



Classifying Network Traffic Using NBAR

First Published: April 4, 2006
Last Updated: June 24, 2009

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 using 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.

Contents

- [Prerequisites for Using NBAR, page 2](#)
- [Restrictions for Using NBAR, page 2](#)
- [Information About Using NBAR, page 3](#)
- [Where to Go Next, page 27](#)
- [Additional References, page 28](#)
- [Glossary, page 32](#)



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

© 2006–2009 Cisco Systems, Inc. All rights reserved.

Prerequisites for Using NBAR

CEF

Before you configure NBAR, you must enable Cisco Express Forwarding (CEF). For more information on CEF, see the “[CEF Feature Roadmap](#)” module.



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

Stateful Switchover Support

NBAR is currently 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 64 MB of DRAM or more. 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, 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.
- 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) Command-Line Interface (CLI) (MQC) to set the IP differentiated services code point (DSCP) field on the NBAR-classified packets and make Multiprotocol Label Switching (MPLS) map the DSCP setting to the MPLS experimental (EXP) setting inside the MPLS header.
- 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 that originate from or that are destined to the router running NBAR.

NBAR is not supported on the following logical interfaces:

- Fast Etherchannel



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.

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 also be used with service modules such as a Firewall Service Module (FWSM) and an Intrusion Detection Service Module (IDSM) 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 IDSM) 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 non-inline mode with service modules even when using Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), or VLAN Access Control List (VACL) Capture functionality 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 Using NBAR

Before classifying network traffic using NBAR, you should understand the following concepts:

- [NBAR Functionality, page 4](#)
- [NBAR Benefits, page 5](#)
- [NBAR and Classification of HTTP Traffic, page 6](#)

- [NBAR and Classification of Citrix ICA Traffic, page 9](#)
- [NBAR and RTP Payload Type Classification, page 11](#)
- [NBAR and Classification of Custom Protocols and Applications, page 11](#)
- [NBAR and Classification of Peer-to-Peer File-Sharing Applications, page 11](#)
- [NBAR and Classification of Streaming Protocols, page 12](#)
- [NBAR and AutoQoS, page 13](#)
- [NBAR and FWSM Integration, page 13](#)
- [NBAR and TelePresence PDLM, page 13](#)
- [NBAR-Supported Protocols, page 14](#)
- [NBAR Memory Management, page 26](#)
- [NBAR Protocol Discovery, page 26](#)
- [NBAR Protocol Discovery MIB, page 27](#)
- [NBAR Configuration Processes, page 27](#)

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 Command-Line Interface (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 QoS features listed below 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 include the following:

- 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 NBAR 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

Improved Network Management

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 that are 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 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 right level of network resources for network traffic.

NBAR and Classification of HTTP Traffic

This section includes information about the following topics:

- [Classification of HTTP Traffic by URL, Host, or MIME, page 6](#)
- [Classification of HTTP Traffic Using the HTTP Header Fields, page 7](#)
- [Combinations of Classification of HTTP Headers and URL, Host, or MIME Type to Identify HTTP Traffic, page 9](#)

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.

[Figure 1](#) illustrates a network topology with NBAR in which Router Y is the NBAR-enabled router.

Figure 1 *Network Topology with NBAR*



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) on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, up to 56 parameters or sub classifications can be specified with the **match protocol http** command. These parameters or sub classifications 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 sub classifications.

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 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 the 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 is able to 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) on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, the **c-header-field** and **s-header-field** keywords and associated arguments 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*.

Examples

In the following example, any request message that contains “somebody@cisco.com” in the User-Agent, Referer, or From fields will be classified by NBAR. Typically, a term with a format similar to “somebody@cisco.com” would be found in the From header field of the HTTP request message.

```
class-map match-all class1
 match protocol http c-header-field "somebody@cisco.com"
```

In the following example, any request message that contains “http://www.cisco.com/routers” in the User-Agent, Referer, or From fields will be classified by NBAR. Typically, a term with a format similar to “http://www.cisco.com/routers” would be found in the Referer header field of the HTTP request message.

```
class-map match-all class2
 match protocol http c-header-field "http://www.cisco.com/routers"
```

In the following example, any request message that contains “CERN-LineMode/2.15” in the User-Agent, Referer, or From header fields will be classified by NBAR. Typically, a term with a format similar to “CERN-LineMode/2.15” would be found in the User-Agent header field of the HTTP request message.

```
class-map match-all class3
 match protocol http c-header-field "CERN-LineMode/2.15"
```

In the following example, any response message that contains “CERN/3.0” in the Content-Base (if available), Content-Encoding, Location, or Server header fields will be classified by NBAR. Typically, a term with a format similar to “CERN/3.0” would be found in the Server header field of the response message.

```
class-map match-all class4
 match protocol http s-header-field "CERN/3.0"
```

In the following example, any response message that contains “http://www.cisco.com/routers” in the Content-Base (if available), Content-Encoding, Location, or Server header fields will be classified by NBAR. Typically, a term with a format similar to “http://www.cisco.com/routers” would be found in the Content-Base (if available) or Location header field of the response message.

```
class-map match-all class5
 match protocol http s-header-field "http://www.cisco.com/routers"
```

In the following example, any response message that contains “gzip” in the Content-Base (if available), Content-Encoding, Location, or Server header fields will be classified by NBAR. Typically, the term “gzip” would be found in the Content-Encoding header field of the response message.

```
class-map match-all class6
 match protocol http s-header-field "gzip"
```

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.

Examples

In the following example, HTTP header fields are combined with a URL to classify traffic. In this example, traffic with a User-Agent field of “CERN-LineMode/3.0” and a Server field of “CERN/3.0,” along with URL “www.cisco.com/routers,” will be classified using NBAR:

```
class-map match-all c-http
  match protocol http c-header-field "CERN-LineMode/3.0"
  match protocol http s-header-field "CERN/3.0"
  match protocol http url "www.cisco.com/routers"
```

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.

This section includes information about the following topics:

- [Classification of Citrix ICA Traffic by Published Application Name, page 9](#)
- [Classification of Citrix ICA Traffic by ICA Tag Number, page 10](#)

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 non-seamless (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 on 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 people 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 as well as 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.

NBAR RTP Payload Type Classification not only allows one to statefully identify real-time audio and video traffic 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

Gnutella is another file-sharing protocol that 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.

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 **file-transfer** keyword indicates that a regular expression variable will be used to identify specific Gnutella or FastTrack traffic. 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 the following 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 on the basis of filename extension or 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*"

```

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

Earlier Cisco IOS releases included two features that allow you 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) 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 has been integrated with the Firewall Service Module (FWSM) on the Catalyst 6500 series switch. Available with this release are 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 above), 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 with the power of the underlying network to deliver an immersive 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 capable of classifying 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

[Table 1](#) lists the NBAR-supported protocols available in Cisco IOS software, sorted by category. The table also provides information about the protocol type, the well-known port numbers (if applicable), the syntax for entering the protocol in NBAR, and the Cisco IOS release in which the protocol was initially supported. This table is updated when a protocol is added to a new Cisco IOS release train.

Many peer-to-peer file-sharing applications not listed in this table can be classified using FastTrack or Gnutella. See the [“NBAR and Classification of Peer-to-Peer File-Sharing Applications”](#) section on [page 11](#) for additional information.

RTSP can be used to classify various types of applications that use streaming audio. See the [“NBAR and Classification of Streaming Protocols”](#) section on [page 12](#) for additional information.

**Note**

Support for some protocols can be added to NBAR using application recognition modules (also known as Packet Description Language Modules [PDLMs]). For more information about PDLMs, see the [“Adding Application Recognition Modules”](#) module.

**Note**

[Table 1](#) includes the NBAR-supported protocols available with the 12.2(18)ZY and 12.2(18)ZYA releases. Protocols included in the 12.2(18)ZY and 12.2(18)ZYA releases are supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA.

Table 1 *NBAR-Supported Protocols*

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Enterprise Application	Citrix ICA	TCP/UDP	TCP: 1494, 2512, 2513, 2598 UDP: 1604	Citrix ICA traffic	citrix citrix app citrix ica-tag	12.1(2)E 12.1(5)T 12.2(18)ZYA1
	PCAnywhere	TCP/UDP	TCP: 5631, 65301 UDP: 22, 5632	Symantic PCAnywhere	pcanywhere	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Novadigm	TCP/UDP	3460–3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T 12.2(18)ZYA1
	SAP	TCP	3300–3315 (sap-pgm.pdlm) 3200–3215 (sap-app.pdlm) 3600–3615 (sap-msg.pdlm)	Application server to application server traffic (sap-pgm.pdlm) Client to application server traffic (sap-app.pdlm) Client to message server traffic (sap-msg.pdlm)	sap	12.1E 12.2T 12.3 12.3T 12.2(18)ZYA1
	Exchange ¹	TCP	135	MS-RPC for Exchange	exchange	12.1(1)E 12.1(5)T 12.2(18)ZY 12.2(18)ZYA 12.2(18)ZYA1
	MAPI	TCP	135	Messaging Application Programming Interface	mapi	12.2(18)ZYA 12.2(18)ZYA1

Table 1 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Routing Protocol	BGP	TCP/ UDP	179	Border Gateway Protocol	bgp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	EGP	IP	8	Exterior Gateway Protocol	egp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	OSPF	IP	89	Open Shortest Path First	ospf	12.3(8)T 12.2(18)ZYA1
	RIP	UDP	520	Routing Information Protocol	rip	12.1(1)E 12.1(5)T 12.2(18)ZYA1
Database	SQL*NET	TCP/ UDP	1521	SQL*NET for Oracle	sqlnet	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	MS- SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	CIFS	TCP	139, 445	Common Internet File System	cifs	12.2(18)ZYA 12.2(18)ZYA1
Health	DiCom	TCP	Dynamically Assigned	Digital Imaging and Communications in Medicine	dicom	12.2(18)ZYA 12.2(18)ZYA1
	HL7	TCP	Dynamically Assigned	Health Level Seven	hl7	12.2(18)ZYA 12.2(18)ZYA1
Financial	FIX	TCP	Dynamically Assigned	Financial Information Exchange	fix	12.2(18)ZYA 12.2(18)ZYA1

Table 1 *NBAR-Supported Protocols (continued)*

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Security and Tunneling	GRE	IP	47	Generic Routing Encapsulation	gre	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	IPINIP	IP	4	IP in IP	ipinip	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	IPsec	IP	50, 51	IP Encapsulating Security Payload/ Authentication-Header	ipsec	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	L2TP	UDP	1701	L2F/L2TP Tunnel	l2tp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	MS-PPTP	TCP	1723	Microsoft Point-to-Point Tunneling Protocol for VPN	pptp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SFTP	TCP	990	Secure FTP	secure-ftp	12.1(1)E 12.1(5)T 12.2(18)ZYA1

Table 1 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Security and Tunneling (Continued)	SHTTP	TCP	443	Secure HTTP	secure-http	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SIMAP	TCP/ UDP	585, 993	Secure IMAP	secure-imap	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SIRC	TCP/ UDP	994	Secure IRC	secure-irc	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SLDAP	TCP/ UDP	636	Secure LDAP	secure-ldap	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SNNTTP	TCP/ UDP	563	Secure NNTP	secure-nntp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SPOP3	TCP/ UDP	995	Secure POP3	secure-pop3	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	STELNET	TCP	992	Secure Telnet	secure-telnet	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SOCKS	TCP	1080	Firewall Security Protocol	socks	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SSH	TCP	22	Secured Shell	ssh	12.1(1)E 12.1(5)T 12.2(18)ZYA1
Network Management	ICMP	IP	1	Internet Control Message Protocol	icmp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SNMP	TCP/ UDP	161, 162	Simple Network Management Protocol	snmp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Syslog	UDP	514	System Logging Utility	syslog	12.1(1)E 12.1(5)T 12.2(18)ZYA1

Table 1 *NBAR-Supported Protocols (continued)*

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Network Mail Services	IMAP	TCP/UDP	143, 220	Internet Message Access Protocol	imap	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	POP3	TCP/UDP	110	Post Office Protocol	pop3	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Notes	TCP/UDP	1352	Lotus Notes	notes	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SMTP	TCP	25	Simple Mail Transfer Protocol	smtp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
Directory	DHCP/BOOTP	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol	dhcp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Finger	TCP	79	Finger User Information Protocol	finger	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	DNS	TCP/UDP	53	Domain Name System	dns	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Kerberos	TCP/UDP	88, 749	Kerberos Network Authentication Service	kerberos	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	12.1(1)E 12.1(5)T 12.2(18)ZYA1

Table 1 *NBAR-Supported Protocols (continued)*

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Streaming Media	CU-SeeMe	TCP/ UDP	TCP: 7648, 7649 UDP: 24032	Desktop Video Conferencing	cuseeme	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Netshow	TCP/ UDP	Dynamically Assigned	Microsoft Netshow	netshow	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	RealAudio	TCP/ UDP	Dynamically Assigned	RealAudio Streaming Protocol	realaudio	12.1(1)E 12.1(5)T
	StreamWorks	UDP	Dynamically Assigned	Xing Technology Stream Works Audio and Video	streamwork	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	VDOLive	TCP/ UDP	Static (7000) with inspection	VDOLive Streaming Video	vdolive	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	RTSP	TCP/ UDP	Dynamically Assigned	Real Time Streaming Protocol	rtsp	12.3(11)T 12.2(18)ZYA1
	MGCP	TCP/ UDP	2427, 2428, 2727	Media Gateway Control Protocol	mgcp	12.3(7)T 12.2(18)ZYA1
	YouTube ²	TCP	Both static (80) and dynamically assigned	Online Video-Sharing Website	youtube	12.2(18)ZYA 12.2(18)ZYA1

Table 1 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Internet	FTP	TCP	Dynamically Assigned	File Transfer Protocol	ftp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Gopher	TCP/ UDP	70	Internet Gopher Protocol	gopher	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	HTTP	TCP	80 ³	Hypertext Transfer Protocol	http	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	IRC	TCP/ UDP	194	Internet Relay Chat	irc	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Telnet	TCP	23	Telnet Protocol	telnet	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	TFTP	UDP	Static (69) with inspection	Trivial File Transfer Protocol	tftp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	NNTP	TCP/ UDP	119	Network News Transfer Protocol	nntp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
Signaling	RSVP	UDP	1698, 1699	Resource Reservation Protocol	rsvp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
RPC	NFS	TCP/ UDP	2049	Network File System	nfs	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Sunrpc	TCP/ UDP	Dynamically Assigned	Sun Remote Procedure Call	sunrpc	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	MSN-messenger	TCP	1863	MSN Messenger Chat Messages ⁴	msn-messenger	12.2(18)ZYA 12.2(18)ZYA1
	Yahoo-messenger	TCP	5050, 5101	Yahoo Messenger Chat Messages	yahoo-messenger	12.2(18)ZYA 12.2(18)ZYA1
	AOL-messenger	TCP	5190, 443	AOL Instant Messenger Chat Messages	aol-messenger	12.2(18)ZYA 12.2(18)ZYA1
Non-IP and LAN/ Legacy	NetBIOS	TCP/ UDP	137, 138, 139	NetBIOS over IP (MS Windows)	netbios	12.1(1)E 12.1(5)T 12.2(18)ZYA1

Table 1 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Misc.	NTP	TCP/ UDP	123	Network Time Protocol	ntp	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Printer	TCP/ UDP	515	Printer	printer	12.1(2)E 12.1(5)T 12.2(18)ZYA1
	X Windows	TCP	6000–6003	X11, X Windows	xwindows	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	r-commands	TCP	Dynamically Assigned	rsh, rlogin, rexec	rcmd	12.1(1)E 12.1(5)T 12.2(18)ZYA1
	AppleQTC	TCP/ UDP	458	Apple Quick Time	appleqtc	12.2(18)ZYA 12.2(18)ZYA1
	Chargen	TCP/ UDP	19	Character Generator	chargen	12.2(18)ZYA 12.2(18)ZYA1
	ClearCase	TCP/ UDP	371	Clear Case Protocol Software Informer	clearcase	12.2(18)ZYA 12.2(18)ZYA1
	Corba	TCP/ UDP	683, 684	Corba Internet Inter-Orb Protocol (IIOP)	corba-iiop	12.2(18)ZYA 12.2(18)ZYA1
	Daytime	TCP/ UDP	13	Daytime Protocol	daytime	12.2(18)ZYA 12.2(18)ZYA1
	Doom	TCP/ UDP	666	Doom	doom	12.2(18)ZYA 12.2(18)ZYA1
	Echo	TCP/ UDP	7	Echo Protocol	echo	12.2(18)ZYA 12.2(18)ZYA1
	IBM DB2	TCP/ UDP	523	IBM Information Management	ibm-db2	12.2(18)ZYA 12.2(18)ZYA1
	IPX	TCP/ UDP	213	Internet Packet Exchange	ipx	12.2(18)ZYA 12.2(18)ZYA1
	ISAKMP	TCP/ UDP	500	Internet Security Association and Key Management	isakmp	12.2(18)ZYA 12.2(18)ZYA1
	ISI-GL	TCP/ UDP	55	Interoperable Self Installation Graphics Language	isi-gl	12.2(18)ZYA 12.2(18)ZYA1
	KLogin	TCP	543	KLogin	klogin	12.2(18)ZYA 12.2(18)ZYA1
	KShell	TCP	544	KShell	kshell	12.2(18)ZYA 12.2(18)ZYA1

Table 1 *NBAR-Supported Protocols (continued)*

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Misc. (Continued)	LockD	TCP/ UDP	4045	LockD	lockd	12.2(18)ZYA 12.2(18)ZYA1
	Microsoft-DS	TCP/ UDP	445	Microsoft Directory Services	microsoftds	12.2(18)ZYA 12.2(18)ZYA1
	Nickname	TCP/ UDP	43	Nickname	nicname	12.2(18)ZYA 12.2(18)ZYA1
	NPP	TCP/ UDP	92	Network Payment Protocol	npp	12.2(18)ZYA 12.2(18)ZYA1
	ORASRV	TCP	1525	ORASRV	ora-srv	12.2(18)ZYA 12.2(18)ZYA1
	RTelnet	TCP/ UDP	107	Remote Telnet Service	rtelnet	12.2(18)ZYA 12.2(18)ZYA1
	RCP	TCP/ UDP	469	Rate Control Protocol	rcp	12.2(18)ZYA 12.2(18)ZYA1
	SQLExec	TCP/ UDP	9088	SQL Exec	sqlexec	12.2(18)ZYA 12.2(18)ZYA1
	Systat	TCP/ UDP	11	System Statistics	systat	12.2(18)ZYA 12.2(18)ZYA1
	TACACS	TCP/ UDP	49, 65	Terminal Access Controller Access-Control System	tacacs	12.2(18)ZYA 12.2(18)ZYA1
	Time	TCP/ UDP	37	Time	time	12.2(18)ZYA 12.2(18)ZYA1
	VNC	UDP	5800, 5900, 5901	Virtual Network Computing	vnc	12.2(18)ZYA 12.2(18)ZYA1
	Whois++	TCP/ UDP	63	Whois++	whois++	12.2(18)ZYA 12.2(18)ZYA1
	XDMCP	UDP	177	X Display Manager Control Protocol	xdmcp	12.2(18)ZYA 12.2(18)ZYA1

Table 1 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Voice	H.323	TCP	Dynamically Assigned	H.323 Teleconferencing Protocol	h323	12.3(7)T 12.2(18)ZYA1
	RTCP	TCP/ UDP	Dynamically Assigned	Real-Time Control Protocol	rtcp	12.1E 12.2T 12.3 12.3T 12.3(7)T 12.2(18)ZYA1
	RTP	TCP/ UDP	Dynamically Assigned	Real-Time Transport Protocol Payload Classification	rtp	12.2(8)T 12.2(18)ZYA1
	Cisco-phone ⁵	UDP	5060	Cisco IP Phones and PC-Based Unified Communicators	cisco-phone	12.2(18)ZYA 12.2(18)ZYA1
	SIP	TCP/ UDP	5060	Session Initiation Protocol	sip	12.3(7)T 12.2(18)ZYA1
	SCCP/ Skinny	TCP	2000, 2001, 2002	Skiny Client Control Protocol	skinny	12.3(7)T 12.2(18)ZYA1
	Skype ⁶	TCP/ UDP	Dynamically Assigned	Peer-to-Peer VoIP Client Software	skype	12.4(4)T
	TelePresence	TCP/ UDP	Dynamically Assigned	Cisco TelePresence System	telepresence-media telepresence-control	12.2(18)ZYA2

Table 1 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Peer-to-Peer File-Sharing Applications	BitTorrent	TCP	Dynamically Assigned, or 6881–6889	BitTorrent File Transfer Traffic	bittorrent	12.4(2)T 12.2(18)ZYA1
	Direct Connect	TCP/UDP	411	Direct Connect File Transfer Traffic	directconnect	12.4(4)T 12.2(18)ZYA1
	eDonkey/ eMule	TCP	4662	eDonkey File-Sharing Application eMule traffic is also classified as eDonkey traffic in NBAR.	edonkey	12.3(11)T 12.2(18)ZYA1
	FastTrack	N/A	Dynamically Assigned	FastTrack	fasttrack	12.1(12c)E 12.2(18)ZYA1
	Gnutella	TCP	Dynamically Assigned	Gnutella	gnutella	12.1(12c)E 12.2(18)ZYA1
	KaZaA	TCP/UDP	Dynamically Assigned	KaZaA Note that earlier KaZaA version 1 traffic can be classified using FastTrack.	kazaa2	12.2(8)T 12.2(18)ZYA1
	WinMX	TCP	6699	WinMX Traffic	winmx	12.3(7)T 12.2(18)ZYA1

1. For Release 12.2(18)ZYA, Cisco supports Exchange 03 and 07 only. MS client access is recognized, but web client access is not recognized.
2. For Release 12.2(18)ZYA, access to YouTube via HTTP only will be recognized.
3. In Release 12.3(4)T, the NBAR Extended Inspection for Hypertext Transfer Protocol (HTTP) Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic that is traversing these ports.
4. For Release 12.2(18)ZYA, messages (“chat”) from Yahoo, MSN, and AOL are recognized. Messages from Lotus and SameTime are not recognized. Video and voice from Instant Messaging are also not recognized.
5. For Release 12.2(18)ZYA, only SIP and Skinny telephone connections (cisco-phone traffic connections) are recognized. H.323 telephone connections are not recognized.
6. Skype was introduced in Cisco IOS Release 12.4(4)T. As a result of this introduction, Skype is now native in (included with) the Cisco IOS software and uses the NBAR infrastructure new to Cisco IOS Release 12.4(4)T. Cisco software supports Skype 1.0, 2.5, and 3.0. Note that certain hardware platforms do not support Skype. For instance, Skype is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor/PISA.

NBAR Memory Management

NBAR uses approximately 150 bytes of DRAM for each traffic flow that requires stateful inspection. (See [Table 1](#) 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, intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, Protocol Discovery supports Layer 2 Etherchannels.

Non-intrusive Protocol Discovery

Cisco IOS Release 12.2(18)ZYA1 includes a feature called Non-intrusive Protocol Discovery. The Non-intrusive Protocol Discovery feature 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.

Non-intrusive 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.

Non-intrusive 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 Non-intrusive 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 Management Information Base (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 view 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.

Where to Go Next

Begin configuring NBAR by first enabling Protocol Discovery. To enable Protocol Discovery, see the [“Enabling Protocol Discovery”](#) module.

Additional References

The following sections provide references related to classifying network traffic using NBAR.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference
QoS features and functionality	“Quality of Service Overview” module
QoS features and functionality on the Catalyst 6500 series switch	“Configuring PFC QoS” module of the <i>Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide</i> , Release 12.2ZY
Classifying network traffic if not using NBAR	“Classifying Network Traffic” module
FWSM and its connection features	“Configuring Advanced Connection Features” module of the <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide</i>
FWSM commands	Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Service Module Command Reference Guide
IDS/IPS	“Configuring IDS/IPS-2” module of the <i>Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface</i>
SPAN or RSPAN	“Configuring SPAN and RSPAN” module of the <i>Catalyst 6500 Series Software Configuration Guide</i>
VACL Capture	“VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running Cisco IOS Software” module
Catalyst 6500 series switch and QoS	“Configuring QoS” module of the <i>Catalyst 6500 Series Software Configuration Guide</i>
Commands used to enable ITR on the Catalyst 6500 series switch equipped with a Supervisor 32/PISA	Catalyst Supervisor Engine 32 PISA IOS Command Reference .
FPM	“Flexible Packet Matching” module
FPM eXtensible Markup Language (XML) Configuration	“Flexible Packet Matching XML Configuration” module
Marking network traffic	“Marking Network Traffic” module
CISCO-NBAR-PROTOCOL-DISCOVERY MIB	“Network-Based Application Recognition Protocol Discovery Management Information Base” module
CEF	“Cisco Express Forwarding Features Roadmap” module
AutoQoS, ¹ AutoQos for the Enterprise, VoIP traffic	“AutoQoS—VoIP” module; “AutoQos for the Enterprise” module
NBAR Protocol Discovery MIB	“Network-Based Application Recognition Protocol Discovery Management Information Base” module
Enabling Protocol Discovery	“Enabling Protocol Discovery” module
Configuring NBAR using the MQC	“Configuring NBAR Using the MQC” module

Related Topic	Document Title
Adding application recognition modules (also known as PDLMs)	“Adding Application Recognition Modules” module
Creating a custom protocol	“Creating a Custom Protocol” module

1. Cisco IOS Release 12.2(18)ZY does not support either the AutoQoS—Voice over IP (VoIP) feature or the AutoQoS for the Enterprise feature on the Catalyst 6500 series switch.

Standards

Standards	Title
ISO 0009	<i>File Transfer Protocol (FTP)</i>
ISO 0013	<i>Domain Names - Concepts and Facilities</i>
ISO 0033	<i>The TFTP Protocol (Revision 2)</i>
ISO 0034	<i>Routing Information Protocol</i>
ISO 0053	<i>Post Office Protocol - Version 3</i>
ISO 0056	<i>RIP Version 2</i>

MIBs

MIBs	MIBs Link
CISCO-NBAR-PROTOCOL-DISCOVERY MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 742	<i>NAME/FINGER Protocol</i>
RFC 759	<i>Internet Message Protocol</i>
RFC 768	<i>User Datagram Protocol</i>
RFC 792	<i>Internet Control Message Protocol</i>
RFC 793	<i>Transmission Control Protocol</i>
RFC 821	<i>Simple Mail Transfer Protocol</i>
RFC 827	<i>Exterior Gateway Protocol</i>
RFC 854	<i>Telnet Protocol Specification</i>
RFC 888	<i>“STUB” Exterior Gateway Protocol</i>
RFC 904	<i>Exterior Gateway Protocol Formal Specification</i>
RFC 951	<i>Bootstrap Protocol</i>

RFC	Title
RFC 959	<i>File Transfer Protocol</i>
RFC 977	<i>Network News Transfer Protocol</i>
RFC 1001	<i>Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods</i>
RFC 1002	<i>Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications</i>
RFC 1057	<i>RPC: Remote Procedure Call</i>
RFC 1094	<i>NFS: Network File System Protocol Specification</i>
RFC 1112	<i>Host Extensions for IP Multicasting</i>
RFC 1157	<i>Simple Network Management Protocol</i>
RFC 1282	<i>BSD Rlogin</i>
RFC 1288	<i>The Finger User Information Protocol</i>
RFC 1305	<i>Network Time Protocol</i>
RFC 1350	<i>The TFTP Protocol (Revision 2)</i>
RFC 1436	<i>The Internet Gopher Protocol</i>
RFC 1459	<i>Internet Relay Chat Protocol</i>
RFC 1510	<i>The Kerberos Network Authentication Service</i>
RFC 1542	<i>Clarifications and Extensions for the Bootstrap Protocol</i>
RFC 1579	<i>Firewall-Friendly FTP</i>
RFC 1583	<i>OSPF Version 2</i>
RFC 1657	<i>Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol</i>
RFC 1701	<i>Generic Routing Encapsulation</i>
RFC 1730	<i>Internet Message Access Protocol—Version 4</i>
RFC 1771	<i>A Border Gateway Protocol 4 (BGP-4)</i>
RFC 1777	<i>Lightweight Directory Access Protocol</i>
RFC 1831	<i>RPC: Remote Procedure Call Protocol Specification Version 2</i>
RFC 1889	<i>A Transport Protocol for Real-Time Applications</i>
RFC 1890	<i>RTP Profile for Audio and Video Conferences with Minimal Control</i>
RFC 1928	<i>SOCKS Protocol Version 5</i>
RFC 1939	<i>Post Office Protocol—Version 3</i>
RFC 1945	<i>Hypertext Transfer Protocol—HTTP/1.0</i>
RFC 1964	<i>The Kerberos Version 5 GSS-API Mechanism</i>
RFC 2045	<i>Multipurpose Internet Mail Extension (MIME) Part One: Format of Internet Message Bodies</i>
RFC 2060	<i>Internet Message Access Protocol—Version 4 rev1</i>
RFC 2068	<i>Hypertext Transfer Protocol—HTTP/1.1</i>
RFC 2131	<i>Dynamic Host Configuration Protocol</i>

RFC	Title
RFC 2205	<i>Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification</i>
RFC 2236	<i>Internet Group Management Protocol, Version 2</i>
RFC 2251	<i>Lightweight Directory Access Protocol (v3)</i>
RFC 2252	<i>Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions</i>
RFC 2253	<i>Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names</i>
RFC 2326	<i>Real Time Streaming Protocol (RTSP)</i>
RFC 2401	<i>Security Architecture for the Internet Protocol</i>
RFC 2406	<i>IP Encapsulating Security Payload</i>
RFC 2453	<i>RIP Version 2</i>
RFC 2616	<i>Hypertext Transfer Protocol—HTTP/1.1</i>
	Note This RFC updates RFC 2068.

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

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.

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

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.

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.

support 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.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.

