



QoS: NBAR Configuration Guide, Cisco IOS Release 15S

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Classifying Network Traffic Using NBAR 1

Finding Feature Information 1

Prerequisites for Using NBAR 2

Restrictions for Using NBAR 2

 Layer 2 NBAR Restrictions 3

Information About Classifying Network Traffic Using NBAR 4

 NBAR Functionality 4

 NBAR Benefits 6

 NBAR and Classification of HTTP Traffic 6

 Classification of HTTP Traffic by URL Host or MIME 6

 Classification of HTTP Traffic Using HTTP Header Fields 7

 Combinations of Classification of HTTP Headers and URL Host or MIME Type to Identify HTTP Traffic 8

 NBAR and Classification of Citrix ICA Traffic 8

 Classification of Citrix ICA Traffic by Published Application Name 8

 Classification of Citrix ICA Traffic by ICA Tag Number 9

 NBAR and RTP Payload Type Classification 10

 NBAR and Classification of Custom Protocols and Applications 10

 NBAR and Classification of Peer-to-Peer File-Sharing Applications 11

 NBAR and Classification of Streaming Protocols 11

 NBAR and AutoQoS 11

 NBAR and FWSM Integration 12

 NBAR and TelePresence PDLM 12

 NBAR-Supported Protocols 13

 NBAR Memory Management 13

 NBAR Protocol Discovery 13

 Nonintrusive Protocol Discovery 13

 NBAR Protocol Discovery MIB 14

NBAR Configuration Processes	14
NBAR Categorization and Attributes	15
Where to Go Next	16
Additional References	16
Feature Information for Classifying Network Traffic Using NBAR	16
Glossary	19

CHAPTER 2

Enabling Protocol Discovery	21
Finding Feature Information	21
Prerequisites for Enabling Protocol Discovery	21
Information About Protocol Discovery	22
Protocol Discovery Functionality	22
How to Configure Protocol Discovery	22
Enabling Protocol Discovery on an Interface	22
Reporting Protocol Discovery Statistics	23
Configuration Examples for Enabling Protocol Discovery	24
Example Enabling Protocol Discovery on an Interface	24
Example Reporting Protocol Discovery Statistics	25
Where to Go Next	25
Additional References	25
Feature Information for Enabling Protocol Discovery	26

CHAPTER 3

Configuring NBAR Using the MQC	29
Finding Feature Information	29
Prerequisites for Configuring NBAR Using the MQC	29
Information About Configuring NBAR Using the MQC	30
NBAR and the MQC Functionality	30
NBAR and the match protocol Commands	31
How to Configure NBAR Using the MQC	31
Configuring a Traffic Class	31
Configuring a Traffic Policy	33
Attaching a Traffic Policy to an Interface or Subinterface	35
Verifying NBAR Using the MCQ	37
Configuration Examples for Configuring NBAR Using the MQC	38
Example Configuring a Traffic Class	38

Example Configuring a Traffic Policy 38

Example Attaching a Traffic Policy to an Interface or Subinterface 39

Example Verifying the NBAR Protocol-to-Port Mappings 39

Where to Go Next 39

Additional References 40

Feature Information for Configuring NBAR Using the MQC 41



CHAPTER

1

Classifying Network Traffic Using NBAR

Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol.

This module contains overview information about classifying network traffic in NBAR. The processes for configuring NBAR are documented in separate modules.



Note

This module includes information for both NBAR and Distributed Network-Based Application Recognition (dNBAR). dNBAR is NBAR used on the Cisco 7500 router with a Versatile Interface Processor (VIP) and on the Catalyst 6500 family of switches with a FlexWAN module or serial interface processor (SIP). The implementation of NBAR and dNBAR is identical. Therefore, unless otherwise noted, the term NBAR is used throughout this module to describe both NBAR and dNBAR. The term dNBAR is used only when applicable.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Using NBAR, page 2](#)
- [Restrictions for Using NBAR, page 2](#)
- [Information About Classifying Network Traffic Using NBAR, page 4](#)
- [Where to Go Next, page 16](#)
- [Additional References, page 16](#)
- [Feature Information for Classifying Network Traffic Using NBAR, page 16](#)
- [Glossary, page 19](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Prerequisites for Using NBAR

Cisco Express Forwarding

Before you configure NBAR, you must enable Cisco Express Forwarding.



Note

This prerequisite does not apply if you are using Cisco IOS Release 12.2(18)ZYA.

Stateful Switchover Support

NBAR is not supported with stateful switchover (SSO). This restriction applies to the Catalyst 6500 switches and to the Cisco 7500 and Cisco 7600 series routers.

Memory Requirements for dNBAR

To use dNBAR on a Cisco 7500 series router, you must be using a slot controller (or VIP processor) that has at least 64 MB of DRAM. Therefore, before configuring dNBAR on your Cisco 7500 series router, review the DRAM specifications for your particular slot controller or VIP processor.

Restrictions for Using NBAR

NBAR does not support the following:

- More than 24 concurrent URLs, hosts, or Multipurpose Internet Mail Extension (MIME) type matches.



Note

For Cisco IOS Release 12.2(18)ZYA and Cisco IOS Release 15.1(2)T, the maximum number of concurrent URLs, hosts, or MIME type matches is 56.

- Matching beyond the first 400 bytes in a packet payload in Cisco IOS releases before Cisco IOS Release 12.3(7)T. In Cisco IOS Release 12.3(7)T, this restriction was removed, and NBAR now supports full payload inspection. The only exception is that NBAR can inspect custom protocol traffic for only 255 bytes into the payload.
- Non-IP traffic.
- Multiprotocol Label Switching (MPLS)-labeled packets. NBAR classifies IP packets only. You can, however, use NBAR to classify IP traffic before the traffic is handed over to MPLS. Use the modular quality of service (QoS) CLI (MQC) to set the IP differentiated services code point (DSCP) field on the NBAR-classified packets and make MPLS map the DSCP setting to the MPLS experimental (EXP) setting inside the MPLS header.

- Multicast and other non-Cisco Express Forwarding switching modes.
- Fragmented packets.
- Pipelined persistent HTTP requests.
- URL/host/MIME classification with secure HTTP.
- Asymmetric flows with stateful protocols.
- Packets that originate from or that are destined to the router running NBAR.

NBAR is not supported on the following logical interfaces:

- Fast Etherchannels



Note Fast Etherchannels *are* supported in Cisco IOS Release 12.2(18)ZYA.

- Dialer interfaces until Cisco IOS Release 12.2(4)T
- Interfaces where tunneling or encryption is used



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



Note A Network Address Translation (NAT)-enabled Cisco device may experience an increase in CPU usage when upgrading the software from a previous release. Real Time Streaming Protocol (RTSP) and Media Gateway Control Protocol (MGCP) NAT Application Layer Gateway (ALG) support was added in Cisco IOS Release 12.3(7)T, which requires NBAR. Use the **no ip nat service nbar** command to disable NBAR processing, which can decrease the CPU utilization rate.



Warning If the **no ip nat service nbar** command is not specified during the startup of the router, results in the crashing of the router, when loading the configuration from the TFTP during the booting process.

Layer 2 NBAR Restrictions

The phrase "Layer 2 NBAR" refers to NBAR functionality used with Layer 2 interfaces (such as switchports, trunks, or Etherchannels).

Layer 2 NBAR functionality can be used with service modules such as a Firewall Service Module (FWSM) and an Intrusion Detection Service Module (IDS) with the following restriction: Layer 2 NBAR is not supported on Layer 2 interfaces that are configured as part of a service module (such as FWSM and IDS) when those service modules are configured in inline mode (that is, network traffic is in a direct path through the service module).

**Note**

This restriction does not apply to NBAR functionality that is used with Layer 3 interfaces.

However, Layer 2 NBAR is supported in noninline mode with service modules even when Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), or VLAN Access Control List (VACL) Capture functionality is used to send traffic to a service module.

For more information about the FWSM and its connection features, see the "[Configuring Advanced Connection Features](#)" module of the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

For more information about the IDSM, see the "[Configuring IDSM-2](#)" module of the *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*.

For more information about SPAN or RSPAN, see the "[Configuring SPAN and RSPAN](#)" module of the *Catalyst 6500 Series Software Configuration Guide*.

For more information about VACL Capture, see the "[VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running Cisco IOS Software](#)" module.

Information About Classifying Network Traffic Using NBAR

NBAR Functionality

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.

When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate QoS for that application or traffic with that protocol. The QoS is applied using the modular quality of service CLI (MQC).

**Note**

For more information about NBAR and its relationship with the MQC, see the "[Configuring NBAR Using the MQC](#)" module.

Examples of the QoS features that can be applied to the network traffic (using the MQC) after NBAR has recognized and classified the application or protocol include the following:

- Class-Based Marking
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)
- Traffic Policing
- Traffic Shaping



Note For Cisco IOS Release 12.2(18)ZYA on the Catalyst 6500 series switch (that is equipped with a Supervisor 32/programmable intelligent services accelerator [PISA]), only the following QoS features can be configured. These features can be configured (using the MQC) after NBAR has recognized and classified the application or protocol.

- Traffic Classification
- Traffic Marking
- Traffic Policing



Note For more information about the QoS features, see the "Quality of Service Overview" module. For more information about the Catalyst 6500 series switch and QoS, see the "[Configuring QoS](#)" module of the *Catalyst 6500 Series Software Configuration Guide*.

NBAR introduces several classification features that identify applications and protocols from Layer 4 through Layer 7. These classification features are as follows:

- Statically assigned TCP and UDP port numbers.
- Non-TCP and non-UDP IP protocols.
- Dynamically assigned TCP and UDP port numbers. This kind of classification requires stateful inspection; that is, the ability to inspect a protocol across multiple packets during packet classification.
- Subport classification or classification based on deep-packet inspection.

Deep-packet classification is classification performed at a finer level of granularity. For instance, if a packet is already classified as HTTP traffic, it may be further classified by HTTP traffic with a specific URL.



Note Access Control Lists (ACLs) can also be used for classifying static port protocols. However, NBAR is easier to configure and can provide classification statistics that are not available when ACLs are used.

NBAR includes a Protocol Discovery feature that provides an easy way to discover application protocols that are operating on an interface. For more information about Protocol Discovery, see the "Enabling Protocol Discovery" module.



Note NBAR classifies network traffic by application or protocol. Network traffic can be classified without using NBAR. For information about classifying network traffic without using NBAR, see the "Classifying Network Traffic" module.

NBAR Benefits

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 number and types of applications and protocols that are running on a network.

NBAR gives network administrators the ability to see the different types of protocols and the amount of traffic generated by each protocol. After NBAR gathers this information, users can organize traffic into classes. These classes can then be used to provide different levels of service for network traffic, thereby allowing better network management by providing the appropriate level of the network resources for network traffic.

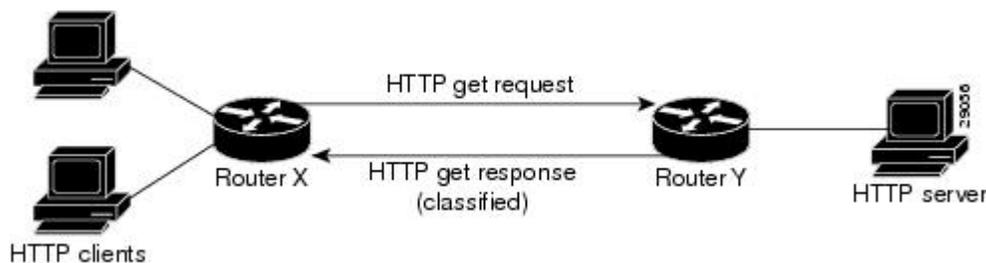
NBAR and Classification of HTTP Traffic

Classification of HTTP Traffic 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 based on content within the payload such as that transaction identifier, message type, or other similar data.

Classification of HTTP traffic 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 client request matching in NBAR supports most HTTP request methods such as GET, PUT, HEAD, POST, DELETE, OPTIONS, CONNECT, and TRACE. The NBAR engine then converts the specified match string into a regular expression.

The figure below illustrates a network topology with NBAR in which Router Y is the NBAR-enabled router.



When specifying a URL for classification, include only the portion of the URL that follows the *www.hostname.domain* in the **match** statement. For example, for the URL `www.cisco.com/latest/whatsnew.html`, include only `/latest/whatsnew.html` with the **match** statement (for instance, **match protocol http url /latest/whatsnew.html**).



Note

For Cisco IOS Release 12.2(18)ZY2 and later releases on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, and for Cisco IOS Release 15.1(2)T and later releases, up to 56 parameters or subclassifications per protocol per router can be specified with the **match protocol http** command. These parameters or subclassifications can be a combination of any of the available match choices, such as host matches, MIME matches, server matches, and URL matches. For other Cisco IOS releases and platforms, the maximum is 24 parameters or subclassifications per protocol per router.

Host specifications are identical to URL specifications. 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 the following URL:

<http://www.iana.org/assignments/media-types/>

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

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.

In Cisco IOS Release 12.3(4)T, the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic that traverses these ports. HTTP traffic classification is no longer limited to the well known and defined TCP ports.

Classification of HTTP Traffic Using HTTP Header Fields

In Cisco IOS Release 12.3(11)T, NBAR introduced expanded ability for users to classify HTTP traffic using information in the HTTP header fields.

HTTP works using a client/server model. HTTP clients open connections by sending a request message to an HTTP server. The HTTP server then returns a response message to the HTTP client (this response message is typically the resource requested in the request message from the HTTP client). After delivering the response, the HTTP server closes the connection and the transaction is complete.

HTTP header fields are used to provide information about HTTP request and response messages. HTTP has numerous header fields. For additional information on HTTP headers, see section 14 of RFC 2616: Hypertext Transfer Protocol--HTTP/1.1. This RFC can be found at the following URL:

<http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html>

NBAR can classify the following HTTP header fields:

- For request messages (client to server), the following HTTP header fields can be identified using NBAR:
 - User-Agent
 - Referer
 - From
- For response messages (server to client), the following HTTP header fields can be identified using NBAR:
 - Server
 - Location
 - Content-Encoding
 - Content-Base

**Note**

Use of the Content-Base field has not been implemented by the HTTP community. (See RFC 2616 for details.) Therefore, the Content-Base field is not identified by NBAR on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA.

Within NBAR, the **match protocol http c-header-field** command is used to specify that NBAR identify request messages (the "c" in the **c-header-field** portion of the command is for client). The **match protocol http s-header-field** command is used to specify response messages (the "s" in the **s-header-field** portion of the command is for server).

**Note**

For Cisco IOS Release 12.2(18)ZY2 and later releases on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, and for Cisco IOS Release 15.1(2)T and later releases, the **c-header-field** and **s-header-field** keywords and associated arguments in the **match protocol http** command are not available. The same functionality is achieved by using the individual keywords and arguments. For more information, see the syntax of the **match protocol http** command in the Cisco IOS Quality of Service Solutions Command Reference.

**Note**

The **c-header-field** performs subclassification based on a single value in the user agent, referrer, or from header field values and the **s-header-field** performs subclassification based on a single value that in the server, location, content-encoding, or content-base header field values. These header field values are not related to each other. Hence the **c-header** and **s-header** fields are replaced by user-agent, referrer, from, server, content-base, content-encoding, and location parameters as per the intent and need of HTTP subclassification.

Combinations of Classification of HTTP Headers and URL Host or MIME Type to Identify HTTP Traffic

Note that combinations of URL, Host, MIME type, and HTTP headers can be used during NBAR configuration. These combinations provide customers with more flexibility to classify specific HTTP traffic based on their network requirements.

NBAR and Classification of Citrix ICA Traffic

NBAR can classify Citrix Independent Computing Architecture (ICA) traffic and perform subport classification of Citrix traffic based on the published application name or ICA tag number.

Classification of Citrix ICA Traffic by Published Application Name

NBAR can monitor Citrix ICA client requests for a published application destined to a Citrix ICA Master browser. After the client requests 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.



Note For Citrix to monitor and classify traffic by the published application name, Server Browser Mode on the Master browser must be used.

In Server Browser Mode, NBAR statefully tracks and monitors traffic and performs a regular expression search on the packet contents for the published application name specified by the **match protocol citrix** command. The published application name is specified by using the **app** keyword and the *application-name-string* argument of the **match protocol citrix** command. For more information about the **match protocol citrix** command, see the Cisco IOS Quality of Service Solutions Command Reference.

The Citrix ICA session triggered to carry the specified application is cached, and traffic is classified appropriately for the published application name.

Citrix ICA Client Modes

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 be used to classify Citrix applications only 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 nonseamless (windows) modes of operation. In nonseamless 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 nonsession 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 in some software releases. In seamless nonsession sharing mode, each application for each particular client uses a separate TCP connection. NBAR can provide interapplication differentiation in seamless nonsession sharing mode.



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

Classification of Citrix ICA Traffic by ICA Tag Number

Citrix uses one TCP session each time an application is opened. In the TCP session, a variety of Citrix traffic may be intermingled in the same session. For example, print traffic may be intermingled with interactive traffic, causing interruption and delay for a particular application. Most users likely would prefer that printing be handled as a background process and that printing not interfere with the processing of higher-priority traffic.

To accommodate this preference, the Citrix ICA protocol includes the ability to identify Citrix ICA traffic based on the ICA tag number of the packet. The ability to identify, tag, and prioritize Citrix ICA traffic is referred to as ICA Priority Packet Tagging. With ICA Priority Packet Tagging, Citrix ICA traffic is categorized as high, medium, low, and background, depending on the ICA tag of the packet.

When ICA traffic priority tag numbers are used, and the priority of the traffic is determined, QoS features can be implemented to determine how the traffic will be handled. For example, QoS traffic policing can be configured to transmit or drop packets with a specific priority.

Citrix ICA Packet Tagging

The Citrix ICA tag is included in the first two bytes of the Citrix ICA packet, after the initial negotiations are completed between Citrix client and server. These bytes are not compressed or encrypted.

The first two bytes of the packet (byte 1 and byte 2) contain the byte count and the ICA priority tag number. Byte 1 contains the low-order byte count, and the first two bits of byte 2 contain the priority tags. The other six bits contain the high-order byte count.

The ICA priority tag value can be a number from 0 to 3. The number indicates the packet priority, with 0 being the highest priority and 3 being the lowest priority.

To prioritize Citrix traffic by the ICA tag number of the packet, you specify the tag number using the **ica-tag** keyword and the *ica-tag-value* argument of the **match protocol citrix** command. For more information about the **match protocol citrix** command, see the Cisco IOS Quality of Service Solutions Command Reference.

NBAR and RTP Payload Type Classification

RTP is a packet format for multimedia data streams. It can be used for media-on-demand and for 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). RTCP is a separate protocol that is supported by NBAR. It is important to note that the NBAR RTP Payload Type Classification feature does not identify RTCP packets and that RTCP packets run on odd-numbered ports while RTP packets run on even-numbered ports.

The data part of RTP is a thin protocol that provides support for applications with real-time properties such as continuous media (audio and video), which includes timing reconstruction, loss detection, and security and content identification. RTP is discussed in RFC 1889 (*A Transport Protocol for Real-Time Applications*) and RFC 1890 (*RTP Profile for Audio and Video Conferences with Minimal Control*).

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

The RTP payload classification takes place in the persistent mode, wherein a fully qualified RTP session NBAR does the payload sub-classification. For example, RFC 2833 requires persistent processing for RTP payload sub-classification within a classified flow.

The NBAR RTP Payload Type Classification feature not only allows real-time audio and video traffic to be statefully identified, but can also differentiate on the basis of audio and video codecs to provide more granular QoS. The RTP Payload Type Classification feature, therefore, looks deep into the RTP header to classify RTP packets.

NBAR and Classification of Custom Protocols and Applications

NBAR supports the use of custom protocols to identify custom applications. Custom protocols support static port-based protocols and applications that NBAR does not currently support. You can add to the set of protocols and application types that NBAR recognizes by creating custom protocols.

Custom protocols extend the capability of NBAR Protocol Discovery to classify and monitor additional static port applications and allows NBAR to classify nonsupported static port traffic.

**Note**

For more information about specifying user-defined (custom) protocols, see the "Creating a Custom Protocol" module.

NBAR and Classification of Peer-to-Peer File-Sharing Applications

The following are the most common peer-to-peer file-sharing applications supported by NBAR:

- BitTorrent
- DirectConnect
- eDonkey
- eMule
- FastTrack
- Grokster
- JTella
- Kazaa (as well as Kazaa Lite and Kazaa Lite Resurrection)
- Morpheus
- Win MX

Gnutella Also Supported

The Gnutella file-sharing protocol became classifiable using NBAR in Cisco IOS Release 12.1(12c)E.

Applications that use the Gnutella protocol include Bearshare, Gnewtellium, Gnucleus, Gtk-Gnutella, Limewire, Mutella, Phex, Qtella, Swapper, and Xolo.

NBAR and Classification of Streaming Protocols

In Cisco IOS Release 12.3(7)T, NBAR introduced support for Real Time Streaming Protocol (RTSP). RTSP is the protocol used for applications with steaming audio, such as the following:

- Apple QuickTime
- RealAudio (RealSystems G2)
- Windows Media Services

NBAR and AutoQoS

In the earlier Cisco IOS releases the two features that allows to automate the deployment of QoS on your network: AutoQoS--Voice over IP (VoIP), and AutoQoS for the Enterprise. Both of these AutoQoS features take advantage of the traffic classification functionality of NBAR.

**Note**

Cisco IOS Release 12.2(18)ZY (and later releases) does not support the AutoQoS--Voice over IP (VoIP) feature on the Catalyst 6500 series switch.

AutoQoS--VoIP

This feature was available with Cisco IOS Release 12.2(15)T. The AutoQoS--VoIP feature allows you to automate the deployment of QoS on your network and provides a means for simplifying the implementation and provisioning of QoS for VoIP traffic. For more information about the AutoQoS--VoIP feature and how it uses NBAR, see the "AutoQoS--VoIP" module.

AutoQoS for the Enterprise

This feature was available with Cisco IOS Release 12.3(11)T. The AutoQoS for the Enterprise feature allows you to automate the deployment of QoS in a general business environment, particularly for midsize companies and branch offices of larger companies. It expands on the functionality available with the AutoQoS--VoIP feature. For more information about the AutoQoS for the Enterprise feature and how it uses NBAR, see the "AutoQoS for the Enterprise" module.

NBAR and FWSM Integration

With Cisco IOS Release 12.2(18)ZYA, the functionality of NBAR to recognize protocols and applications was integrated with the Firewall Service Module (FWSM) on the Catalyst 6500 series switch. Available with this release were the following commands that can be used for classifying and tagging traffic to the FWSM:

- **ip nbar protocol-tagging**
- **show ip nbar protocol-tagging**

For more information about the FWSM and its connection features, see the "[Configuring Advanced Connection Features](#)" module of the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

For more information about FWSM commands (including the two commands listed), see the [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Service Module Command Reference Guide](#).

NBAR and TelePresence PDLM

Cisco IOS Release 12.2(18)ZYA2 NBAR introduced support for the Cisco TelePresence PDLM.

Cisco TelePresence integrates advanced audio, high-definition video, and interactive elements to deliver an great meeting experience.

The Telepresence PDLM uses NBAR to identify TelePresence media and TelePresence control traffic over the network. TelePresence media traffic and TelePresence control traffic are treated differently by QoS and so must be classified separately. TelePresence media traffic must have a low latency. TelePresence control traffic does not require a low latency but should not be dropped.

NBAR-Supported Protocols

The **match protocol**(NBAR) command is used to classify traffic on the basis of protocols supported by NBAR. NBAR is can classify the following 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 use statically assigned port numbers but still require stateful inspection
- TCP and UDP protocols that dynamically assign port numbers and therefore require stateful inspection

To view the list of protocols supported in a protocol pack, see [NBAR Protocol Library](#).

NBAR Memory Management

NBAR uses approximately 150 bytes of DRAM for each traffic flow that requires stateful inspection. (See [NBAR Memory Management](#), on page 13 for a list of protocols supported by NBAR that require stateful inspection.)

When NBAR is configured, it allocates 1 MB of DRAM to support up to 5000 concurrent traffic flows. NBAR checks to see if more memory is required to handle additional concurrent stateful traffic flows. If such a need is detected, NBAR expands its memory usage in increments of 200 to 400 Kb.

**Note**

This expansion of memory by NBAR does not apply if a PISA is in use.

NBAR Protocol Discovery

NBAR includes a feature called Protocol Discovery. Protocol discovery provides an easy way to discover the application protocols that are operating on an interface. For more information about protocol discovery, see the "Enabling Protocol Discovery" module.

**Note**

With Cisco IOS Release 12.2(18)ZYA, which is intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, Protocol Discovery supports Layer 2 Etherchannels.

Nonintrusive Protocol Discovery

Cisco IOS Release 12.2(18)ZYA1 includes the Nonintrusive Protocol Discovery feature which, enables the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA to perform protocol discovery in out-of-band (that is, offline) mode. In offline mode, a copy of the network traffic is used to discover the application protocols that are operating on an interface, leaving the network traffic undisturbed and available for other purposes.

Nonintrusive Protocol Discovery is closely associated with a feature called Intelligent Traffic Redirect (ITR). ITR allows network administrators to optimize system performance by identifying the specific traffic that needs to be redirected to the Supervisor 32/PISA for deep-packet inspection.

Nonintrusive Protocol Discovery is achieved by enabling ITR on an interface on which protocol discovery has been enabled. For more information about the commands used to enable ITR, see the Catalyst Supervisor Engine 32 PISA IOS Command Reference. For more information about protocol discovery, see the "Enabling Protocol Discovery" module.

**Note**

For the Nonintrusive Protocol Discovery feature to function properly, no other "intrusive" features (for example, Flexible Packet Matching [FPM]) can be in use on the interface in either the input or output direction. An intrusive feature is one that somehow manipulates the packets (such as modifying a statistic or a packet counter). If such a feature is in use, the actual traffic (and not a copy of the traffic) is redirected.

NBAR Protocol Discovery MIB

The NBAR Protocol Discovery MIB expands the capabilities of NBAR Protocol Discovery by providing the following new functionality through Simple Network Management Protocol (SNMP):

- Enable or disable Protocol Discovery per interface.
- Display Protocol Discovery statistics.
- Configure and display multiple top-n tables that list protocols by bandwidth usage.
- Configure thresholds based on traffic of particular NBAR-supported protocols or applications that report breaches and send notifications when these thresholds are crossed.

For more information about the NBAR Protocol Discovery MIB, see the "Network-Based Application Recognition Protocol Discovery Management Information Base" module.

NBAR Configuration Processes

Configuring NBAR consists of the following processes:

- Enabling Protocol Discovery (required)

When you configure NBAR, the first process is to enable Protocol Discovery.

- Configuring NBAR using the MQC (optional)

After you enable Protocol Discovery, you have the option to configure NBAR using the functionality of the MQC.

- Adding application recognition modules (also known as Packet Description Language Modules [PDLMs]) (optional)

Adding PDLMs extends the functionality of NBAR by enabling NBAR to recognize additional protocols on your network.

- Creating custom protocols (optional)

Custom protocols extend the capability of NBAR Protocol Discovery to classify and monitor additional static port applications and allow NBAR to classify nonsupported static port traffic.

NBAR Categorization and Attributes

The NBAR Categorization and Attributes feature provides the mechanism to match protocols or applications based on certain attributes. As there are many protocols and applications, categorizing them into different groups will help with reporting as well as performing group actions, such as applying QoS policies, on them. Attributes are statically assigned to each protocol or application, and they are not dependent on the traffic. The following attributes are available to configure the match criteria using the **match protocol attribute** command. They are:

application-group: The **application-group** attribute allows the configuration of applications grouped together based on the same networking application as the match criteria. For example, Yahoo-Messenger, Yahoo-VoIP-messenger, and Yahoo-VoIP-over-SIP are grouped together under the yahoo-messenger-group.

category: The **category** attribute allows you to configure applications that are grouped together based on the first level of categorization for each protocol as the match criteria. Similar applications are grouped together under one category. For example, the email category contains all email applications such as, Internet Mail Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), Lotus Notes, and so forth.

sub-category: The **sub-category** attribute provides the option to configure applications grouped together based on the second level of categorization for each protocol as the match criteria. For example, clearcase, dbase, rda, mysql and other database applications are grouped under the database group.

encrypted: The **encrypted** attribute provides the option to configure applications grouped together based on whether the protocol is an encrypted protocol or not as the match criteria. Applications are grouped together based on whether they are encrypted and non-encrypted status of the applications. Protocols for which the NBAR does not provide any value are categorized under the unassigned encrypted group.

tunnel: The **tunnel** attribute provides the option to configure protocols based on whether or not a protocol tunnels the traffic of other protocols. Protocols for which the NBAR does not provide any value are categorized under the unassigned tunnel group. For example, Layer 2 Tunneling Protocols (L2TP).



Note

Attribute-based protocol match configuration does not impact the granularity of classification either in reporting or in the protocol discovery information.

You can create custom values for the attributes application-group, category, and sub-category. The custom values enable you to name the attributes based on grouping of protocols. Use the **ip nbar attribute application-group custom application-group-name**, **ip nbar attribute category custom category-name**, and **ip nbar attribute sub-category custom sub-category-name** commands to add custom values for the attributes application-group, category, and sub-category, respectively.

The dynamically created custom attribute values can be used for attribute-map creation when using the **ip nbar attribute-map** command, and for configuring the match criterion for a class-map when using the **match protocol attribute** command.

The output from the **show ip nbar attribute-custom** command displays the number of custom values that can be defined for attributes, and the custom values that are currently defined. The **show ip nbar attribute** command displays all the attributes including the custom attributes used by NBAR.

To remove the custom values, use the **no ip nbar attribute** command.

Where to Go Next

Begin configuring NBAR by first enabling Protocol Discovery. To enable Protocol Discovery, see the "Enabling Protocol Discovery" module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Classifying Network Traffic Using NBAR

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 1: Feature Information for Classifying Network Traffic Using NBAR

Feature Name	Releases	Feature Information
Additional PDL Support for NBAR	15.1(2)T	<p>The Additional PDL Support for NBAR feature provides additional PDLs as part of feature parity between Cisco IOS Release 12.2(18)ZY and Cisco IOS Release 15.1(2)T.</p> <p>The following section includes information about this PDL support extended to Cisco IOS Release 15.1(2)T: NBAR-Supported Protocols.</p>
Distributed Network-based Application Recognition (dNBAR)	12.1(6)E 12.2(4)T 12.2(18)SXF	<p>dNBAR is NBAR used on the Cisco 7500 router with a VIP and on the Catalyst 6500 family of switches with a FlexWAN module or SIP. The implementation of NBAR and dNBAR is identical.</p> <p>The following section provides information about this feature: Information About Classifying Network Traffic Using NBAR.</p>
Enhanced NBAR	15.2(1)T	<p>The Enhanced NBAR feature provides support for additional protocols.</p> <p>The following section includes information about this feature: NBAR-Supported Protocols.</p>
nBAR: IANA Protocol Extensions Pack1	15.1(3)T	<p>The nBAR: IANA Protocol Extensions Pack1 feature allows NBAR to detect and classify a set of protocols and applications standardized by IANA.</p> <p>The following section provides information about this feature: NBAR-Supported Protocols.</p>

Feature Name	Releases	Feature Information
NBAR Categorization and Attributes	15.2(2)T	<p>The NBAR Categorization and Attributes feature provides the mechanism of matching the protocols grouped under specific categories based on the attributes. These categories are available for Class-Based Policy Language (CPL) as a match criteria for application recognition.</p> <p>The following section provides information about this feature: NBAR Categorization and Attributes.</p>
NBAR—Network-based Application Recognition	12.1(1)E 12.1(5)T 12.2(11)YT 12.2(18)ZY	<p>NBAR is a classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate QoS for that application or traffic with that protocol.</p> <p>The following section provides information about this feature: Information About Classifying Network Traffic Using NBAR.</p> <p>The following commands were introduced or modified: ip nbar protocol-tagging, match protocol citrix, match protocol fasttrack, match protocol gnutella, match protocol http, show ip nbar protocol-tagging.</p>

Feature Name	Releases	Feature Information
NBAR2: Add/Rename Static Attributes	15.4(1)T	<p>The custom values enable you to name the attributes based on grouping of protocols. You can create custom values for the attributes application-group, category, and sub-category.</p> <p>The following section provides information about this feature: NBAR Categorization and Attributes.</p> <p>The following commands were introduced or modified: ip nbar attribute, show ip nbar attribute-custom, and show ip nbar category.</p>
NBAR2 GETVPN (Cryptomap) Support	15.4(2)T	<p>GETVPN is supported.</p> <p>The following section provides information about this feature: NBAR Support for GETVPN</p>

Glossary

encryption --Encryption is the application of a specific algorithm to data so as to alter the appearance of the data, making it incomprehensible to those who are not authorized to see the information.

dNBAR --Distributed Network-Based Application Recognition. dNBAR is NBAR used on the Cisco 7500 router with a Versatile Interface Processor (VIP) and on the Catalyst 6500 family of switches with a FlexWAN module or serial interface processor (SIP). The implementation of NBAR and dNBAR is identical.

HTTP --Hypertext Transfer Protocol. The protocol used by web browsers and web servers to transfer files, such as text and graphic files.

IANA --Internet Assigned Numbers Authority. An organization operated under the auspices of the Internet Society (ISOC) as a part of the Internet Architecture Board (IAB). IANA delegates authority for IP address-space allocation and domain-name assignment to the InterNIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP stack, including autonomous system numbers.

LAN --local-area network. A high-speed, low-error data network that covers a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the Open System Interconnection (OSI) model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

MIME --Multipurpose Internet Mail Extension. The standard for transmitting nontext data (or data that cannot be represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as Russian

or Chinese), audio, and video data. MIME is defined in RFC 2045, *Multipurpose Internet Mail Extension (MIME) Part One: Format of Internet Message Bodies*.

MPLS --Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

MQC --modular quality of service command-line interface. A CLI that allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach policy maps to interfaces. Policy maps are used to apply the appropriate quality of service (QoS) to network traffic.

NBAR --Network-Based Application Recognition. A classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol.

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

Protocol Discovery --A feature included with NBAR. Protocol Discovery provides a way to discover the application protocols that are operating on an interface.

QoS --quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

RTCP --RTP Control Protocol. A protocol that monitors the QoS of an IPv6 Real-Time Transport Protocol (RTP) connection and conveys information about the ongoing session.

RTSP --Real Time Streaming Protocol. A means for enabling the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such as live audio and video, and stored content, such as prerecorded events. RTSP is designed to work with established protocols, such as Real-Time Transport Protocol (RTP) and HTTP.

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 that is contained in the packet payload, that is, information found beyond the TCP or UDP port number.

TCP --Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

tunneling --Tunneling is an architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

UDP --User Datagram Protocol. A connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768, *User Datagram Protocol*.

WAN --wide-area network. A data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers.



Enabling Protocol Discovery

Network-Based Application Recognition (NBAR) includes a feature called Protocol Discovery. Protocol Discovery provides an easy way to discover the application protocols that are operating on an interface. When you configure NBAR, the first task is to enable Protocol Discovery.

This module contains concepts and tasks for enabling the Protocol Discovery feature.

- [Finding Feature Information, page 21](#)
- [Prerequisites for Enabling Protocol Discovery, page 21](#)
- [Information About Protocol Discovery, page 22](#)
- [How to Configure Protocol Discovery, page 22](#)
- [Configuration Examples for Enabling Protocol Discovery, page 24](#)
- [Where to Go Next, page 25](#)
- [Additional References, page 25](#)
- [Feature Information for Enabling Protocol Discovery, page 26](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Prerequisites for Enabling Protocol Discovery

Before enabling Protocol Discovery, read the information in the "Classifying Network Traffic Using NBAR" module.

Information About Protocol Discovery

Protocol Discovery Functionality

NBAR determines which protocols and applications are currently running on your network. NBAR includes a feature called Protocol Discovery. Protocol Discovery provides an easy way of discovering the application protocols that are operating on an interface so that appropriate quality of service (QoS) features can be applied. With Protocol Discovery, you can discover any protocol traffic that is supported by NBAR and obtain statistics that are associated with that protocol.

Protocol Discovery maintains the following per-protocol statistics for enabled interfaces:

- Total number of input packets and bytes
- Total number of output packets and bytes
- Input bit rates
- Output bit rates

The statistics can then be used when you later define classes and traffic policies (sometimes known as policy maps) for each traffic class. The traffic policies (policy maps) are used to apply specific QoS features and functionality to the traffic classes.

How to Configure Protocol Discovery

Enabling Protocol Discovery on an Interface

The **ip nbar protocol-discovery** command is used to enable Protocol Discovery on an interface. With Cisco IOS Release 12.2(18)ZYA, intended for use on the Cisco 6500 series switch that is equipped with a Supervisor 32/PISA, the **ip nbar protocol-discovery** command is supported on both Layer 2 and Layer 3 Etherchannels.

To enable Protocol Discovery on an interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip nbar protocol-discovery**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>name-tag</i>] Example: Router(config)# interface ethernet 2/4	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> • Enter the interface type and the interface number.
Step 4	ip nbar protocol-discovery Example: Router(config-if)# ip nbar protocol-discovery	Configures NBAR to discover traffic for all protocols known to NBAR on a particular interface.
Step 5	end Example: Router(config-if)# end	(Optional) Exits interface configuration mode.

Reporting Protocol Discovery Statistics

To display a report of the Protocol Discovery statistics per interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map interface** *type number*
3. **show ip nbar protocol-discovery** [**interface** *type number*] [**stats** {**byte-count** | **bit-rate** | **packet-count** | **max-bit-rate**}] [**protocol** *protocol-name* | **top-n** *number*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show policy-map interface <i>type number</i> Example: Router# show policy-map interface Fastethernet 6/0	(Optional) Displays the packet and class statistics for all policy maps on the specified interface. <ul style="list-style-type: none"> • Enter the interface type and the interface number.
Step 3	show ip nbar protocol-discovery [interface <i>type number</i>] [stats {byte-count bit-rate packet-count max-bit-rate}] [protocol <i>protocol-name</i> top-n <i>number</i>] Example: Router# show ip nbar protocol-discovery interface Fastethernet 6/0	Displays the statistics gathered by the NBAR Protocol Discovery feature. <ul style="list-style-type: none"> • (Optional) Enter keywords and arguments to fine-tune the statistics displayed.
Step 4	exit Example: Router# exit	(Optional) Exits privileged EXEC mode.

Configuration Examples for Enabling Protocol Discovery

Example Enabling Protocol Discovery on an Interface

In the following sample configuration, Protocol Discovery is enabled on Ethernet interface 2/4.

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/4
Router(config-if)# ip nbar protocol-discovery
Router(config-if)# end
```

Example Reporting Protocol Discovery Statistics

The following example displays output from the `show ip nbar protocol-discovery` command for the five most active protocols on an Ethernet interface:

```
Router# show ip nbar protocol-discovery top-n 5

Ethernet2/0

Protocol                               Input                               Output
-----                               -
Packet Count                            Packet Count
Byte Count                               Byte Count
30sec Bit Rate (bps)                    30sec Bit Rate (bps)
30sec Max Bit Rate (bps)                30sec Max Bit Rate (bps)
-----
rtp                                     3272685                             3272685
                                         242050604                           242050604

                                         768000                               768000
                                         2002000                              2002000
gnutella                               513574                               513574
                                         118779716                            118779716
                                         383000                                383000
                                         987000                                987000
ftp                                     482183                               482183
                                         37606237                              37606237
                                         121000                                121000
                                         312000                                312000
http                                    144709                               144709
                                         32351383                              32351383
                                         105000                                105000
                                         269000                                269000
netbios                                96606                                96606
                                         10627650                              10627650
                                         36000                                 36000
                                         88000                                 88000
unknown                                1724428                              1724428
                                         534038683                            534038683
                                         2754000                              2754000
                                         4405000                              4405000
Total                                  6298724                              6298724
                                         989303872                            989303872
                                         4213000                              4213000
                                         8177000                              8177000
```

Where to Go Next

After you enable Protocol Discovery, you have the option to configure NBAR using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). To configure NBAR using the MQC, see the "Configuring NBAR Using the MQC" module.

Additional References

The following sections provide references related to enabling Protocol Discovery.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
Concepts and information about NBAR	"Classifying Network Traffic Using NBAR" module
Configuring NBAR using the MQC	"Configuring NBAR Using the MQC" module
Adding application recognition modules (also known as PDLMs)	"Adding Application Recognition Modules" module
Creating a custom protocol	"Creating a Custom Protocol" module

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Enabling Protocol Discovery

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 Enabling Protocol Discovery

Feature Name	Releases	Feature Information
NBAR--Network-Based Application Recognition	12.2(18)ZYA	<p>Integrates NBAR and Firewall Service Module (FWSM) functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA).</p> <p>The following commands were modified: ip nbar protocol-discovery, show ip nbar protocol-discovery.</p>



Configuring NBAR Using the MQC

After you enable Protocol Discovery, you can configure Network-Based Application Recognition (NBAR) using the functionality of the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). The MQC uses traffic classes and traffic policies (policy maps) to apply QoS features to classes of traffic and applications recognized by NBAR.

This module contains concepts and tasks for configuring NBAR using the MQC.

- [Finding Feature Information, page 29](#)
- [Prerequisites for Configuring NBAR Using the MQC, page 29](#)
- [Information About Configuring NBAR Using the MQC, page 30](#)
- [How to Configure NBAR Using the MQC, page 31](#)
- [Configuration Examples for Configuring NBAR Using the MQC, page 38](#)
- [Where to Go Next, page 39](#)
- [Additional References, page 40](#)
- [Feature Information for Configuring NBAR Using the MQC, page 41](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Prerequisites for Configuring NBAR Using the MQC

- Before configuring NBAR using the MQC, read the information in the "Classifying Network Traffic Using NBAR" module.

- As applicable, enable Protocol Discovery and use it to obtain statistics about the protocols and applications that are used in your network. You will need this information when using the MQC.

**Note**

This prerequisite assumes that you do not already have this information about the protocols and applications in use in your network.

Information About Configuring NBAR Using the MQC

NBAR and the MQC Functionality

To configure NBAR using the MQC, you must define a traffic class, configure a traffic policy (policy map), and then attach that traffic policy to the appropriate interface. These three tasks can be accomplished by using the MQC. The MQC is a command-line interface that allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach these traffic policies to interfaces.

In the MQC, the **class-map** command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.

Using the MQC to configure NBAR consists of the following:

- Defining a traffic class with the **class-map** command.
- Creating a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).
- Attaching the traffic policy to the interface with the **service-policy** command.

A traffic class contains three major elements: a name, one or more **match** commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands (that is, **match-all** or **match-any**). The traffic class is named in the **class-map** command line; for example, if you enter the **class-map cisco** command while configuring the traffic class in the CLI, the traffic class would be named "cisco."

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

**Note**

For NBAR, the **match protocol** commands are used to specify the match criteria, as described in the [NBAR and the match protocol Commands](#), on page 31.

NBAR and the match protocol Commands

NBAR recognizes specific network protocols and network applications that are used in your network. Once a protocol or application is recognized by NBAR, you can use the MQC to group the packets associated with those protocols or applications into classes. These classes are grouped on the basis of whether the packets conform to certain criteria.

For NBAR, the criterion is whether the packet matches a specific protocol or application known to NBAR. Using the MQC, network traffic with one network protocol (citrix, for example) can be placed into one traffic class, while traffic that matches a different network protocol (gnutella, for example) can be placed into another traffic class. Later, the network traffic within each class can be given the appropriate QoS treatment by using a traffic policy (policy map).

You specify the criteria used to classify traffic by using a **match protocol** command. The table below lists some of the available **match protocol** commands and the corresponding protocol or traffic type recognized and supported by NBAR.



Note

For a more complete list of the protocol types supported by NBAR, see the "Classifying Network Traffic Using NBAR" module.

Table 3: match protocol Commands and Corresponding Protocol or Traffic Type

match protocol Command ¹	Protocol Type
match protocol (NBAR)	Protocol type supported by NBAR
match protocol citrix	Citrix protocol
match protocol fasttrack	FastTrack peer-to-peer traffic
match protocol gnutella	Gnutella peer-to-peer traffic
match protocol http	Hypertext Transfer Protocol
match protocol rtp	Real-Time Transport Protocol traffic

¹ Cisco IOS match protocol commands can vary by release. For more information, see the command documentation for the Cisco IOS release that you are using.

How to Configure NBAR Using the MQC

Configuring a Traffic Class

Traffic classes can be used to organize packets into groups based on a user-specified criteria. For example, traffic classes can be configured to match packets on the basis of the protocol type or application recognized by NBAR. In this task, the traffic class is configured to match on the basis of the Citrix protocol type.



Note The **match protocol citrix** command is shown in Step [Configuring a Traffic Class](#). The **match protocol citrix** command is just an example of one of the **match protocol** commands that can be used. For a complete list of **match protocol** commands, see the command documentation for the Cisco IOS release that you are using.

To configure a traffic class, perform the following steps.



Note Typically, a single traffic class contains one or more **match** commands that can be used to organize packets into groups on the basis of a protocol type or application. You can create as many traffic classes as needed. However, for Cisco IOS Release 12.2(18)ZY, the following restrictions apply:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match protocol citrix**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map [match-all match-any] <i>class-map-name</i> Example: Router(config)# class-map cmap1	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode. <ul style="list-style-type: none"> • Enter the name of the class map.

	Command or Action	Purpose
Step 4	match protocol citrix Example: <pre>Router(config-cmap)# match protocol citrix</pre>	Configures NBAR to match Citrix traffic. Note The match protocol citrix command is just an example of one of the match protocol commands that can be used. For a complete list of match protocol commands, see the command documentation for the Cisco IOS release that you are using. Note For Cisco IOS Release 12.2(18)ZY, a maximum of 8 match protocol commands can be configured in a single traffic class.
Step 5	end Example: <pre>Router(config-cmap)# end</pre>	(Optional) Returns to privileged EXEC mode.

Configuring a Traffic Policy

Traffic that matches a user-specified criterion can be organized into a specific class that can, in turn, receive specific user-defined QoS treatment when that class is included in a policy map.

To configure a traffic policy, perform the following steps.



Note The **bandwidth** command is shown in Step [Configuring a Traffic Policy](#). The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use. As of Cisco IOS Release 12.2(18)ZY, CBWFQ is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA).



Note For Cisco IOS Release 12.2(18)ZY, an existing traffic policy (policy map) cannot be modified if the traffic policy is already attached to the interface. To remove the policy map from the interface, use the **no** form of the **service-policy** command.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: Router (config)# policy-map policy1	Creates or modifies a policy map that can be attached to one or more interfaces and enters policy-map configuration mode. <ul style="list-style-type: none"> • Enter the name of the policy map.
Step 4	class { <i>class-name</i> class-default } Example: Router (config-pmap)# class class1	Specifies the name of the class whose policy you want to create or change and enters policy-map class configuration mode. <ul style="list-style-type: none"> • Enter the specific class name or enter the class-default keyword.
Step 5	bandwidth { <i>bandwidth-kbps</i> remaining percent <i>percentage</i> percent <i>percentage</i> } Example: Router (config-pmap-c)# bandwidth percent 50 Example:	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. <ul style="list-style-type: none"> • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. <p>Note The bandwidth command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.</p> <p>Note As of Cisco IOS Release 12.2(18)ZY, CBWFQ is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA.</p>
Step 6	end Example: Router (config-pmap-c)# end	(Optional) Returns to privileged EXEC mode.

Attaching a Traffic Policy to an Interface or Subinterface

After a policy map is created, the next step is to attach the traffic policy (sometimes called a policy map) to an interface or subinterface. Traffic policies can be attached to either the input or output direction of the interface or subinterface.



Note

Depending on the needs of your network, you may need to attach the traffic policy to an ATM PVC, a Frame Relay data-link connection identifier (DLCI), or other type of interface.

To attach a traffic policy (policy map) to an interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **pvc** [*name*] *vpi* / *vci* [*ilmi*] **qsaal** | **smds** | **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**} *policy-map-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>name-tag</i>] Example: Router(config)# interface ethernet 2/4	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> • Enter the interface type and the interface number.

	Command or Action	Purpose
Step 4	<p>pvc [<i>name</i>] <i>vpi</i> / <i>vci</i> [<i>ilmi</i>] <i>qsaal</i> <i>smds</i> <i>l2transport</i>]</p> <p>Example:</p> <pre>Router(config-if)# pvc cisco 0/16</pre>	<p>(Optional) Creates or assigns a name to an ATM permanent virtual circuit (PVC), specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode.</p> <ul style="list-style-type: none"> Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. <p>Note This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, advance to Attaching a Traffic Policy to an Interface or Subinterface.</p>
Step 5	<p>exit</p> <p>Example:</p> <pre>Router(config-atm-vc)# exit</pre>	<p>(Optional) Returns to interface configuration mode.</p> <p>Note This step is required only if you are attaching the policy map to an ATM PVC and you completed Attaching a Traffic Policy to an Interface or Subinterface. If you are not attaching the policy map to an ATM PVC, advance to Attaching a Traffic Policy to an Interface or Subinterface.</p>
Step 6	<p>service-policy {input output} <i>policy-map-name</i></p> <p>Example:</p> <pre>Router(config-if)# service-policy input policy1</pre>	<p>Attaches a policy map (traffic policy) to an input or output interface.</p> <ul style="list-style-type: none"> Specify either the input or output keyword, and enter the policy map name. <p>Note Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached vary according your network configuration. When using the service-policy command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.</p> <p>Note After you use the service-policy command, you may see two messages similar to the following:</p> <pre>%PISA-6-NBAR_ENABLED: feature accelerated on input direction of: [interface name and type] %PISA-6-NBAR_ENABLED: feature accelerated on output direction of: [interface name and type</pre> <p>While both of these messages appear, NBAR is enabled in the direction specified by the input or output keyword only.</p>
Step 7	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	<p>(Optional) Returns to privileged EXEC mode.</p>

Verifying NBAR Using the MQC

After you create the traffic classes and traffic policies (policy maps), you may want to verify that the end result is the one you intended. That is, you may want to verify whether your traffic is being classified correctly and whether it is receiving the QoS treatment as intended. You may also want to verify that the protocol-to-port mappings are correct.

To verify the NBAR traffic classes, traffic policies, and protocol-to-port mappings, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show class-map** *[class-map-name]*
3. **show policy-map** *[policy-map]*
4. **show policy-map interface** *type number*
5. **show ip nbar port-map** *[protocol-name]*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show class-map <i>[class-map-name]</i> Example: Router# show class-map	(Optional) Displays all class maps and their matching criteria. <ul style="list-style-type: none"> • (Optional) Enter the name of a specific class map.
Step 3	show policy-map <i>[policy-map]</i> Example: Router# show policy-map Example:	(Optional) Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. <ul style="list-style-type: none"> • (Optional) Enter the name of a specific policy map.
Step 4	show policy-map interface <i>type number</i> Example: Router# show policy-map interface Fastethernet 6/0	(Optional) Displays the packet and class statistics for all policy maps on the specified interface. <ul style="list-style-type: none"> • Enter the interface type and the interface number.

	Command or Action	Purpose
Step 5	show ip nbar port-map [<i>protocol-name</i>] Example: Router# show ip nbar port-map	(Optional) Displays the current protocol-to-port mappings in use by NBAR. <ul style="list-style-type: none"> (Optional) Enter a specific protocol name.
Step 6	exit Example: Router# exit	(Optional) Exits privileged EXEC mode.

Configuration Examples for Configuring NBAR Using the MQC

Example Configuring a Traffic Class

In the following example, a class called `cmap1` has been configured. All traffic that matches the citrix protocol will be placed in the `cmap1` class.

```
Router> enable
Router# configure terminal
Router(config)# class-map cmap1
Router(config-cmap)# match protocol citrix
Router(config-cmap)# end
```

Example Configuring a Traffic Policy

In the following example, a traffic policy (policy map) called `policy1` has been configured. Policy1 contains a class called `class1`, within which CBWFQ has been enabled.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
```

**Note**

In the above example, the **bandwidth** command is used to enable Class-Based Weighted Fair Queuing (CBWFQ). CBWFQ is only an example of one QoS feature that can be applied in a policy map. Use the appropriate command for the QoS feature that you want to use. As of Cisco IOS Release 12.2(18)ZY, CBWFQ is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA.

Example Attaching a Traffic Policy to an Interface or Subinterface

In the following example, the traffic policy (policy map) called `policy1` has been attached to Ethernet interface 2/4 in the input direction of the interface.

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/4

Router(config-if)# service-policy input policy1
Router(config-if)# end
```

Example Verifying the NBAR Protocol-to-Port Mappings

The following is sample output of the **show ip nbar port-map** command. This command displays the current protocol-to-port mappings in use by NBAR. Use the display to verify that these mappings are correct.

```
Router# 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
```

If the **ip nbar port-map** command has been used, the **show ip nbar port-map** command displays the ports assigned 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. To limit the display to a specific protocol, use the *protocol-name* argument of the **show ip nbar port-map** command.

Where to Go Next

To add application recognition modules (also known as Packet Description Language Modules or PDLMs) to your network, see the "Adding Application Recognition Modules" module.

To classify network traffic on the basis of a custom protocol, see the "Creating a Custom Protocol" module.

Additional References

The following sections provide references related to configuring NBAR using the MQC.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
QoS features and functionality on the Catalyst 6500 series switch	"Configuring PFC QoS" chapter of the <i>Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide</i> , Release 12.2ZY
MQC, traffic policies (policy maps), and traffic classes	"Applying QoS Features Using the MQC" module
CBWFQ	"Configuring Weighted Fair Queueing" module
Concepts and information about NBAR	"Classifying Network Traffic Using NBAR" module
Information about enabling Protocol Discovery	"Enabling Protocol Discovery" module
Information about adding application recognition modules (also known as PDLMs)	"Adding Application Recognition Modules" module
Creating a custom protocol	"Creating a Custom Protocol" module

Technical Assistance

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

Feature Information for Configuring NBAR Using the MQC

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 4: Feature Information for Configuring NBAR Using the MQC

Feature Name	Releases	Feature Information
QoS: DirectConnect PDLM	12.4(4)T	Provides support for the DirectConnect protocol and Packet Description Language Module (PDLM). The DirectConnect protocol can now be recognized when using the MQC to classify traffic. The following sections provide information about the QoS: DirectConnect PDLM feature:
QoS: Skype Classification	12.4(4)T	Provides support for the Skype protocol. The Skype protocol can now be recognized when using the MQC to classify traffic. Note Cisco currently supports Skype Version 1 only. The following sections provide information about the QoS: Skype Classification feature:
NBAR--BitTorrent PDLM	12.4(2)T	Provides support for the BitTorrent PDLM and protocol. The BitTorrent protocol can now be recognized when using the MQC to classify traffic. The following sections provide information about the NBAR-BitTorrent PDLM feature:

Feature Name	Releases	Feature Information
NBAR--Citrix ICA Published Applications	12.4(2)T	<p>Enables NBAR to classify traffic on the basis of the Citrix Independent Computing Architecture (ICA) published application name and tag number.</p> <p>The following sections provide information about the NBAR-Citrix ICA Published Applications feature:</p>
NBAR--Multiple Matches Per Port	12.4(2)T	<p>Provides the ability for NBAR to distinguish between values of an attribute within the traffic stream of a particular application on a TCP or UDP port.</p> <p>The following sections provide information about the NBAR-Multiple Matches Per Port feature:</p>
NBAR Extended Inspection for HTTP Traffic	12.3(4)T	<p>Allows NBAR to scan TCP ports that are not well known and identify HTTP traffic that traverses these ports.</p> <p>The following sections provide information about the NBAR Extended Inspection for HTTP Traffic feature:</p>
NBAR Real-Time Transport Protocol Payload Classification	12.2(15)T	<p>Enables stateful identification of real-time audio and video traffic.</p> <p>The following section provides information about the NBAR Real-Time Transport Protocol Payload Classification feature:</p>

Feature Name	Releases	Feature Information
NBAR--Network-Based Application Recognition	12.2(18)ZYA	<p>Integrates NBAR and Firewall Service Module (FWSM) functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA). Additional protocols are now recognized by NBAR.</p> <p>The following sections provide information about the NBAR feature:</p> <p>The following command was modified: match protocol (NBAR).</p>
NBAR--Network-Based Application Recognition (Hardware Accelerated NBAR)	12.2(18)ZY	<p>Enables NBAR functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA).</p> <p>The following section provides information about the NBAR--Network-Based Application Recognition (Hardware Accelerated NBAR) feature:</p>



INDEX

P

PDLM [19](#)

S

Stateful Protocol [19](#)

Static Protocol [19](#)

subport classification [19](#)

