbar pdlm *pdlm-name*

Syntax Description

pdlm-name	The URL where the PDLM can be found in Flash memory.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

This command is used in global configuration mode to extend the list of protocols recognized by a given version of NBAR or to enhance an existing protocol-recognition capability. NBAR can be given an external PDLM at run time. In most cases, the PDLM enables NBAR to recognize new protocols without requiring a new IOS image or a router reload. Only Cisco can provide you with a new PDLM.

To view a list of currently available PDLMs or to download a PDLM, go to the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/pdlm

Examples

The following example configures NBAR to load the citrix.pdlm PDLM from Flash memory on the router:

```
ip nbar pdlm flash://citrix.pdlm
```

Related Commands

Command	Description
show ip nbar pdlm *pdlm-name*	Displays the current PDLM in use by NBAR.

ip nbar port-map

To configure NBAR to search for a protocol or protocol name using a port number other than the well-known port, use the **ip nbar port-map** global configuration command. Use the **no** form of this command to look for the protocol name using only the well-known port number.

ip nbar port-map *protocol-name* [**tcp** | **udp**] *port-number*

no ip nbar port-map *protocol-name* [**tcp** | **udp**] *port-number*

Syntax Description

protocol-name	Name of protocol known to NBAR.
tcp	Specifies that a TCP port will be searched for the specified *protocol-name*.
udp	Specifies that a UDP port will be searched for the specified *protocol-name*.
port-number	Assigned port for named protocol. The *port-number* is either a UDP or a TCP port number, depending on which protocol is specified in this command line. Up to 16 *port-numbers* can be specified in one command line.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

This command is used in global configuration mode to tell NBAR to look for the protocol *protocol-name*, using a port number or numbers other than the well-known (IANA-assigned) port number. For example, use this command to configure NBAR to look for Telnet on a port other than 23. From 1 to 16 ports can be specified with this command. Port number values can range from 0 to 65535.

Examples

The following example configures NBAR to look for the protocol SQL*NET on port numbers 63000 and 63001 instead of on the well-known port number:

```
ip nbar port-map sqlnet tcp 63000 63001
```

Command History

Command	Description
show ip nbar port-map *protocol-name*	Displays the current protocol-to-port mappings in use by NBAR.

ip nbar protocol-discovery

To configure NBAR to discover traffic for all protocols known to NBAR on a particular interface, use the **ip nbar protocol-discovery** interface configuration command. Use the **no** form of this command to disable traffic discovery.

ip nbar protocol-discovery

no ip nbar protocol-discovery

Syntax Description

None

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

Use the **ip nbar protocol-discovery** command to configure NBAR to keep traffic statistics for all protocols known to NBAR. Protocol Discovery provides an easy way to discover application protocols traversing an interface so that QoS policies can be developed and applied. The Protocol Discovery feature discovers any protocol traffic supported by NBAR. Protocol Discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled.

Examples

The following example configures Protocol Discovery on an Ethernet interface:

```
interface ethernet 1/3
ip nbar protocol-discovery
```

Related Commands

Command	Description
show ip nbar protocol-discovery	Displays the statistics gathered by the NBAR Protocol Discovery feature.

match protocol

To match traffic by a particular protocol, use the **match protocol** class map configuration mode command. Use the **no** form of this command to turn off traffic matching by protocol type.

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

protocol-name	Identifies a particular protocol as a matching criterion.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

This command can be used to match protocols that are known to NBAR. See the tables in the "Supported Protocols" section on page 12 for a list of protocols currently supported by NBAR.

Examples

The following example configures NBAR to match FTP traffic:

```
match protocol ftp
```

match protocol citrix

To configure NBAR to match Citrix traffic, use the **match protocol citrix** class map configuration command. Use the **no** form of this command to disable NBAR from matching Citrix traffic.

match protocol citrix [**app** *application-name-string*]

no match protocol citrix [**app** *application-name-string*]

Syntax Description

app	Specifies matching of an application name string.
application-name-string	Specifies string to be used as the subprotocol parameter.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

Entering the **match protocol citrix** command without any other keywords establishes all Citrix traffic as successful match criteria.

Examples

The following example configures NBAR to match all Citrix traffic:

```
match protocol citrix
```

The following example configures NBAR to match Citrix traffic with the application name of packet1:

```
match protocol citrix app packet1
```

match protocol fasttrack

To configure NBAR to match FastTrack peer-to-peer traffic, use the **match protocol fasttrack** class map configuration command. Use the **no** form of this command to disable NBAR from matching FastTrack traffic.

match protocol fasttrack file-transfer "*regular-expression***"**

no match protocol fasttrack file-transfer "*regular-expression*"

Syntax Description

regular-expression	A regular expression is used to identify specific FastTrack traffic. For instance, entering "cisco" as the regular expression would classify the FastTrack traffic containing the string "cisco" as matches for the traffic policy. To specify that all FastTrack traffic be identified by the traffic class, use * as the regular expression.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

To specify that all FastTrack traffic be identified by the traffic class, use "*" as the regular expression.

Applications that use FastTrack include KaZaA, Grokster, and Morpheus (although newer versions of Morpheus use Gnutella).

Examples

The following example configures NBAR to match all FastTrack traffic:

```
match protocol fasttrack file-transfer "*"
```

In the following example, all FastTrack files that have the ".mpeg" extension will be classified into class map nbar.

```
class-map match-all nbar
match protocol fasttrack file-transfer "*.mpeg"
```

The following example configures NBAR to match FastTrack traffic that contains the string "cisco":

```
match protocol fasttrack file-transfer "*cisco*"
```

match protocol gnutella

To configure NBAR to match Gnutella peer-to-peer traffic, use the **match protocol gnutella** class map configuration command. Use the **no** form of this command to disable NBAR from matching Gnutella traffic.

match protocol gnutella file-transfer "*regular-expression***"**

no match protocol gnutella file-transfer "*regular-expression*"

Syntax Description

regular-expression	A regular expression is used to identify specific Gnutella traffic. For instance, entering "cisco" as the regular expression would classify the Gnutella traffic containing the string "cisco" as matches for the traffic policy. To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression.

Applications that use Gnutella include:

- BearShare
- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- JTella
- LimeWire
- Morpheus
- Mutella
- Phex
- Qtella

- Swapper
- XoloX
- XCache

Examples

The following example configures NBAR to match all Gnutella traffic:

```
match protocol gnutella file-transfer "*"
```

In the following example, all gnutella files that have the ".mpeg" extension will be classified into class map nbar.

```
class-map match-all nbar
match protocol gnutella file-transfer "*.mpeg"
```

In the following example, only gnutella traffic that contains the characters "cisco" is classified:

```
class-map match-all nbar
match protocol gnutella file-transfer "*cisco*"
```

match protocol http

To configure NBAR to match HTTP traffic by URL, host, or MIME type, use the **match protocol http** class map configuration command. Use the **no** form of this command to disable NBAR from matching HTTP traffic by URL, host, or MIME type.

match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type*]

no match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type*]

Syntax Description

url	Specifies matching by a URL.
url-string	User-specified URL of HTTP traffic to be matched.
host	Specifies matching by a host name.
hostname-string	User-specified Host name to be matched.
mime	Specifies matching by MIME text string.
MIME-type	User-specified MIME text string to be matched.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(2)E	This command was enhanced to include the *hostname-string* variable.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

When matching by MIME type, the MIME type can contain any user-specified text string. Refer to the following web page for the IANA-registered MIME types:

ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/media-types

When matching by MIME type, NBAR matches a packet containing the MIME type and all subsequent packets until the next HTTP transaction.

When matching by host, NBAR performs a regular expression match on the host field contents inside the HTTP packet and classifies all packets from that host.

HTTP URL matching supports GET, PUT, HEAD, POST, DELETE, and TRACE. When matching by URL, NBAR recognizes the HTTP packets containing the URL, and then matches all packets that are part of the HTTP request. When specifying a URL for classification, include only the portion of the URL following www.hostname.domain in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html include only /latest/whatsnew.html.

To match the www.anydomain.com portion, use the host name matching feature. The URL or host specification strings can take the form of a regular expression with the following options:

Option	Description
*	Match any zero or more characters in this position.
?	Match any one character in this position.
|	Match one of a choice of characters.
(|)	Match one of a choice of characters in a range. For example foo.(gif | jpg) matches either foo.gif or foo.jpg.
[ ]	Match any character in the range specified, or one of the special characters. For example, [0-9] is all of the digits. [*] is the "*" character and [[] is the "[" character.

Examples

The following example classifies, within class map foo, HTTP packets based on any URL containing the string whatsnew/latest followed by zero or more characters:

```
class-map foo
match protocol http url whatsnew/latest*
```

The following example classifies, within class map foo, packets based on any host name containing the string cisco followed by zero or more characters:

```
class-map foo
match protocol http host cisco*
```

The following example classifies, within class map foo, packets based on the JPEG MIME type:

```
class-map foo
match protocol http mime "*jpeg"
```

match protocol rtp

To configure NBAR to match RTP traffic, use the **match protocol rtp** class map configuration command. Use the **no** form of the command to disable NBAR from matching RTP traffic.

match protocol rtp [**audio | video | payload-type** *payload-string*]

no match protocol rtp [**audio | video | payload-type** *payload-string*]

Syntax Description

audio	Specifies matching by payload-type values 0-23. These payload-type values are reserved for audio traffic.
video	Specifies matching by payload-type values 24-33. These payload-type values are reserved for video traffic.
payload-type	Specifies matching by a specific payload-type value, providing more granularity than the **audio** or **video** options.
payload-string	A user-specified string containing the specific payload-type values. A *payload-string* can contain commas to separate payload-type values and hyphens to indicate a range of payload-type values. A *payload-string* can be specified in hexadecimal (prepend 0x to the value) and binary (prepend b to the value) notations in addition to standard number values.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was introduced on the Cisco IOS Release 12.1 E train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

Entering the **match protocol rtp** command without any other keywords establishes all RTP traffic as successful match criteria.

RTP is a packet format for multimedia data streams. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part. The control part is called Real-time Transport Control Protocol (RTCP). It is important to note that the NBAR RTP Payload Classification feature does not identify RTCP packets, and that RTCP packets run on odd port numbered ports while RTP packets run on even numbered port.

The payload type field of an RTP packet identifies the format of the RTP payload and is represented by a number. NBAR matches RTP traffic based on this field in the RTP packet, so a working knowledge of RTP and RTP payload types is helpful if you want to configure NBAR to match RTP traffic. The RTP Request for Comments is RFC 1889.

Examples

The following example configures NBAR to match all RTP traffic:

```
class-map foo
match protocol rtp
```

The following example configures NBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 64:

```
class-map foo
match protocol rtp payload-type “0, 1, 4-0x10, 10001b-10010b, 64”
```

show ip nbar pdlm

To display the currently loaded Packet Description Language Modules (PDLMs), use the **show ip nbar pdlm** EXEC command.

show ip nbar pdlm

Syntax Description

None

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

This command is used to display a list of all the PDLMs that have been loaded into NBAR using the **ip nbar pdlm** command.

Examples

In this example of the **show ip nbar pdlm** command, the citrix.pdlm PDLM has been loaded from Flash memory:

```
show ip nbar pdlm
The following PDLMs have been loaded:
flash://citrix.pdlm
```

Related Commands

Command	Description
ip nbar pdlm	Extends or enhances the list of protocols recognized by NBAR through a PDLM.

show ip nbar port-map

To display the current protocol-to-port mappings in use by NBAR, use the **show ip nbar port-map** EXEC command.

show ip nbar port-map [*protocol-name*]

Syntax Description

protocol-name	Limits the command display to the specified protocol.

Defaults

This command displays port assignments for NBAR protocols.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

This command is used to display the current protocol-to-port mappings in use by NBAR. When the **ip nbar port-map** command has been used, the **show ip nbar port-map** command displays the ports assigned by the user to the protocol. If the **no ip nbar port-map** command has been used, the **show ip nbar port-map** command displays the default ports. The *protocol-name* variable can also be used to limit the display to a specific protocol.

Examples

The following example displays the **show ip nbar port-map** command:

```
show ip nbar-port-map
port-map bgp      udp 179
port-map bgp      tcp 179
port-map cuseeme  udp 7648 7649
port-map cuseeme  tcp 7648 7649
port-map dhcp     udp 67 68
port-map dhcp     tcp 67 68
port-map dns      udp 53
port-map dns      tcp 53
```

Related Commands

Command	Description
ip nbar port-map	Configures NBAR to search for a protocol or protocol name using a port number other than the well-known port.

show ip nbar protocol-discovery

To display the statistics gathered by the NBAR Protocol Discovery feature, use the **show ip nbar protocol-discovery** privileged EXEC command.

show ip nbar protocol-discovery [**interface** *interface-spec*] [**stats** {**byte-count** | **bit-rate** | **packet-count**}][{**protocol** *protocol-name* | **top-n** *number*}]

Syntax Description

interface	Specifies that Protocol Discovery statistics for the interface are to be displayed.
interface-spec	Specifies an interface to display.
stats	Specifies that the byte count, byte rate, or packet count is to be displayed.
byte-count	Specifies that the byte count is to be displayed.
bit-rate	Specifies that the bit rate is to be displayed.
packet-count	Specifies that the packet count is to be displayed.
protocol	Specifies that statistics for a specific protocol are to be displayed.
protocol-name	User-specified protocol name for which the statistics are to be displayed.
top-n	Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols will be displayed.
number	Specifies the number of most active NBAR-supported protocols to be displayed.

Defaults

Statistics for all interfaces on which the Protocol Discovery feature is enabled are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was introduced for the Cisco IOS Release 12.1 E train.
12.1(5)T	This command was introduced for the Cisco IOS Release 12.1 T train.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was introduced for the Cisco IOS Release 12.2 S train.

Usage Guidelines

Use the **show ip nbar protocol-discovery** command to display statistics gathered by the Protocol Discovery feature for NBAR. This command, by default, displays statistics for all interfaces on which Protocol Discovery is currently enabled. The default output of this command includes, in the following order, input bit rate (bps), input byte count, input packet count, and protocol name.

Protocol Discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled. Protocol Discovery gathers statistics for packets switched to output interfaces. These statistics are not necessarily for packets that exited the router on the output interfaces, because packets may have been dropped after switching for various reasons, including policing at the output interface, access lists, or queue drops.

Examples

The following example displays partial output of the **show ip nbar protocol-discovery** command for an Ethernet interface:

```
show ip nbar protocol-discovery interface FastEthernet 6/0

 FastEthernet6/0
                              Input                     Output
   Protocol                   Packet Count              Packet Count
                              Byte Count                Byte Count
                              5 minute bit rate (bps)   5 minute bit rate (bps)
   ------------------------   ------------------------  ------------------------
   igrp                       316773                    0
                              26340105                  0
                              3000                      0
   streamwork                 4437                      7367
                              2301891                   339213
                              3000                      0
   rsvp                       279538                    14644
                              319106191                 673624
                              0                         0
   ntp                        8979                      7714
                              906550                    694260
                              0                         0
.
.
.
Total                      17203819                  151684936
                              19161397327               50967034611
                              4179000                   6620000
```

Related Commands

Command	Description
ip nbar protocol-discovery	Discovers traffic for all protocols known to NBAR.

Glossary

Modular QoS CLI—Modular Quality of Service Command-Line Interface. A CLI for QoS features that makes configuring and implementing packet classification and QoS policies easier than with the existing CLI.

PDLM—Packet Description Language Module. A file containing Packet Description Language statements used to define the signature of one or more application protocols.

Stateful protocol—A protocol that uses TCP and UDP port numbers that are determined at connection time.

Static protocol—A protocol that uses well-defined (predetermined) TCP and UDP ports for communication.

Subport classification—The classification of network traffic by information contained in the packet payload; that is, information found beyond the TCP or UDP port number.

Appendix

Sample Configuration

Below is a sample of how NBAR can be used.

E-Express Inc.'s network administrators wish to enforce the following policies on a 64-Kb WAN link:

- Reserve a minimum bandwidth of 32 Kb out of the 64 Kb available on the WAN link for all e-commerce traffic. This e-commerce traffic will be secure HTTP traffic or files being served from the http://www.eexpress.com/transact/ directory through regular HTTP on the E-Express Inc. network.
- SuperNetwork Inc. is a very important partner to E-Express Inc. Reserve a minimum of 10 Kb for all traffic flowing from E-Express Inc. to SuperNetwork Inc.
- Limit to a maximum of 10 Kb all audio, video, and image web traffic.

Follow the steps below to configure the above policies:

Step 1 Classify all secure HTTP and HTTP traffic for the /transact/ directory:

```
Router(config)# class-map match-all http_transact
Router(config-cmap)# match protocol http url "/transact/*"

Router(config)# class-map match-all http_secure
Router(config-cmap)# match protocol secure-http

Router(config)# class-map match-any ecommerce
Router(config-cmap)# match class-map http_transact
Router(config-cmap)# match class-map http_secure
```

Step 2 Classify all traffic to SuperNetwork Inc:

```
Router(config)# access-list 101 permit ip 10.0.0.1 0.0.0.0 10.0.0.3 0.0.0.0

Router(config)# class-map match-all super_network
Router(config-cmap)# match access-group 101
```

Step 3 Classify all audio, video, and image web traffic:

```
Router(config)# class-map match-any audio_video
Router(config-cmap)# match protocol http mime "audio/*"
Router(config-cmap)# match protocol http mime "video/*"

Router(config)# class-map match-any web_images
Router(config-cmap)# match protocol http url "*.gif"
Router(config-cmap)# match protocol http url "*.jpg|*.jpeg"

Router(config)# class-map match-any av_im_web
Router(config-cmap)# match class-map audio_video
Router(config-cmap)# match class-map web_images
```

Step 4 Create the policies:

```
Router(config)# policy-map e-express
Router(config-pmap)# class ecommerce
Router(config-pmap-c)# bandwidth 32
Router(config-pmap-c)# class super_network
Router(config-pmap-c)# bandwidth 10
Router(config-pmap-c)# class av_im_web
Router(config-pmap-c)# police 10000 conform transmit exceed drop
```

Step 5 Attach the policy to the WAN link:

```
Router(config)# interface hssi1/0
Router(config-if)# service-policy output e-express
```