QoS: NBAR Configuration Guide Cisco IOS Release 12.2SX

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

CONTENTS

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 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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

CEF

Before you configure NBAR, you must enable Cisco Express Forwarding (CEF).

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 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.
- 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, page 3

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

- NBAR Functionality, page 4

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

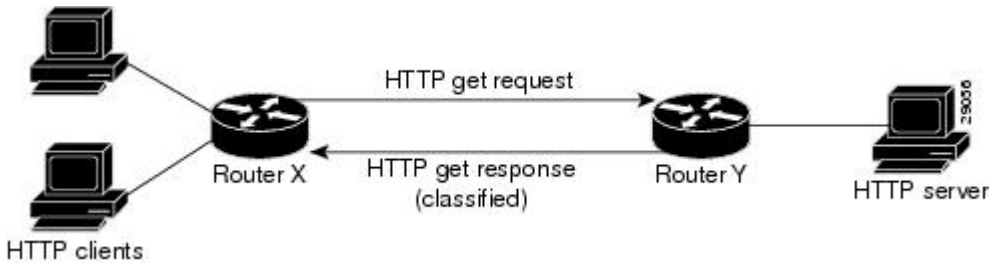
This section includes information about the following topics:

Classification of HTTP Traffic by URL Host or MIME

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 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 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 sub-classification based on a single value in the user-agent, referrer, or from header field values and the **s-header-field** performs sub-classification 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 sub-classification.

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.

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-clasification within a classified flow.

The NBAR RTP Payload Type Classification feature 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

The table below 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, 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, 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 The table below 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 15.1(2)T
	PCAnywhere	TCP/UDP	TCP: 5631, 65301 UDP: 22, 5632	Symantic PCAnywhere	pcanywhere	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	Novadigm	TCP/ UDP	3460-3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	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 12.2(18)ZYA1 12.3 12.3T 15.1(2)T
	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 15.1(2)T
	MAPI	TCP	135	Messaging Application Programming Interface	mapi	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
Routing Protocol	BGP	TCP/ UDP	179	Border Gateway Protocol	bgp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	EGP	IP	8	Exterior Gateway Protocol	egp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

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.

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	OSPF	IP	89	Open Shortest Path First	ospf	12.2(18)ZYA1 12.3(8)T 15.1(2)T
	RIP	UDP	520	Routing Information Protocol	rip	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
Database	SQL*NET	TCP/ UDP	1521	SQL*NET for Oracle	sqlnet	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	MS- SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferenci ng	sqlserver	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	CIFS	TCP	139, 445	Common Internet File System	cifs	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
Health	DiCom	TCP	Dynamically Assigned	Digital Imaging and Communication s in Medicine	dicom	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	HL7	TCP	Dynamically Assigned	Health Level Seven	hl7	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
Financial	FIX	TCP	Dynamically Assigned	Financial Information Exchange	fix	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
Security and Tunneling	GRE	IP	47	Generic Routing Encapsulation	gre	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	IPINIP	IP	4	IP in IP	ipinip	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	IPsec	IP	50, 51	IP Encapsulating Security Payload/	ipsec	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
				Authentication-Header		
	L2TP	UDP	1701	L2F/L2TP Tunnel	l2tp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	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 15.1(2)T
	SFTP	TCP	990	Secure FTP	secure-ftp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
Security and Tunneling (Continued)	SHTTP	TCP	443	Secure HTTP	secure-http	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SIMAP	TCP/ UDP	585, 993	Secure IMAP	secure-imap	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SIRC	TCP/ UDP	994	Secure IRC	secure-irc	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SLDAP	TCP/ UDP	636	Secure LDAP	secure-ldap	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SNNTP	TCP/ UDP	563	Secure NNTP	secure-nntp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SPOP3	TCP/ UDP	995	Secure POP3	secure-pop3	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	STELNET	TCP	992	Secure Telnet	secure-telnet	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SOCKS	TCP	1080	Firewall Security Protocol	socks	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SSH	TCP	22	Secured Shell	ssh	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
Network Management	ICMP	IP	1	Internet Control Message Protocol	icmp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SNMP	TCP/ UDP	161, 162	Simple Network Management Protocol	snmp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Syslog	UDP	514	System Logging Utility	syslog	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
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 15.1(2)T
	POP3	TCP/ UDP	110	Post Office Protocol	pop3	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Notes	TCP/ UDP	1352	Lotus Notes	notes	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	SMTP	TCP	25	Simple Mail Transfer Protocol	smtp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
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 15.1(2)T
	Finger	TCP	79	Finger User Information Protocol	finger	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	DNS	TCP/ UDP	53	Domain Name System	dns	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Kerberos	TCP/ UDP	88, 749	Kerberos Network Authentication Service	kerberos	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	LDAP	TCP/ UDP	389	Lightweight Directory Access Protocol	ldap	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
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 15.1(2)T
	Netshow	TCP/ UDP	Dynamically Assigned	Microsoft Netshow	netshow	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	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 15.1(2)T
	VDOLive	TCP/ UDP	Static (7000) with inspection	VDOLive Streaming Video	vdolive	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	RTSP	TCP/ UDP	Dynamically Assigned	Real Time Streaming Protocol	rtsp	12.2(18)ZYA1 12.3(11)T 15.1(2)T
	MGCP	TCP/ UDP	2427, 2428, 2727	Media Gateway Control Protocol	mgcp	12.3(7)T 12.2(18)ZYA1 15.1(2)T
	YouTube[2]	TCP	Both static (80) and dynamically assigned	Online Video-Sharing Website	youtube	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
Internet	FTP	TCP	Dynamically Assigned	File Transfer Protocol	ftp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Gopher	TCP/ UDP	70	Internet Gopher Protocol	gopher	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	HTTP	TCP	80[3]	Hypertext Transfer Protocol	http	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	IRC	TCP/ UDP	194	Internet Relay Chat	irc	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Telnet	TCP	23	Telnet Protocol	telnet	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	TFTP	UDP	Static (69) with inspection	Trivial File Transfer Protocol	tftp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	NNTP	TCP/ UDP	119	Network News Transfer Protocol	nntp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

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.

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Signaling	RSVP	UDP	1698, 1699	Resource Reservation Protocol	rsvp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
RPC	NFS	TCP/ UDP	2049	Network File System	nfs	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Sunrpc	TCP/ UDP	Dynamically Assigned	Sun Remote Procedure Call	sunrpc	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	MSN-messenger	TCP	1863	MSN Messenger Chat Messages[4]	msn-messenger	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	Yahoo-messenger	TCP	5050, 5101	Yahoo Messenger Chat Messages	yahoo-messenger	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	AOL-messenger	TCP	5190, 443	AOL Instant Messenger Chat Messages	aol-messenger	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
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 15.1(2)T
Misc.	NTP	TCP/ UDP	123	Network Time Protocol	ntp	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	Printer	TCP/ UDP	515	Printer	printer	12.1(2)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	X Windows	TCP	6000-6003	X11, X Windows	xwindows	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T

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.

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	r-commands	TCP	Dynamically Assigned	rsh, rlogin, rexec	rcmd	12.1(1)E 12.1(5)T 12.2(18)ZYA1 15.1(2)T
	AppleQTC	TCP/UDP	458	Apple Quick Time	appleqtc	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	Chargen	TCP/UDP	19	Character Generator	chargen	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	ClearCase	TCP/UDP	371	Clear Case Protocol Software Informer	clearcase	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
Corba	TCP/UDP	683, 684	Corba Internet Inter-Orb Protocol (IIOP)	corba-iiop	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
Daytime	TCP/UDP	13	Daytime Protocol	daytime	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
Doom	TCP/UDP	666	Doom	doom	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
Echo	TCP/UDP	7	Echo Protocol	echo	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
IBM DB2	TCP/UDP	523	IBM Information Management	ibm-db2	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
IPX	TCP/UDP	213	Internet Packet Exchange	ipx	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
ISAKMP	TCP/UDP	500	Internet Security Association and Key Management	isakmp	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
ISI-GL	TCP/UDP	55	Interoperable Self Installation	isi-gl	12.2(18)ZYA 12.2(18)ZYA1	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
			Graphics Language			
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	
3Com AMP3	TCP/UDP	629	3Com AMP3	3com-amp3	15.1(3)T	
3Com TSMUX	TCP/UDP	106	3Com TSMUX	3com-tsmux	15.1(3)T	
3PC	TCP/UDP	34	Third Party Connect Protocol	3pc	15.1(3)T	
914 C/G	TCP/UDP	211	Texas Instruments 914 Terminal	914c/g	15.1(3)T	
9PFS	TCP/UDP	564	Plan 9 file service	9pfs	15.1(3)T	
ACAP	TCP/UDP	674	ACAP	acap	15.1(3)T	
	ACAS	TCP/UDP	62	ACA Services	acas	15.1(3)T
	AccessBuilder	TCP/UDP	888	Access Builder	accessbuilder	15.1(3)T
AccessNetwork	TCP/UDP	699	Access Network	accessnetwork	15.1(3)T	
ACP	TCP/UDP	599	Aeolon Core Protocol	acp	15.1(3)T	
ACR-NEMA	TCP/UDP	104	ACR-NEMA Digital Img	acr-nema	15.1(3)T	
AED-512	TCP/UDP	149	AED 512 Emulation service	aed-512	15.1(3)T	
Agentx	TCP/UDP	705	AgentX	agentx	15.1(3)T	
Alpes	TCP/UDP	463	Alpes	alpes	15.1(3)T	
AMInet	TCP/UDP	2639	AMInet	aminet	15.1(3)T	
AN	TCP/UDP	107	Active Networks	an	15.1(3)T	
ANET	TCP/UDP	212	ATEXSSTR	anet	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
ANSANotify	TCP/UDP	116	ANSA REX Notify	ansanotify	15.1(3)T	
ANSATrader	TCP/UDP	124	ansatrader	ansatrader	15.1(3)T	
AODV	TCP/UDP	654	AODV	aodv	15.1(3)T	
Apertus-LDP	TCP/UDP	539	Apertus Tech Load Distribution	apertus-ldp	15.1(3)T	
AppleQTSRVR	TCP/UDP	545	appleqtcsrvr	appleqtcsrvr	15.1(3)T	
Applix	TCP/UDP	999	Applix ac	applix	15.1(3)T	
ARCISDMS	TCP/UDP	262	arcisdms	arcisdms	15.1(3)T	
ARGUS	TCP/UDP	13	ARGUS	argus	15.1(3)T	
Ariel1	TCP/UDP	419	Ariel1	ariel1	15.1(3)T	
	Ariel2	TCP/UDP	421	Ariel2	ariel2	15.1(3)T
	Ariel3	TCP/UDP	422	Ariel3	ariel3	15.1(3)T
ARIS	TCP/UDP	104	ARIS	aris	15.1(3)T	
ARNS	TCP/UDP	384	A remote network server system	arns	15.1(3)T	
ASA	TCP/UDP	386	ASA Message router object def	asa	15.1(3)T	
ASA-Appl-Proto	TCP/UDP	502	asa-appl-proto	asa-appl-proto	15.1(3)T	
ASIPRegistry	TCP/UDP	687	asipregistry	asipregistry	15.1(3)T	
ASIP-Webadmin	TCP/UDP	311	AppleShare IP WebAdmin	asip-webadmin	15.1(3)T	
AS-Servermap	TCP/UDP	449	AS Server Mapper	as-servermap	15.1(3)T	
AT-3	TCP/UDP	203	AppleTalk Unused	at-3	15.1(3)T	
AT-5	TCP/UDP	205	AppleTalk Unused	at-5	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
AT-7	TCP/UDP	207	AppleTalk Unused	at-7	15.1(3)T	
AT-8	TCP/UDP	208	AppleTalk Unused	at-8	15.1(3)T	
AT-Echo	TCP/UDP	204	AppleTalk Echo	at-echo	15.1(3)T	
AT-NBP	TCP/UDP	202	AppleTalk Name Binding	at-nbp	15.1(3)T	
AT-RTMP	TCP/UDP	201	AppleTalk Routing Maintenance	at-rtmp	15.1(3)T	
AT-ZIS	TCP/UDP	206	AppleTalk Zone Information	at-zis	15.1(3)T	
Audit	TCP/UDP	182	Unisys Audit SITP	audit	15.1(3)T	
Auditd	TCP/UDP	48	Digital Audit daemon	auditd	15.1(3)T	
Aurora-CMGR	TCP/UDP	364	Aurora CMGR	aurora-cmgr	15.1(3)T	
	AURP	TCP/UDP	387	Appletalk Update-Based Routing Pro.	aurp	15.1(3)T
	AUTH	TCP/UDP	113	Authentication Service	auth	15.1(3)T
Avian	TCP/UDP	486	avian	avian	15.1(3)T	
AX25	TCP/UDP	93	AX.25 Frames	ax25	15.1(3)T	
Banyan-RPC	TCP/UDP	567	banyan-rpc	banyan-rpc	15.1(3)T	
Banyan-VIP	TCP/UDP	573	banyan-vip	banyan-vip	15.1(3)T	
BBNRCCMON	TCP/UDP	10	BBN RCC Monitoring	bbnrccmon	15.1(3)T	
BDP	TCP/UDP	581	Bundle Discovery protocol	bdp	15.1(3)T	
BFTP	TCP/UDP	152	Background File Transfer Program	bftp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
BGMP	TCP/UDP	264	BGMP	bgmp	15.1(3)T	
BGP	TCP/UDP	179	Border Gateway Protocol	bgp	15.1(3)T	
BGS-NSI	TCP/UDP	482	bgs-nsi	bgs-nsi	15.1(3)T	
Bhevent	TCP/UDP	357	bhevent	bhevent	15.1(3)T	
BHFHS	TCP/UDP	248	bhfhs	bhfhs	15.1(3)T	
BHMDS	TCP/UDP	310	bhmds	bhmds	15.1(3)T	
BL-IDM	TCP/UDP	142	Britton Lee IDM	bl-idm	15.1(3)T	
BMPP	TCP/UDP	632	bmpp	bmpp	15.1(3)T	
BNA	TCP/UDP	49	BNA	bna	15.1(3)T	
Bnet	TCP/UDP	415	bnet	bnet	15.1(3)T	
Borland-DSJ	TCP/UDP	707	borland-dsj	borland-dsj	15.1(3)T	
	BR-SAT-Mon	TCP/UDP	76	Backroom SATNET Monitoring	br-sat-mon	15.1(3)T
	Cableport-AX	TCP/UDP	282	Cable Port A/X	cableport-ax	15.1(3)T
Cab-Protocol	TCP/UDP	595	CAB Protocol	cab-protocol	15.1(3)T	
Cadlock	TCP/UDP	770	cadlock	cadlock	15.1(3)T	
CAIlic	TCP/UDP	216	Computer Associates Intl License Server	CAIlic	15.1(3)T	
CBT	TCP/UDP	7	CBT	cbt	15.1(3)T	
CDC	TCP/UDP	223	Certificate Distribution Center	cdc	15.1(3)T	
CFDPTKT	TCP/UDP	120	cfdptkt	cfdptkt	15.1(3)T	
CFTP	TCP/UDP	62	CFTP	cftp	15.1(3)T	
CHAOS	TCP/UDP	16	Chaos	chaos	15.1(3)T	
ChShell	TCP/UDP	562	chcmd	chshell	15.1(3)T	
Cimplex	TCP/UDP	673	cimplex	cimplex	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Cisco-FNA	TCP/UDP	130	cisco FNATIVE	cisco-fna	15.1(3)T	
Cisco-SYS	TCP/UDP	132	cisco SYSMAINT	cisco-sys	15.1(3)T	
Cisco-TDP	TCP/UDP	711	Cisco TDP	cisco-tdp	15.1(3)T	
Cisco-TNA	TCP/UDP	131	cisco TNATIVE	cisco-tna	15.1(3)T	
Cloanto-Net-1	TCP/UDP	356	cloanto-net-1	cloanto-net-1	15.1(3)T	
CMIP-Agent	TCP/UDP	164	CMIP/TCP Agent	cmip-agent	15.1(3)T	
CMIP-Man	TCP/UDP	163	CMIP/TCP Manager	cmip-man	15.1(3)T	
Coauthor	TCP/UDP	1529	oracle	coauthor	15.1(3)T	
	Codaauth2	TCP/UDP	370	codaauth2	codaauth2	15.1(3)T
	Collaborator	TCP/UDP	622	collaborator	collaborator	15.1(3)T
Commerce	TCP/UDP	542	commerce	commerce	15.1(3)T	
Compaq-Peer	TCP/UDP	110	Compaq Peer Protocol	compaq-peer	15.1(3)T	
Compressnet	TCP/UDP	2	Management Utility	compressnet	15.1(3)T	
COMSCM	TCP/UDP	437	comscm	comscm	15.1(3)T	
CON	TCP/UDP	759	con	con	15.1(3)T	
Conference	TCP/UDP	531	chat	conference	15.1(3)T	
Connendp	TCP/UDP	693	almanid Connection Endpoint	connendp	15.1(3)T	
ContentServer	TCP/UDP	3365	contentserver	contentserver	15.1(3)T	
CoreRJD	TCP/UDP	284	corerjd	corerjd	15.1(3)T	
Courier	TCP/UDP	530	rpc	courier	15.1(3)T	
Covia	TCP/UDP	64	Communications Integrator	covia	15.1(3)T	
CPHB	TCP/UDP	73	Computer Protocol Heart Beat	cphb	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
CPNX	TCP/UDP	72	Computer Protocol Network Executive	cpnx	15.1(3)T	
Creativepartnr	TCP/UDP	455	creativepartnr	creativepartnr	15.1(3)T	
Creativeserver	TCP/UDP	453	creativeserver	creativeserver	15.1(3)T	
CRS	TCP/UDP	507	crs	crs	15.1(3)T	
CRTP	TCP/UDP	126	Combat Radio Transport Protocol	crtp	15.1(3)T	
CRUDP	TCP/UDP	127	Combat Radio User Datagram	crudp	15.1(3)T	
	CryptoAdmin	TCP/UDP	624	Crypto Admin	cryptoadmin	15.1(3)T
	CSI-SGWP	TCP/UDP	348	Cabletron Management Protocol	csi-sgwp	15.1(3)T
CSNET-NS	TCP/UDP	105	Mailbox Name Nameserver	csnet-ns	15.1(3)T	
CTF	TCP/UDP	84	Common Trace Facility	ctf	15.1(3)T	
CUSTIX	TCP/UDP	528	Customer Ixchange	custix	15.1(3)T	
CVC_Hostd	TCP/UDP	442	cvc_hostd	cvc_hostd	15.1(3)T	
Cybercash	TCP/UDP	551	cybercash	cybercash	15.1(3)T	
Cycleserv	TCP/UDP	763	cycleserv	cycleserv	15.1(3)T	
Cycleserv2	TCP/UDP	772	cycleserv2	cycleserv2	15.1(3)T	
Dantz	TCP/UDP	497	dantz	dantz	15.1(3)T	
DASP	TCP/UDP	439	dasp	dasp	15.1(3)T	
DataSurfSRV	TCP/UDP	461	DataRamp Svr	datasurfsrv	15.1(3)T	
DataSurfSRVSec	TCP/UDP	462	DataRamp Svr svs	datasurfsrvsec	15.1(3)T	
Datex-ASN	TCP/UDP	355	datex-asn	datex-asn	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Dbase	TCP/UDP	217	dBASE Unix	dbase	15.1(3)T	
DCCP	TCP/UDP	33	Datagram Congestion Control Protocol	dccp	15.1(3)T	
DCN-Meas	TCP/UDP	19	DCN Measurement Subsystems	dcn-meas	15.1(3)T	
DCP	TCP/UDP	93	Device Control Protocol	dcp	15.1(3)T	
DCTP	TCP/UDP	675	dctp	dctp	15.1(3)T	
DDM-DFM	TCP/UDP	447	DDM Distributed File management	ddm-dfm	15.1(3)T	
	DDM-RDB	TCP/UDP	446	DDM-Remote Relational Database Access	ddm-rdb	15.1(3)T
DDM-SSL	TCP/UDP	448	DDM-Remote DB Access Using Secure Sockets	ddm-ssl	15.1(3)T	
DDP	TCP/UDP	37	Datagram Delivery Protocol	ddp	15.1(3)T	
DDX	TCP/UDP	116	D-II Data Exchange	ddx	15.1(3)T	
DEC_DLM	TCP/UDP	625	dec_dlm	dec_dlm	15.1(3)T	
Decap	TCP/UDP	403	decap	decap	15.1(3)T	
Decauth	TCP/UDP	316	decauth	decauth	15.1(3)T	
Decbsrv	TCP/UDP	579	decbsrv	decbsrv	15.1(3)T	
Decladebug	TCP/UDP	410	DECLadebug Remote Debug Protocol	decladebug	15.1(3)T	
Decvms-sysmgt	TCP/UDP	441	decvms-sysmgt	decvms-sysmgt	15.1(3)T	
DEI-ICDA	TCP/UDP	618	dei-icda	dei-icda	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
DEOS	TCP/UDP	76	Distributed External Object Store	deos	15.1(3)T	
Device	TCP/UDP	801	device	device	15.1(3)T	
DGP	TCP/UDP	86	Dissimilar Gateway Protocol	dgp	15.1(3)T	
DHCP-Failover	TCP/UDP	647	DHCP Failover	dhcp-failover	15.1(3)T	
DHCP-Failover2	TCP/UDP	847	dhcp-failover2	dhcp-failover2	15.1(3)T	
DHCPv6-client	TCP/UDP	546	DHCPv6 Client	dhcpv6-client	15.1(3)T	
DHCPv6-server	TCP/UDP	547	DHCPv6 Server	dhcpv6-server	15.1(3)T	
Digital-VRC	TCP/UDP	466	digital-vrc	digital-vrc	15.1(3)T	
	Directplay	TCP/UDP	2234	DirectPlay	directplay	15.1(3)T
Directplay8	TCP/UDP	6073	DirectPlay8	directplay8	15.1(3)T	
Directv-Catlg	TCP/UDP	3337	Direct TV Data Catalog	directv-catlg	15.1(3)T	
Directv-Soft	TCP/UDP	3335	Direct TV Software Updates	directv-soft	15.1(3)T	
Directv-Tick	TCP/UDP	3336	Direct TV Tickers	directv-tick	15.1(3)T	
Directv-Web	TCP/UDP	3334	Direct TV Webcasting	directv-web	15.1(3)T	
Discard	TCP/UDP	9	Discard	discard	15.1(3)T	
Disclose	TCP/UDP	667	campaign contribution disclosures	disclose	15.1(3)T	
Dixie	TCP/UDP	96	DIXIE Protocol Specification	dixie	15.1(3)T	
DLS	TCP/UDP	197	Directory Location Service	dls	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
DLS-Mon	TCP/UDP	198	Directory Location Service Monitor	dls-mon	15.1(3)T	
DN6-NLM-AUD	TCP/UDP	195	DNSIX Network Level Module Audit	dn6-nlm-aud	15.1(3)T	
DNA-CML	TCP/UDP	436	DNA-CML	dna-cml	15.1(3)T	
DNS	TCP/UDP	53	Domain Name Server lookup	dns	15.1(3)T	
DNSIX	TCP/UDP	90	DNSIX Securit Attribute Token Map	dnsix	15.1(3)T	
DPSI	TCP/UDP	315	dpsi	dpsi	15.1(3)T	
DSFGW	TCP/UDP	438	dsfgw	dsfgw	15.1(3)T	
DSP	TCP/UDP	33	Display Support Protocol	dsp	15.1(3)T	
DSP3270	TCP/UDP	246	Display Systems Protocol	dsp3270	15.1(3)T	
	DSR	TCP/UDP	48	Dynamic Source Routing Protocol	dsr	15.1(3)T
DTAG-DTE-SB	TCP/UDP	352	DTAG	dtag-ste-sb	15.1(3)T	
DTK	TCP/UDP	365	dtk	dtk	15.1(3)T	
DWR	TCP/UDP	644	dwr	dwr	15.1(3)T	
EGP	TCP/UDP	8	Exterior Gateway Protocol	egp	15.1(3)T	
EIGRP	TCP/UDP	88	Enhanced Interior Gateway Routing Protocol	eigrp	15.1(3)T	
ELCSD	TCP/UDP	704	errlog copy/ server daemon	elcsd	15.1(3)T	
EMBL-NDT	TCP/UDP	394	EMBL Nucleic Data Transfer	embl-ndt	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
EMCON	TCP/UDP	14	EMCON	emcon	15.1(3)T	
EMFIS-CNTLl	TCP/UDP	141	EMFIS Control Service	emfis-cntl	15.1(3)T	
EMFIS-Data	TCP/UDP	140	EMFIS Data Service	emfis-data	15.1(3)T	
Encap	TCP/UDP	98	Encapsulation Header	encap	15.1(3)T	
Entomb	TCP/UDP	775	entomb	entomb	15.1(3)T	
Entrust-AAAS	TCP/UDP	680	entrust-aaas	entrust-aaas	15.1(3)T	
Entrust-AAMS	TCP/UDP	681	entrust-aams	entrust-aams	15.1(3)T	
Entrust-ASH	TCP/UDP	710	Entrust Administration Service Handler	entrust-ash	15.1(3)T	
Entrust-KMSH	TCP/UDP	709	Entrust Key Management Service Handler	entrust-kmsh	15.1(3)T	
Entrust-SPS	TCP/UDP	640	entrust-sps	entrust-sps	15.1(3)T	
ERPC	TCP/UDP	121	Encore Expedited Remote Pro.Call	erpc	15.1(3)T	
	ESCP-IP	TCP/UDP	621	escp-ip	escp-ip	15.1(3)T
	ESRO-GEN	TCP/UDP	259	Efficient Short Remote Operations	esro-gen	15.1(3)T
ESRP-EMSDP	TCP/UDP	642	ESRO-EMSDP V1.3	esro-emsdp	15.1(3)T	
EtherIP	TCP/UDP	97	Ethernet-within-IP Encapsulation	etherip	15.1(3)T	
Eudora-Set	TCP/UDP	592	Eudora Set	eudora-set	15.1(3)T	
EXEC	TCP/UDP	512	remote process execution;	exec	15.1(3)T	
Fatserv	TCP/UDP	347	Fatmen Server	fatserv	15.1(3)T	
FC	TCP/UDP	133	Fibre Channel	fc	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
FCP	TCP/UDP	510	FirstClass Protocol	fcp	15.1(3)T	
Finger	TCP/UDP	79	Finger	finger	15.1(3)T	
FIRE	TCP/UDP	125	FIRE	fire	15.1(3)T	
FlexLM	TCP/UDP	744	Flexible License Manager	flexlm	15.1(3)T	
FLN-SPX	TCP/UDP	221	Berkeley rlogind with SPX auth	fln-spx	15.1(3)T	
FTP-Agent	TCP/UDP	574	FTP Software Agent System	ftp-agent	15.1(3)T	
FTP-Data	TCP/UDP	20	File Transfer	ftp-data	15.1(3)T	
FTPS-Data	TCP/UDP	989	ftp protocol, data, over TLS/ SSL	ftps-data	15.1(3)T	
Fujitsu-Dev	TCP/UDP	747	Fujitsu Device Control	fujitsu-dev	15.1(3)T	
GACP	TCP/UDP	190	Gateway Access Control Protocol	gacp	15.1(3)T	
GDOMAP	TCP/UDP	538	gdomap	gdomap	15.1(3)T	
Genie	TCP/UDP	402	Genie Protocol	genie	15.1(3)T	
	Genrad-MUX	TCP/UDP	176	genrad-mux	genrad-mux	15.1(3)T
	GGF-NCP	TCP/UDP	678	GNU Generation Foundation NCP	ggf-ncp	15.1(3)T
GGP	TCP/UDP	3	Gateway-to-Gateway	ggp	15.1(3)T	
Ginad	TCP/UDP	634	ginad	ginad	15.1(3)T	
GMTP	TCP/UDP	100	GMTP	gmtp	15.1(3)T	
Go-Login	TCP/UDP	491	go-login	go-login	15.1(3)T	
Gopher	TCP/UDP	70	Gopher	gopher	15.1(3)T	
Graphics	TCP/UDP	41	Graphics	graphics	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
GRE	TCP/UDP	47	General Routing Encapsulation	gre	15.1(3)T	
Groove	TCP/UDP	2492	groove	groove	15.1(3)T	
GSS-HTTP	TCP/UDP	488	gss-http	gss-http	15.1(3)T	
GSS-XLICEN	TCP/UDP	128	GNU Generation Foundation NCP	gss-xlicen	15.1(3)T	
GTP-User	TCP/UDP	2152	GTP-User Plane	gtp-user	15.1(3)T	
HA-Cluster	TCP/UDP	694	ha-cluster	ha-cluster	15.1(3)T	
HAP	TCP/UDP	661	hap	hap	15.1(3)T	
Hassle	TCP/UDP	375	hassle	hassle	15.1(3)T	
HCP-Wismar	TCP/UDP	686	Hardware Control Protocol Wismar	hcp-wismar	15.1(3)T	
HDAP	TCP/UDP	263	hdap	hdap	15.1(3)T	
Hello-port	TCP/UDP	652	HELLO_PORT	hello-port	15.1(3)T	
HEMS	TCP/UDP	151	hems	hems	15.1(3)T	
	HIP	TCP/UDP	139	Host Identity Protocol	hip	15.1(3)T
	HMMP-IND	TCP/UDP	612	HMMP Indication	hmmp-ind	15.1(3)T
HMMP-OP	TCP/UDP	613	HMMP Operation	hmmp-op	15.1(3)T	
HMP	TCP/UDP	20	Host Monitoring	hmp	15.1(3)T	
HOPOPT	TCP/UDP	0	IPv6 Hop-by-Hop Option	hopopt	15.1(3)T	
Hostname	TCP/UDP	101	NIC Host Name Server	hostname	15.1(3)T	
HP-Alarm-Mgr	TCP/UDP	383	hp performance data alarm manager	hp-alarm-mgr	15.1(3)T	
HP-Collector	TCP/UDP	381	hp performance data collector	hp-collector	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
HP-Managed-Node	TCP/UDP	382	hp performance data managed node	hp-managed-node	15.1(3)T	
HTTP-ALT	TCP/UDP	8080	HTTP Alternate	http-alt	15.1(3)T	
HTTP-Mgmt	TCP/UDP	280	http-mgmt	http-mgmt	15.1(3)T	
HTTP-RPC-EPMAP	TCP/UDP	593	HTTP RPC Ep Map	http-rpc-epmap	15.1(3)T	
Hybrid-POP	TCP/UDP	473	hybrid-pop	hybrid-pop	15.1(3)T	
Hyper-G	TCP/UDP	418	hyper-g	hyper-g	15.1(3)T	
Hyperwave-ISP	TCP/UDP	692	hyperwave-isp	hyperwave-isp	15.1(3)T	
IAFDBase	TCP/UDP	480	iafdbase	iafdbase	15.1(3)T	
IAFServer	TCP/UDP	479	iafserver	iafserver	15.1(3)T	
IASD	TCP/UDP	432	iasd	iasd	15.1(3)T	
IATP	TCP/UDP	117	Interactive Agent Transfer Protocol	iatp	15.1(3)T	
IBM-App	TCP/UDP	385	IBM Application	ibm-app	15.1(3)T	
	IBM-DB2	TCP/UDP	523	IBM-DB2	ibm-db2	15.1(3)T
IBProtocol	TCP/UDP	6714	Internet Backplane Protocol	ibprotocol	15.1(3)T	
ICLCNet-Locate	TCP/UDP	886	ICL coNETion locate server	iclcnet-locate	15.1(3)T	
ICLNet_SVInfo	TCP/UDP	887	ICL coNETion server info	iclcnet_svinfo	15.1(3)T	
ICMP	TCP/UDP	1	Internet Control Message	icmp	15.1(3)T	
IDFP	TCP/UDP	549	idfp	idfp	15.1(3)T	
IDPR	TCP/UDP	35	Inter-Domain Policy Routing Protocol	idpr	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
IDPRr-CMTP	TCP/UDP	38	IDPR Control Message Transport Proto	idpr-cmtp	15.1(3)T	
IDRP	TCP/UDP	45	Inter-Domain Routing Protocol	idrp	15.1(3)T	
IEEE-MMS	TCP/UDP	651	ieee-mms	ieee-mms	15.1(3)T	
IEEE-MMS-SSL	TCP/UDP	695	ieee-mms-ssl	ieee-mms-ssl	15.1(3)T	
IFMP	TCP/UDP	101	Ipsilon Flow Management Protocol	ifmp	15.1(3)T	
IGRP	TCP/UDP	9	Cisco interior gateway	igrp	15.1(3)T	
IIOP	TCP/UDP	535	iiop	iiop	15.1(3)T	
IL	TCP/UDP	40	IL Transport Protocol	il	15.1(3)T	
IMSP	TCP/UDP	406	Interactive Mail Support Protocol	imsp	15.1(3)T	
InBusiness	TCP/UDP	244	inbusiness	inbusiness	15.1(3)T	
Infoseek	TCP/UDP	414	InfoSeek	infoseek	15.1(3)T	
Ingres-Net	TCP/UDP	134	INGRES-NET Service	ingres-net	15.1(3)T	
	I-NLSP	TCP/UDP	52	Integrated Net Layer Security TUBA	i-nlsp	15.1(3)T
Intecourier	TCP/UDP	495	intecourier	intecourier	15.1(3)T	
Integra-SME	TCP/UDP	484	Integra Software Management Environment	integra-sme	15.1(3)T	
Intrinsia	TCP/UDP	503	intrinsa	intrinsa	15.1(3)T	
IPCD	TCP/UDP	576	ipcd	ipcd	15.1(3)T	
IPComp	TCP/UDP	108	IP Payload Compression Protocol	ipcomp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
IPCServer	TCP/UDP	600	Sun IPC server	ipcserver	15.1(3)T	
IPCV	TCP/UDP	71	Internet Packet Core Utility	ipcv	15.1(3)T	
IPDD	TCP/UDP	578	ipdd	ipdd	15.1(3)T	
IPINIP	TCP/UDP	4	IP in IP	ipinip	15.1(3)T	
IPIP	TCP/UDP	94	IP-within-IP Encapsulation Protocol	ipip	15.1(3)T	
IPLT	TCP/UDP	129	IPLT	iplt	15.1(3)T	
IPP	TCP/UDP	631	Internet Printing Protocol	ipp	15.1(3)T	
IPPC	TCP/UDP	67	Internet Pluribus Packet Core	ippc	15.1(3)T	
Ipv6-Frag	TCP/UDP	44	Fragment Header for IPv6	ipv6-frag	15.1(3)T	
Ipv6-ICMP	TCP/UDP	58	ICMP for IPv6	ipv6-icmp	15.1(3)T	
Ipv6INIP	TCP/UDP	41	Ipv6 encapsulated	ipv6inip	15.1(3)T	
ipv6-NonXT	TCP/UDP	59	No Next Header for IPv6	ipv6-nonxt	15.1(3)T	
Ipv6-OPTS	TCP/UDP	60	Destination Options for IPv6	ipv6-opts	15.1(3)T	
	Ipv6-Route	TCP/UDP	43	Routing Header for IPv6	ipv6-route	15.1(3)T
IRC	TCP/UDP	194	Internet Relay Chat	irc	15.1(3)T	
IRC-SERV	TCP/UDP	529	IRC-SERV	irc-serv	15.1(3)T	
IRTP	TCP/UDP	28	Internet Reliable Transaction	irtp	15.1(3)T	
IS99C	TCP/UDP	379	TIA/EIA/IS-99 modem client	is99c	15.1(3)T	
IS99S	TCP/UDP	380	TIA/EIA/IS-99 modem server	is99s	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
ISAKMP	TCP/UDP	500	Internet Security Association & Key Management Protocol	isakmp	15.1(3)T	
ISIS	TCP/UDP	124	ISIS over IPv4	isis	15.1(3)T	
ISO-ILL	TCP/UDP	499	ISO ILL Protocol	iso-ill	15.1(3)T	
ISO-IP	TCP/UDP	147	iso-ip	iso-ip	15.1(3)T	
ISO-TP0	TCP/UDP	146	iso-tp0	iso-tp0	15.1(3)T	
ISO-TP4	TCP/UDP	29	ISO Transport Protocol Class 4	iso-tp4	15.1(3)T	
ISO-TSAP	TCP/UDP	102	ISO-TSAP Class 0	iso-tsap	15.1(3)T	
ISO-TSAP-C2	TCP/UDP	399	ISO Transport Class 2 Non-Control	iso-tsap-c2	15.1(3)T	
ITM-MCELL-S	TCP/UDP	828	itm-mcell-s	itm-mcell-s	15.1(3)T	
IXP-IN-IP	TCP/UDP	111	IPX in IP	ixp-in-ip	15.1(3)T	
Jargon	TCP/UDP	148	Jargon	jargon	15.1(3)T	
Kali	TCP/UDP	2213	kali	kali	15.1(3)T	
K-Block	TCP/UDP	287	k-block	k-block	15.1(3)T	
	Keyserver	TCP/UDP	584	Key Server	keyserver	15.1(3)T
	KIS	TCP/UDP	186	KIS Protocol	kis	15.1(3)T
	Knet-CMP	TCP/UDP	157	KNET/VM Command/ Message Protocol	knet-cmp	15.1(3)T
	Konspire2b	TCP/UDP	6085	konspire2b p2p network	Konspire2b	15.1(3)T
	Kpasswd	TCP/UDP	464	kpasswd	kpasswd	15.1(3)T
	Kryptolan	TCP/UDP	398	kryptolan	kryptolan	15.1(3)T
	L2TP	TCP/UDP	1701	l2tp	l2tp	15.1(3)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	LA-Maint	TCP/UDP	51	IMP Logical Address Maintenance	la-maint	15.1(3)T
	LANServer	TCP/UDP	637	lanserver	lanserver	15.1(3)T
	LARP	TCP/UDP	91	Locus Address Resolution Protocol	larp	15.1(3)T
	LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	15.1(3)T
	LDP	TCP/UDP	646	LDP	ldp	15.1(3)T
	Leaf-1	TCP/UDP	25	Leaf-1	leaf-1	15.1(3)T
	Leaf-2	TCP/UDP	26	Leaf-2	leaf-2	15.1(3)T
	Legent-1	TCP/UDP	373	Legent Corporation	legent-1	15.1(3)T
	Legent-2	TCP/UDP	374	Legent Corporation	legent-2	15.1(3)T
	LJK-Login	TCP/UDP	472	ljk-login	ljk-login	15.1(3)T
	Locus-Con	TCP/UDP	127	Locus PC-Interface Conn Server	locus-con	15.1(3)T
	Locus-Map	TCP/UDP	125	Locus PC-Interface Net Map Ser	locus-map	15.1(3)T
	MAC-SRVR-Admin	TCP/UDP	660	MacOS Server Admin	mac-srvr-admin	15.1(3)T
	Magenta-Logic	TCP/UDP	313	magenta-logic	magenta-logic	15.1(3)T
Mailbox-LM	TCP/UDP	505	mailbox-lm	mailbox-lm	15.1(3)T	
Mailq	TCP/UDP	174	MAILQ	mailq	15.1(3)T	
Maitrd	TCP/UDP	997	maitrd	maitrd	15.1(3)T	
MANET	TCP/UDP	138	MANET Protocols	manet	15.1(3)T	
MasqDialer	TCP/UDP	224	masqdialer	masqdialer	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Matip-Type-A	TCP/UDP	350	MATIP Type A	matip-type-a	15.1(3)T	
Matip-Type-B	TCP/UDP	351	MATIP Type B	matip-type-b	15.1(3)T	
MCIDAS	TCP/UDP	112	McIDAS Data Transmission Protocol	mcidas	15.1(3)T	
MCNS-Sec	TCP/UDP	638	mcns-sec	mcns-sec	15.1(3)T	
MDC-Portmapper	TCP/UDP	685	mdc-portmapper	mdc-portmapper	15.1(3)T	
MeComm	TCP/UDP	668	mecomm	mecomm	15.1(3)T	
MeRegister	TCP/UDP	669	meregister	meregister	15.1(3)T	
Merit-INP	TCP/UDP	32	MERIT Internodal Protocol	merit-inp	15.1(3)T	
Meta5	TCP/UDP	393	meta5	meta5	15.1(3)T	
Metagram	TCP/UDP	99	metagram	metagram	15.1(3)T	
Meter	TCP/UDP	570	meter	meter	15.1(3)T	
Mfcobol	TCP/UDP	86	Micro Focus Cobol	mfcobol	15.1(3)T	
MFE-NSP	TCP/UDP	31	MFE Network Services Protocol	mfe-nsp	15.1(3)T	
	MFTP	TCP/UDP	349	mftp	mftp	15.1(3)T
	Micom-PFS	TCP/UDP	490	micom-pfs	micom-pfs	15.1(3)T
MICP	TCP/UDP	95	Mobile Internetworking Control Pro.	micp	15.1(3)T	
Micromuse-LM	TCP/UDP	1534	micromuse-lm	micromuse-lm	15.1(3)T	
MIT-DOV	TCP/UDP	91	MIT Dover Spooler	mit-dov	15.1(3)T	
MIT-ML-Dev	TCP/UDP	83	MIT ML Device	mit-ml-dev	15.1(3)T	
Mobile	TCP/UDP	55	IP Mobility	mobile	15.1(3)T	
MobileIP-Agent	TCP/UDP	434	mobileip-agent	mobileip-agent	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
MobilIP-MN	TCP/UDP	435	mobilip-mn	mobilip-mn	15.1(3)T	
Mondex	TCP/UDP	471	mondex	mondex	15.1(3)T	
Monitor	TCP/UDP	561	monitor	monitor	15.1(3)T	
Mortgageware	TCP/UDP	367	mortgageware	mortgageware	15.1(3)T	
MPLS-IN-IP	TCP/UDP	137	MPLS-in-IP	mpls-in-ip	15.1(3)T	
MPM	TCP/UDP	45	Message Processing Module	mpm	15.1(3)T	
MPM-Flags	TCP/UDP	44	MPM FLAGS Protocol	mpm-flags	15.1(3)T	
MPM-SND	TCP/UDP	46	MPM [default send]	mpm-snd	15.1(3)T	
MPP	TCP/UDP	218	Netix Message Posting Protocol	mpp	15.1(3)T	
MPTN	TCP/UDP	397	Multi Protocol Trans. Net	mptn	15.1(3)T	
MRM	TCP/UDP	679	mrm	mrm	15.1(3)T	
MSDP	TCP/UDP	639	msdp	msdp	15.1(3)T	
	MSExch-Routing	TCP/UDP	691	MS Exchange Routing	msexch-routing	15.1(3)T
	MSFT-GC	TCP/UDP	3268	Microsoft Global Catalog	msft-gc	15.1(3)T
MSFT-GC-SSL	TCP/UDP	3269	Microsoft Global Catalog with LDAP/SSL	msft-gc-ssl	15.1(3)T	
MSG-AUTH	TCP/UDP	31	msg-auth	msg-auth	15.1(3)T	
MSG-ICP	TCP/UDP	29	msg-icp	msg-icp	15.1(3)T	
MSNP	TCP/UDP	1863	msnp	msnp	15.1(3)T	
MS-OLAP	TCP/UDP	2393	Microsoft OLAP	ms-olap	15.1(3)T	
MSP	TCP/UDP	18	Message Send Protocol	msp	15.1(3)T	
MS-Rome	TCP/UDP	569	microsoft rome	ms-rome	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
MS-Shuttle	TCP/UDP	568	microsoft shuttle	ms-shuttle	15.1(3)T	
MS-SQLl-M	TCP/UDP	1434	Microsoft-SQL-Monitor	ms-sql-m	15.1(3)T	
MTP	TCP/UDP	92	Multicast Transport Protocol	mtp	15.1(3)T	
Multiling-HTTP	TCP/UDP	777	Multiling HTTP	multiling-http	15.1(3)T	
Multiplex	TCP/UDP	171	Network Innovations Multiplex	multiplex	15.1(3)T	
Mumps	TCP/UDP	188	Plus Fives MUMPS	mumps	15.1(3)T	
MUX	TCP/UDP	18	Multiplexing	mux	15.1(3)T	
Mylex-MAPD	TCP/UDP	467	mylex-mapd	mylex-mapd	15.1(3)T	
MySQL	TCP/UDP	3306	MySQL	mysql	15.1(3)T	
Name	TCP/UDP	42	Host Name Server	name	15.1(3)T	
NAMP	TCP/UDP	167	namp	namp	15.1(3)T	
	NARP	TCP/UDP	54	NBMA Address Resolution Protocol	narp	15.1(3)T
	NAS	TCP/UDP	991	Netnews Administration System	nas	15.1(3)T
NCED	TCP/UDP	404	nced	nced	15.1(3)T	
NCLD	TCP/UDP	405	ncld	ncld	15.1(3)T	
NCP	TCP/UDP	524	NCP	ncp	15.1(3)T	
NDSAuth	TCP/UDP	353	NDSAUTH	ndsauth	15.1(3)T	
Nest-Protocol	TCP/UDP	489	nest-protocol	nest-protocol	15.1(3)T	
Net8-CMAN	TCP/UDP	1830	Oracle Net8 CMan Admin	net8-cman	15.1(3)T	
Net-Assistant	TCP/UDP	3283	net-assistant	net-assistant	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Netblt	TCP/UDP	30	Bulk Data Transfer Protocol	netblt	15.1(3)T	
NetGW	TCP/UDP	741	netgw	netgw	15.1(3)T	
NetNews	TCP/UDP	532	readnews	netnews	15.1(3)T	
NetRCS	TCP/UDP	742	Network based RCS	netrcs	15.1(3)T	
NetRJS-1	TCP/UDP	71	Remote Job Service	netrjs-1	15.1(3)T	
NetRJS-2	TCP/UDP	72	Remote Job Service	netrjs-2	15.1(3)T	
NetRJS-3	TCP/UDP	73	Remote Job Service	netrjs-3	15.1(3)T	
NetRJS-4	TCP/UDP	74	Remote Job Service	netrjs-4	15.1(3)T	
NETSC-Dev	TCP/UDP	155	NETSC	netsc-dev	15.1(3)T	
NETSC-Prod	TCP/UDP	154	NETSC	netsc-prod	15.1(3)T	
NetViewDM1	TCP/UDP	729	IBM NetView DM	netviewdm1	15.1(3)T	
	NetviewDM2	TCP/UDP	730	IBM NetView DM	netviewdm2	15.1(3)T
	NetviewDM3	TCP/UDP	731	IBM NetView DM	netviewdm3	15.1(3)T
Netwall	TCP/UDP	533	for emergency broadcasts	netwall	15.1(3)T	
Netware-IP	TCP/UDP	396	Novell Netware over IP	netware-ip	15.1(3)T	
New-RWHO	TCP/UDP	550	new who	new-rwho	15.1(3)T	
NextStep	TCP/UDP	178	NextStep Window Server	nextstep	15.1(3)T	
NFS	TCP/UDP	2049	Network File System	nfs	15.1(3)T	
NicName	TCP/UDP	43	Who Is	nicname	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
NI-FTP	TCP/UDP	47	NI FTP	ni-ftp	15.1(3)T	
NI-Mail	TCP/UDP	61	NI MAIL	ni-mail	15.1(3)T	
Nlogin	TCP/UDP	758	nlogin	nlogin	15.1(3)T	
NMAP	TCP/UDP	689	nmap	nmap	15.1(3)T	
NMSP	TCP/UDP	537	Networked Media Streaming Protocol	nmsp	15.1(3)T	
NNSP	TCP/UDP	433	nnsp	nnsp	15.1(3)T	
Notes	TCP/UDP	1352	Lotus Notes(R)	notes	15.1(3)T	
NovaStorBakcup	TCP/UDP	308	Novastor Backup	novastorbakcup	15.1(3)T	
NPMP-GUI	TCP/UDP	611	npmp-gui	npmp-gui	15.1(3)T	
NPMP-Local	TCP/UDP	610	npmp-local	npmp-local	15.1(3)T	
NPMP-Trap	TCP/UDP	609	npmp-trap	npmp-trap	15.1(3)T	
NQS	TCP/UDP	607	nqs	nqs	15.1(3)T	
	NS	TCP/UDP	760	ns	ns	15.1(3)T
NSFNET-IGP	TCP/UDP	85	NSFNET-IGP	nsfnet-igp	15.1(3)T	
NSIIOPS	TCP/UDP	261	IIOP Name Service over TLS/SSL	nsiiops	15.1(3)T	
NSRMP	TCP/UDP	359	Network Security Risk Management Protocol	nsrmp	15.1(3)T	
NSS-Routing	TCP/UDP	159	NSS-Routing	nss-routing	15.1(3)T	
NSW-FE	TCP/UDP	27	NSW User System FE	nsw-fe	15.1(3)T	
Ntalk	TCP/UDP	518	ntalk	ntalk	15.1(3)T	
NTP	TCP/ UDP	123	Network Time Protocol	ntp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
NVP-II	TCP/UDP	11	Network Voice Protocol	nvp-ii	15.1(3)T	
NXEdit	TCP/UDP	126	nxedit	nxedit	15.1(3)T	
OBCBinder	TCP/UDP	183	ocbinder	ocbinder	15.1(3)T	
OBEX	TCP/UDP	650	obex	obex	15.1(3)T	
ObjCall	TCP/UDP	94	Tivoli Object Dispatcher	objcall	15.1(3)T	
OCS_AMU	TCP/UDP	429	ocs_amu	ocs_amu	15.1(3)T	
OCS_CMU	TCP/UDP	428	ocs_cmu	ocs_cmu	15.1(3)T	
OCServer	TCP/UDP	184	ocserver	ocserver	15.1(3)T	
ODMR	TCP/UDP	366	odmr	odmr	15.1(3)T	
OHIMSRV	TCP/UDP	506	ohimsrv	ohimsrv	15.1(3)T	
OLSR	TCP/UDP	698	olsr	olsr	15.1(3)T	
	OMGInitialRefs	TCP/UDP	900	omginitialrefs	omginitialrefs	15.1(3)T
	OMServ	TCP/UDP	764	omserv	omserv	15.1(3)T
ONMUX	TCP/UDP	417	onmux	onmux	15.1(3)T	
Opalis-RDV	TCP/UDP	536	opalis-rdv	opalis-rdv	15.1(3)T	
Opalis-Robot	TCP/UDP	314	opalis-robot	opalis-robot	15.1(3)T	
OPC-Job-Start	TCP/UDP	423	IBM Operations Planning and Control Start	opc-job-start	15.1(3)T	
OPC-Job-Track	TCP/UDP	424	IBM Operations Planning and Control Track	opc-job-track	15.1(3)T	
Openport	TCP/UDP	260	openport	openport	15.1(3)T	
OpenVMS-Sysipc	TCP/UDP	557	openvms-sysipc	openvms-sysipc	15.1(3)T	
OracleNames	TCP/UDP	1575	oraclenames	oraclenames	15.1(3)T	
OracleNet8CMAN	TCP/UDP	1630	Oracle Net8 Cman	oraclenet8cman	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
ORA-Srv	TCP/UDP	1525	Oracle TCP/IP Listener	ora-srv	15.1(3)T	
Orbix-Config	TCP/UDP	3076	Orbix 2000 Config	orbix-config	15.1(3)T	
Orbix-Locator	TCP/UDP	3075	Orbix 2000 Locator	orbix-locator	15.1(3)T	
Orbix-Loc-SSL	TCP/UDP	3077	Orbix 2000 Locator SSL	orbix-loc-ssl	15.1(3)T	
OSPF	TCP/UDP	89	Open Shortest Path First	ospf	15.1(3)T	
OSU-NMS	TCP/UDP	192	OSU Network Monitoring System	osu-nms	15.1(3)T	
Parsec-Game	TCP/UDP	6582	Parsec Gameserver	parsec-game	15.1(3)T	
Passgo	TCP/UDP	511	passgo	passgo	15.1(3)T	
Passgo-Tivoli	TCP/UDP	627	passgo-tivoli	passgo-tivoli	15.1(3)T	
	Password-Chg	TCP/UDP	586	Password Change	password-chg	15.1(3)T
Pawserv	TCP/UDP	345	Perf Analysis Workbench	pawserv	15.1(3)T	
PCMail-SRV	TCP/UDP	158	PCMail Server	pcmail-srv	15.1(3)T	
PDAP	TCP/UDP	344	Prospero Data Access Protocol	pdap	15.1(3)T	
Personal-link	TCP/UDP	281	personal-link	personal-link	15.1(3)T	
PFTP	TCP/UDP	662	pftp	pftp	15.1(3)T	
PGM	TCP/UDP	113	PGM Reliable Transport Protocol	pgm	15.1(3)T	
Philips-VC	TCP/UDP	583	Philips Video-Conferencing	philips-vc	15.1(3)T	
Phonebook	TCP/UDP	767	Phone	phonebook	15.1(3)T	
Photuris	TCP/UDP	468	photuris	photuris	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
PIM	TCP/UDP	103	Protocol Independent Multicast	pim	15.1(3)T	
PIM-RP-DISC	TCP/UDP	496	PIM-RP-DISC	pim-rp-disc	15.1(3)T	
PIP	TCP/UDP	1321	pip	pip	15.1(3)T	
PIPE	TCP/UDP	131	Private IP Encapsulation within IP	pipe	15.1(3)T	
PIRP	TCP/UDP	553	pirp	pirp	15.1(3)T	
PKIX-3-CA-RA	TCP/UDP	829	PKIX-3 CA/RA	pkix-3-ca-ra	15.1(3)T	
PKIX-Timestamp	TCP/UDP	318	pkix-timestamp	pkix-timestamp	15.1(3)T	
PNNI	TCP/UDP	102	PNNI over IP	pnni	15.1(3)T	
Pop2	TCP/UDP	109	Post Office Protocol - Version 2	pop2	15.1(3)T	
	Pop3	TCP/UDP	110	Post Office Protocol	pop3	15.1(3)T
	POV-Ray	TCP/UDP	494	pov-ray	pov-ray	15.1(3)T
Powerburst	TCP/UDP	485	Air Soft Power Burst	powerburst	15.1(3)T	
PPTP	TCP/UDP	1723	Point-to-Point Tunneling Protocol	pptp	15.1(3)T	
Print-SRV	TCP/UDP	170	Network PostScript	print-srv	15.1(3)T	
PRM	TCP/UDP	21	Packet Radio Measurement	prm	15.1(3)T	
PRM-NM	TCP/UDP	409	Prospero Resource Manager Node Man	prm-nm	15.1(3)T	
PRM-SM	TCP/UDP	408	Prospero Resource Manager Sys. Man	prm-sm	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Profile	TCP/UDP	136	PROFILE Naming System	profile	15.1(3)T	
Prospero	TCP/UDP	191	Prospero Directory Service	prospero	15.1(3)T	
PTCNameService	TCP/UDP	597	PTC Name Service	ptcnameservice	15.1(3)T	
PTP	TCP/UDP	123	Performance Transparency Protocol	ptp	15.1(3)T	
PTP-Event	TCP/UDP	319	PTP Event	ptp-event	15.1(3)T	
PTP-General	TCP/UDP	320	PTP General	ptp-general	15.1(3)T	
Pump	TCP/UDP	751	pump	pump	15.1(3)T	
PUP	TCP/UDP	12	PUP	pup	15.1(3)T	
Purenoise	TCP/UDP	663	purenoise	purenoise	15.1(3)T	
PVP	TCP/UDP	75	Packet Video Protocol	pvp	15.1(3)T	
PWDGen	TCP/UDP	129	Password Generator Protocol	pwdgen	15.1(3)T	
QBIKGDP	TCP/UDP	368	qbikgdp	qbikgdp	15.1(3)T	
	QFT	TCP/UDP	189	Queued File Transport	qft	15.1(3)T
	QMQP	TCP/UDP	628	qmqp	qmqp	15.1(3)T
QMTP	TCP/UDP	209	The Quick Mail Transfer Protocol	qmtp	15.1(3)T	
QNX	TCP/UDP	106	QNX	qnx	15.1(3)T	
QoTD	TCP/UDP	17	Quote of the Day	qotd	15.1(3)T	
QRH	TCP/UDP	752	qrh	qrh	15.1(3)T	
QUOTD	TCP/UDP	762	quotad	quotad	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
RAP	TCP/UDP	38	Route Access Protocol	rap	15.1(3)T	
RDA	TCP/UDP	630	rda	rda	15.1(3)T	
RDB-DBS-DISP	TCP/UDP	1571	Oracle Remote Data Base	rdb-dbs-disp	15.1(3)T	
RDP	TCP/UDP	27	Reliable Data Protocol	rdp	15.1(3)T	
Realm-RUSD	TCP/UDP	688	ApplianceWare managment protocol	realm-rusd	15.1(3)T	
RE-Mail-CK	TCP/UDP	50	Remote Mail Checking Protocol	re-mail-ck	15.1(3)T	
RemoteFS	TCP/UDP	556	rfs server	remotefs	15.1(3)T	
Remote-KIS	TCP/UDP	185	remote-kis	remote-kis	15.1(3)T	
REPCMD	TCP/UDP	641	repcmd	repcmd	15.1(3)T	
REPSCMD	TCP/UDP	653	repscmd	repscmd	15.1(3)T	
RESCAP	TCP/UDP	283	rescap	rescap	15.1(3)T	
RIP	TCP/UDP	520	Routing Information Protocol	rip	15.1(3)T	
RIPING	TCP/UDP	521	ripng	ripng	15.1(3)T	
	RIS	TCP/UDP	180	Intergraph	ris	15.1(3)T
	RIS-CM	TCP/UDP	748	Russell Info Sci Calendar Manager	ris-cm	15.1(3)T
RJE	TCP/UDP	5	Remote Job Entry	rje	15.1(3)T	
RLP	TCP/UDP	39	Resource Location Protocol	rlp	15.1(3)T	
RLZDBASE	TCP/UDP	635	rlzdbase	rlzdbase	15.1(3)T	
RMC	TCP/UDP	657	rmc	rmc	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
RMIActivation	TCP/UDP	1098	rmiactivation	rmiactivation	15.1(3)T	
RMIRegistry	TCP/UDP	1099	rmiregistry	rmiregistry	15.1(3)T	
RMonitor	TCP/UDP	560	rmonitord	rmonitor	15.1(3)T	
RMT	TCP/UDP	411	Remote MT Protocol	rmt	15.1(3)T	
RPC2Portmap	TCP/UDP	369	rpc2portmap	rpc2portmap	15.1(3)T	
RRH	TCP/UDP	753	rrh	rrh	15.1(3)T	
RRP	TCP/UDP	648	Registry Registrar Protocol	rrp	15.1(3)T	
RSH-SPX	TCP/UDP	222	Berkeley rshd with SPX auth	rsh-spx	15.1(3)T	
RSVD	TCP/UDP	168	rsvd	rsvd	15.1(3)T	
RSVP_Tunnel	TCP/UDP	363	rsvp_tunnel	rsvp_tunnel	15.1(3)T	
RSVP-E2E-Ignore	TCP/UDP	134	RSVP-E2E-IGNORE	rsvp-e2e-ignore	15.1(3)T	
Rsync	TCP/UDP	873	rsync	rsync	15.1(3)T	
RTIP	TCP/UDP	771	rtip	rtip	15.1(3)T	
RTSPS	TCP/UDP	322	RTSPS	rtsps	15.1(3)T	
	Rushd	TCP/UDP	696	rushd	rushd	15.1(3)T
RVD	TCP/UDP	66	MIT Remote Virtual Disk Protocol	rvd	15.1(3)T	
RXE	TCP/UDP	761	rxe	rxe	15.1(3)T	
SAFT	TCP/UDP	487	saft Simple Asynchronous File Transfer	saft	15.1(3)T	
Sanity	TCP/UDP	643	sanity	sanity	15.1(3)T	
SAT-EXPAK	TCP/UDP	64	SATNET and Backroom EXPAK	sat-expak	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
SAT-Mon	TCP/UDP	69	SATNET Monitoring	sat-mon	15.1(3)T	
SCC-Security	TCP/UDP	582	scc-security	scc-security	15.1(3)T	
SCC-SP	TCP/UDP	96	Semaphore Communications Sec. Pro.	scc-sp	15.1(3)T	
SCO-DTMgr	TCP/UDP	617	SCO Desktop Administration Server	sco-dtmgr	15.1(3)T	
SCOHELP	TCP/UDP	457	scohelp	scohelp	15.1(3)T	
SCOI2ODialog	TCP/UDP	360	scoi2odialog	scoi2odialog	15.1(3)T	
SCO-Inetmgr	TCP/UDP	615	Internet Configuration Manager	sco-inetmgr	15.1(3)T	
SCO-SysMgr	TCP/UDP	616	SCO System Administration Server	sco-sysmgr	15.1(3)T	
SCO-WebsrvrMg3	TCP/UDP	598	SCO Web Server Manager 3	sco-websrvrmg3	15.1(3)T	
SCO-WebsrvrMgr	TCP/UDP	620	SCO WebServer Manager	sco-websrvrmgr	15.1(3)T	
SCPS	TCP/UDP	105	SCPS	scps	15.1(3)T	
	SCTP	TCP/UDP	132	Stream Control Transmission Protocol	sctp	15.1(3)T
SCX-Proxy	TCP/UDP	470	scx-proxy	scx-proxy	15.1(3)T	
SDNSKMP	TCP/UDP	558	SDNSKMP	sdnskmp	15.1(3)T	
SDRP	TCP/UDP	42	Source Demand Routing Protocol	sdrp	15.1(3)T	
Secure-ftp	TCP/UDP	990	ftp protocol, control, over TLS/SSL	secure-ftp	15.1(3)T	
Secure-IRC	TCP/UDP	994	irc protocol over TLS	secure-irc	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Secure-LDAP	TCP/UDP	636	ldap protocol over TLS	secure-ldap	15.1(3)T	
Secure-NNTP	TCP/UDP	563	nntp protocol over TLS	secure-nntp	15.1(3)T	
Secure-Pop3	TCP/UDP	995	pop3 protocol over TLS	secure-pop3	15.1(3)T	
Secure-Telnet	TCP/UDP	992	telnet protocol over TLS	secure-telnet	15.1(3)T	
Secure-VMTP	TCP/UDP	82	SECURE-VMTP	secure-vmtp	15.1(3)T	
Semantix	TCP/UDP	361	semantix	semantix	15.1(3)T	
Send	TCP/UDP	169	SEND	send	15.1(3)T	
Server-IPX	TCP/UDP	213	Internetwork Packet Exchange Protocol	server-ipx	15.1(3)T	
Servstat	TCP/UDP	633	Service Status update	servstat	15.1(3)T	
SET	TCP/UDP	257	Secure Electronic Transaction	set	15.1(3)T	
SFS-Config	TCP/UDP	452	Cray SFS config server	sfs-config	15.1(3)T	
SFS-SMP-Net	TCP/UDP	451	Cray Network Semaphore server	sfs-smp-net	15.1(3)T	
SFTP	TCP/UDP	115	Simple File Transfer Protocol	sftp	15.1(3)T	
	SGCP	TCP/UDP	440	sgcp	sgcp	15.1(3)T
	SGMP	TCP/UDP	153	sgmp	sgmp	15.1(3)T
SGMP-Traps	TCP/UDP	160	sgmp-traps	sgmp-traps	15.1(3)T	
Shockwave	TCP/UDP	1626	Shockwave	shockwave	15.1(3)T	
Shrinkwrap	TCP/UDP	358	shrinkwrap	shrinkwrap	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
SIAM	TCP/UDP	498	siam	siam	15.1(3)T	
SIFT-UFT	TCP/UDP	608	Sender-Initiated/ Unsolicited File Transfer	sift-uft	15.1(3)T	
SILC	TCP/UDP	706	silc	silc	15.1(3)T	
SitaraDir	TCP/UDP	2631	sitaradir	sitaradir	15.1(3)T	
SitaraMgmt	TCP/UDP	2630	sitaramgmt	sitaramgmt	15.1(3)T	
Sitaraserver	TCP/UDP	2629	sitaraserver	sitaraserver	15.1(3)T	
SKIP	TCP/UDP	57	SKIP	skip	15.1(3)T	
SKRONK	TCP/UDP	460	skronk	skronk	15.1(3)T	
SM	TCP/UDP	122	SM	sm	15.1(3)T	
Smakynet	TCP/UDP	122	smakynet	smakynet	15.1(3)T	
SmartSDP	TCP/UDP	426	smartsdp	smartsdp	15.1(3)T	
SMP	TCP/UDP	121	Simple Message Protocol	smp	15.1(3)T	
SMPNameRes	TCP/UDP	901	smpnameres	smpnameres	15.1(3)T	
SMSD	TCP/UDP	596	smsd	smsd	15.1(3)T	
SMSP	TCP/UDP	413	Storage Management Services Protocol	smsp	15.1(3)T	
	SMTP	TCP/UDP	25	Simple Mail Transfer Protocol	smtp	15.1(3)T
	SMUX	TCP/UDP	199	SMUX	smux	15.1(3)T
SNAGas	TCP/UDP	108	SNA Gateway Access Server	snagas	15.1(3)T	
Snare	TCP/UDP	509	snare	snare	15.1(3)T	
S-Net	TCP/UDP	166	Sirius Systems	s-net	15.1(3)T	
SNP	TCP/UDP	109	Sitara Networks Protocol	snp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
SNPP	TCP/UDP	444	Simple Network Paging Protocol	snpp	15.1(3)T	
SNTP-Heartbeat	TCP/UDP	580	SNTP HEARTBEAT	sntp-heartbeat	15.1(3)T	
SoftPC	TCP/UDP	215	Insignia Solutions	softpc	15.1(3)T	
Sonar	TCP/UDP	572	sonar	sonar	15.1(3)T	
SPMP	TCP/UDP	656	spmp	spmp	15.1(3)T	
Sprite-RPC	TCP/UDP	90	Sprite RPC Protocol	sprite-rpc	15.1(3)T	
SPS	TCP/UDP	130	Secure Packet Shield	sps	15.1(3)T	
SPSC	TCP/UDP	478	spsc	spsc	15.1(3)T	
SQL*Net	TCP/UDP	66	Oracle SQL*NET	sql*net	15.1(3)T	
SQL-Net	TCP/UDP	150	SQL-NET	sql-net	15.1(3)T	
SQLServ	TCP/UDP	118	SQL Services	sqlserv	15.1(3)T	
SQLServer	TCP/UDP	1433	Microsoft-SQL-Server	sqlserver	15.1(3)T	
SRC	TCP/UDP	200	IBM System Resource Controller	src	15.1(3)T	
SRMP	TCP/UDP	193	Spider Remote Monitoring Protocol	srmp	15.1(3)T	
	SRP	TCP/UDP	119	SpectraLink Radio Protocol	srp	15.1(3)T
	SRSSend	TCP/UDP	362	srssend	srssend	15.1(3)T
SS7NS	TCP/UDP	477	ss7ns	ss7ns	15.1(3)T	
SSCOPMCE	TCP/UDP	128	SSCOPMCE	sscopmce	15.1(3)T	
SSH	TCP/UDP	22	Secure Shell Protocol	ssh	15.1(3)T	
Sshell	TCP/UDP	614	SSLshell	sshell	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
SST	TCP/UDP	266	SCSI on ST	sst	15.1(3)T	
ST	TCP/UDP	5	Stream	st	15.1(3)T	
StatSRV	TCP/UDP	133	Statistics Service	statsrv	15.1(3)T	
STMF	TCP/UDP	501	stmf	stmf	15.1(3)T	
STP	TCP/UDP	118	Schedule Transfer Protocol	stp	15.1(3)T	
StreetTalk	TCP/UDP	566	streettalk	streettalk	15.1(3)T	
Stun-NAT	TCP/UDP	3478	STUN	stun-nat	15.1(3)T	
STX	TCP/UDP	527	Stock IXChange	stx	15.1(3)T	
Submission	TCP/UDP	587	submission	submission	15.1(3)T	
Subntbcst_TFTP	TCP/UDP	247	subntbcst_tftp	subntbcst_tftp	15.1(3)T	
SU-MIT-TG	TCP/UDP	89	SU/MIT Telnet Gateway	su-mit-tg	15.1(3)T	
Sun-DR	TCP/UDP	665	sun-dr	sun-dr	15.1(3)T	
Sun-ND	TCP/UDP	77	SUN ND PROTOCOL-Temporary	sun-nd	15.1(3)T	
SupDup	TCP/UDP	95	SUPDUP	supdup	15.1(3)T	
	Surf	TCP/UDP	1010	surf	surf	15.1(3)T
Sur-Meas	TCP/UDP	243	Survey Measurement	sur-meas	15.1(3)T	
Svrloc	TCP/UDP	427	Server Location	svrloc	15.1(3)T	
Swift-RVF	TCP/UDP	97	Swift Remote Virtural File Protocol	swift-rvf	15.1(3)T	
Swipe	TCP/UDP	53	IP with Encryption	swipe	15.1(3)T	
Synoptics-Trap	TCP/UDP	412	Trap Convention Port	synoptics-trap	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Synotics-Broker	TCP/UDP	392	SynOptics Port Broker Port	synotics-broker	15.1(3)T	
Synotics-Relay	TCP/UDP	391	SynOptics SNMP Relay Port	synotics-relay	15.1(3)T	
TAC News	TCP/UDP	98	TAC News	tacnews	15.1(3)T	
Talk	TCP/UDP	517	talk	talk	15.1(3)T	
TCF	TCP/UDP	87	TCF	tcf	15.1(3)T	
TD-Replica	TCP/UDP	268	Tobit David Replica	td-replica	15.1(3)T	
TD-Service	TCP/UDP	267	Tobit David Service Layer	td-service	15.1(3)T	
Teedtap	TCP/UDP	559	teedtap	teedtap	15.1(3)T	
Tell	TCP/UDP	754	send	tell	15.1(3)T	
Telnet	TCP/UDP	23	Telnet	telnet	15.1(3)T	
Tempo	TCP/UDP	526	newdate	tempo	15.1(3)T	
Tenfold	TCP/UDP	658	tenfold	tenfold	15.1(3)T	
Texar	TCP/UDP	333	Texar Security Port	texar	15.1(3)T	
	TICF-1	TCP/UDP	492	Transport Independent Convergence for FNA	ticf-1	15.1(3)T
TICF-2	TCP/UDP	493	Transport Independent Convergence for FNA	ticf-2	15.1(3)T	
Timbuktu	TCP/UDP	407	Timbuktu	timbuktu	15.1(3)T	
Timed	TCP/UDP	525	timeserver	timed	15.1(3)T	
TINC	TCP/UDP	655	tinc	tinc	15.1(3)T	
TLISRV	TCP/UDP	1527	oracle	tlisrv	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
TLSP	TCP/UDP	56	Transport Layer Security Protocol	tlsp	15.1(3)T	
TNETOS	TCP/UDP	377	NEC Corporation	tnETOS	15.1(3)T	
TNS-CML	TCP/UDP	590	tns-cml	tns-cml	15.1(3)T	
TN-TL-FD1	TCP/UDP	476	tn-tl-fd1	tn-tl-fd1	15.1(3)T	
TP++	TCP/UDP	39	TP++ Transport Protocol	tp++	15.1(3)T	
TPIP	TCP/UDP	594	tpip	tpip	15.1(3)T	
Trunk-1	TCP/UDP	23	Trunk-1	trunk-1	15.1(3)T	
Trunk-2	TCP/UDP	24	Trunk-2	trunk-2	15.1(3)T	
TServer	TCP/UDP	450	Computer Supported Telecomunicatio n Applications	tserver	15.1(3)T	
TTP	TCP/UDP	84	TTP	ttp	15.1(3)T	
UAAC	TCP/UDP	145	UAAC Protocol	uaac	15.1(3)T	
UARPs	TCP/UDP	219	Unisys ARPs	uarps	15.1(3)T	
	UDPLite	TCP/UDP	136	UDPLite	udplite	15.1(3)T
	UIS	TCP/UDP	390	uis	uis	15.1(3)T
uLISTProc	TCP/UDP	372	List Processor	ulistproc	15.1(3)T	
ULP	TCP/UDP	522	ulp	ulp	15.1(3)T	
ULPNet	TCP/UDP	483	ulpnet	ulpnet	15.1(3)T	
Unidata-LDM	TCP/UDP	388	Unidata LDM	unidata-ldm	15.1(3)T	
Unify	TCP/UDP	181	Unify	unify	15.1(3)T	
UPS	TCP/UDP	401	Uninterruptible Power Supply	ups	15.1(3)T	
URM	TCP/UDP	606	Cray Unified Resource Manager	urm	15.1(3)T	
UTI	TCP/UDP	120	UTI	uti	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Utime	TCP/UDP	519	unixtime	utime	15.1(3)T	
UTMPCD	TCP/UDP	431	utmpcd	utmpcd	15.1(3)T	
UTMPSD	TCP/UDP	430	utmpsd	utmpsd	15.1(3)T	
UUCP	TCP/UDP	540	uucpd	uucp	15.1(3)T	
UUCP-Path	TCP/UDP	117	UUCP Path Service	uucp-path	15.1(3)T	
UUCP-rLogin	TCP/UDP	541	uucp-rlogin	uucp-rlogin	15.1(3)T	
UUIDGEN	TCP/UDP	697	UUIDGEN	uuidgen	15.1(3)T	
VACDSM-App	TCP/UDP	671	VACDSM-APP	vacdsm-app	15.1(3)T	
VACDSM-SWS	TCP/UDP	670	VACDSM-SWS	vacdsm-sws	15.1(3)T	
VATP	TCP/UDP	690	Velazquez Application Transfer Protocol	vatp	15.1(3)T	
	VEMMI	TCP/UDP	575	vemmi	vemmi	15.1(3)T
	VID	TCP/UDP	769	vid	vid	15.1(3)T
Videotex	TCP/UDP	516	videotex	videotex	15.1(3)T	
VISA	TCP/UDP	70	VISA Protocol	visa	15.1(3)T	
VMNet	TCP/UDP	175	vmnet	vmnet	15.1(3)T	
VMPWSCS	TCP/UDP	214	vmpwscs	vmpwscs	15.1(3)T	
VMTP	TCP/UDP	81	VMTP	vmtp	15.1(3)T	
VNAS	TCP/UDP	577	vnas	vnas	15.1(3)T	
VPP	TCP/UDP	677	Virtual Presence Protocol	vpp	15.1(3)T	
VPPS-QUA	TCP/UDP	672	vpps-qua	vpps-qua	15.1(3)T	
VPPS-VIA	TCP/UDP	676	vpps-via	vpps-via	15.1(3)T	
VRRP	TCP/UDP	112	Virtual Router Redundancy Protocol	vrrp	15.1(3)T	
VSINet	TCP/UDP	996	vsinet	vsinet	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
VSLMP	TCP/UDP	312	vslmp	vslmp	15.1(3)T	
WAP-Push	TCP/UDP	2948	WAP PUSH	wap-push	15.1(3)T	
WAP-Push-HTTP	TCP/UDP	4035	WAP Push OTA-HTTP port	wap-push-http	15.1(3)T	
WAP-Push-HTTPS	TCP/UDP	4036	WAP Push OTA-HTTP secure	wap-push-https	15.1(3)T	
WAP-Pushsecure	TCP/UDP	2949	WAP PUSH SECURE	wap-pushsecure	15.1(3)T	
WAP-VACL-S	TCP/UDP	9207	WAP vCal Secure	wap-vcal-s	15.1(3)T	
WAP-VCAL	TCP/UDP	9205	WAP vCal	wap-vcal	15.1(3)T	
	WAP-VCARD	TCP/UDP	9204	WAP vCard	wap-vcard	15.1(3)T
	WAP-VCARD-S	TCP/UDP	9206	WAP vCard Secure	wap-vcard-s	15.1(3)T
WAP-WSP	TCP/UDP	9200	WAP connectionless session service	wap-wsp	15.1(3)T	
WAP-WSP-S	TCP/UDP	9202	WAP secure connectionless session service	wap-wsp-s	15.1(3)T	
WAP-WSP-WTP	TCP/UDP	9201	WAP session service	wap-wsp-wtp	15.1(3)T	
WAP-WSP-WTP-S	TCP/UDP	9203	WAP secure session service	wap-wsp-wtp-s	15.1(3)T	
WB-Expak	TCP/UDP	79	WIDEBAND EXPAK	wb-expak	15.1(3)T	
WB-Mon	TCP/UDP	78	WIDEBAND Monitoring	wb-mon	15.1(3)T	
Webster	TCP/UDP	765	webster	webster	15.1(3)T	
WhoAmI	TCP/UDP	565	whoami	whoami	15.1(3)T	
WorldFusion	TCP/UDP	2595	World Fusion	worldfusion	15.1(3)T	
WPGS	TCP/UDP	780	wpgs	wpgs	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
WSN	TCP/UDP	74	Wang Span Network	wsn	15.1(3)T	
XAct-Backup	TCP/UDP	911	xact-backup	xact-backup	15.1(3)T	
X-Bone-CTL	TCP/UDP	265	Xbone CTL	x-bone-ctl	15.1(3)T	
XDTP	TCP/UDP	3088	eXtensible Data Transfer Protocol	xdtp	15.1(3)T	
XFER	TCP/UDP	82	XFER Utility	xfer	15.1(3)T	
XNET	TCP/UDP	15	Cross Net Debugger	xnet	15.1(3)T	
XNS-Auth	TCP/UDP	56	XNS Authentication	xns-auth	15.1(3)T	
XNS-CH	TCP/UDP	54	XNS Clearinghouse	xns-ch	15.1(3)T	
	XNS-Courier	TCP/UDP	165	Xerox	xns-courier	15.1(3)T
XNS-IDP	TCP/UDP	22	XEROX NS IDP	xns-idp	15.1(3)T	
XNS-Mail	TCP/UDP	58	XNS mail	xns-mail	15.1(3)T	
XNS-Time	TCP/UDP	52	XNS Time Protocol	xns-time	15.1(3)T	
XTP	TCP/UDP	36	XTP	xtp	15.1(3)T	
XVTTP	TCP/UDP	508	xvttp	xvttp	15.1(3)T	
XYPlex-Mux	TCP/UDP	173	Xyplex	xyplex-mux	15.1(3)T	
z39.50	TCP/UDP	210	ANSI Z39.50	z39.50	15.1(3)T	
Zannet	TCP/UDP	317	zannet	zannet	15.1(3)T	
ZServ	TCP/UDP	346	Zebra server	zserv	15.1(3)T	
LockD	TCP/UDP	4045	LockD	lockd	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
Microsoft-DS	TCP/UDP	445	Microsoft Directory Services	microsoftds	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Nickname	TCP/UDP	43	Nickname	nicname	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
NPP	TCP/UDP	92	Network Payment Protocol	npp	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
ORASRV	TCP	1525	ORASRV	ora-srv	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
RTelnet	TCP/UDP	107	Remote Telnet Service	rtelnet	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
RCP	TCP/UDP	469	Rate Control Protocol	rcp	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T	
	SQLExec	TCP/UDP	9088	SQL Exec	sqlexec	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	Systat	TCP/UDP	11	System Statistics	systat	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	TACACS	TCP/UDP	49, 65	Terminal Access Controller Access-Control System	tacacs	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	Time	TCP/UDP	37	Time	time	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	VNC	UDP	5800, 5900, 5901	Virtual Network Computing	vnc	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	Whois++	TCP/UDP	63	Whois++	whois++	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	XDMCP	UDP	177	X Display Manager Control Protocol	xdmcp	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Miscellaneous (contd.)	3pc	IP	34	Third Party Connect Protocol	3pc	15.1(3)T
AN	IP	107	Active Networks	an	15.1(3)T	
ARGUS	IP	13	ARGUS	argus	15.1(3)T	
ARIS	IP	104	ARIS	aris	15.1(3)T	
AX25	IP	93	AX.25 Frames	ax25	15.1(3)T	
BBNR RCC Mon	IP	10	BBN RCC Monitoring	bbnrccmon	15.1(3)T	
BNA	IP	49	BNA	bna	15.1(3)T	
BR-SAT-Mon	IP	76	Backroom SATNET Monitoring	br-sat-mon	15.1(3)T	
CBT	IP	7	CBT	cbt	15.1(3)T	
CFTP	IP	62	CFTP	cftp	15.1(3)T	
Choas	IP	16	Chaos	chaos	15.1(3)T	
Compaq-Peer	IP	110	Compaq Peer Protocol	compaq-peer	15.1(3)T	
CPHB	IP	73	Computer Protocol Heart Beat	cphb	15.1(3)T	
	CPNX	IP	72	Computer Protocol Network Executive	cpnx	15.1(3)T
	CRTP	IP	126	Combat Radio Transport Protocol	crtp	15.1(3)T
CRUDP	IP	127	Combat Radio User Datagram	crudp	15.1(3)T	
DCCP	IP	33	Datagram Congestion Control Protocol	dccp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
DCN-Meas	IP	19	DCN Measurement Subsystems	dcn-meas	15.1(3)T	
DDP	IP	37	Datagram Delivery Protocol	ddp	15.1(3)T	
DDX	IP	116	D-II Data Exchange	ddx	15.1(3)T	
DGP	IP	86	Dissimilar Gateway Protocol	dgp	15.1(3)T	
DSR	IP	48	Dynamic Source Routing Protocol	dsr	15.1(3)T	
EGP	IP	8	Exterior Gateway Protocol	egp	15.1(3)T	
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	15.1(3)T	
EMCON	IP	14	EMCON	emcon	15.1(3)T	
Encap	IP	98	Encapsulation Header	encap	15.1(3)T	
EtherIP	IP	97	Ethernet-within-IP Encapsulation	etherip	15.1(3)T	
FC	IP	133	Fibre Channel	fc	15.1(3)T	
FIRE	IP	125	FIRE	fire	15.1(3)T	
GGP	IP	3	Gateway-to-Gateway	ggp	15.1(3)T	
GMTP	IP	100	GMTP	gmtp	15.1(3)T	
GRE	IP	47	General Routing Encapsulation	gre	15.1(3)T	
HIP	IP	139	Host Identity Protocol	hip	15.1(3)T	
HMP	IP	20	Host Monitoring	hmp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
HopOpt	IP	0	IPv6 Hop-by-Hop Option	hopopt	15.1(3)T	
	IATP	IP	117	Interactive Agent Transfer Protocol	iatp	15.1(3)T
	ICMP	IP	1	Internet Control Message	icmp	15.1(3)T
IDPR	IP	35	Inter-Domain Policy Routing Protocol	idpr	15.1(3)T	
IDPR-CMTP	IP	38	IDPR Control Message Transport Proto	idpr-cmtp	15.1(3)T	
IDRP	IP	45	Inter-Domain Routing Protocol	idrp	15.1(3)T	
IFMP	IP	101	Ipsilon Flow Management Protocol	ifmp	15.1(3)T	
IGRP	IP	9	Cisco interior gateway	igrp	15.1(3)T	
IL	IP	40	IL Transport Protocol	il	15.1(3)T	
I-NLSP	IP	52	Integrated Net Layer Security TUBA	i-nlsp	15.1(3)T	
IMPCOMP	IP	108	IP Payload Compression Protocol	ipcomp	15.1(3)T	
IPCU	IP	71	Internet Packet Core Utility	ipcv	15.1(3)T	
IPinIP	IP	4	IP in IP	ipinip	15.1(3)T	
IPIP	IP	94	IP-within-IP Encapsulation Protocol	ipip	15.1(3)T	
IPLT	IP	129	IPLT	iplt	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
IPPC	IP	67	Internet Pluribus Packet Core	ippc	15.1(3)T	
IPv6-Frag	IP	44	Fragment Header for IPv6	ipv6-frag	15.1(3)T	
IPv6-ICMP	IP	58	ICMP for IPv6	ipv6-icmp	15.1(3)T	
IPv6INIP	IP	41	Ipv6 encapsulated	ipv6inip	15.1(3)T	
IPv6-NONXT	IP	59	No Next Header for IPv6	ipv6-nonxt	15.1(3)T	
IPv6-Opts	IP	60	Destination Options for IPv6	ipv6-opts	15.1(3)T	
	IPv6-Route	IP	43	Routing Header for IPv6	ipv6-route	15.1(3)T
	IRTP	IP	28	Internet Reliable Transaction	irtp	15.1(3)T
ISIS	IP	124	ISIS over IPv4	isis	15.1(3)T	
ISO-TP4	IP	29	ISO Transport Protocol Class 4	iso-tp4	15.1(3)T	
IXP-in-IP	IP	111	IPX in IP	ixp-in-ip	15.1(3)T	
LARP	IP	91	Locus Address Resolution Protocol	larp	15.1(3)T	
Leaf-1	IP	25	Leaf-1	leaf-1	15.1(3)T	
Leaf-2	IP	26	Leaf-2	leaf-2	15.1(3)T	
MANET	IP	138	MANET Protocols	manet	15.1(3)T	
Merit-Inp	IP	32	MERIT Internodal Protocol	merit-inp	15.1(3)T	
MFE-NSP	IP	31	MFE Network Services Protocol	mfe-nsp	15.1(3)T	
MICP	IP	95	Mobile Internetworking Control Pro.	micp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Mobile	IP	55	IP Mobility	mobile	15.1(3)T	
MPLS-in-IP	IP	137	MPLS-in-IP	mpls-in-ip	15.1(3)T	
MTP	IP	92	Multicast Transport Protocol	mtp	15.1(3)T	
Mux	IP	18	Multiplexing	mux	15.1(3)T	
NARP	IP	54	NBMA Address Resolution Protocol	narp	15.1(3)T	
Netblt	IP	30	Bulk Data Transfer Protocol	netblt	15.1(3)T	
NSFNET-IGP	IP	85	NSFNET-IGP	nsfnet-igp	15.1(3)T	
NVP-II	IP	11	Network Voice Protocol	nvp-ii	15.1(3)T	
OSPF	IP	89	Open Shortest Path First	ospf	15.1(3)T	
PGM	IP	113	PGM Reliable Transport Protocol	pgm	15.1(3)T	
PIM	IP	103	Protocol Independent Multicast	pim	15.1(3)T	
	Pipe	IP	131	Private IP Encapsulation within IP	pipe	15.1(3)T
	PNNI	IP	102	PNNI over IP	pnni	15.1(3)T
PRM	IP	21	Packet Radio Measurement	prm	15.1(3)T	
PTP	IP	123	Performance Transparency Protocol	ptp	15.1(3)T	
PUP	IP	12	PUP	pup	15.1(3)T	
PVP	IP	75	Packet Video Protocol	pvp	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
QNX	IP	106	QNX	qnx	15.1(3)T	
RDP	IP	27	Reliable Data Protocol	rdp	15.1(3)T	
RSVP-E2E-Ignore	IP	134	RSVP-E2E-IGNORE	rsvp-e2e-ignore	15.1(3)T	
RVD	IP	66	MIT Remote Virtual Disk Protocol	rvd	15.1(3)T	
SAT-EXPAK	IP	64	SATNET and Backroom EXPAK	sat-expak	15.1(3)T	
SAT-Mon	IP	69	SATNET Monitoring	sat-mon	15.1(3)T	
SCC-SP	IP	96	Semaphore Communications Sec. Pro.	scc-sp	15.1(3)T	
SCPS	IP	105	SCPS	scps	15.1(3)T	
SCTP	IP	132	Stream Control Transmission Protocol	sctp	15.1(3)T	
SDRP	IP	42	Source Demand Routing Protocol	sdrp	15.1(3)T	
Secure-VMTP	IP	82	SECURE-VMTP	secure-vmtp	15.1(3)T	
SKIP	IP	57	SKIP	skip	15.1(3)T	
SM	IP	122	SM	sm	15.1(3)T	
SMP	IP	121	Simple Message Protocol	smp	15.1(3)T	
SNP	IP	109	Sitara Networks Protocol	snp	15.1(3)T	
	Sprite-RPC	IP	90	Sprite RPC Protocol	sprite-rpc	15.1(3)T
	SPS	IP	130	Secure Packet Shield	sps	15.1(3)T

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
SRP	IP	119	SpectraLink Radio Protocol	srp	15.1(3)T	
SSCOPMCE	IP	128	SSCOPMCE	sscopmce	15.1(3)T	
ST	IP	5	Stream	st	15.1(3)T	
STP	IP	118	Schedule Transfer Protocol	stp	15.1(3)T	
SUN-ND	IP	77	SUN ND PROTOCOL-Temporary	sun-nd	15.1(3)T	
Swipe	IP	53	IP with Encryption	swipe	15.1(3)T	
TCF	IP	87	TCF	tcf	15.1(3)T	
TLSP	IP	56	Transport Layer Security Protocol	tlsp	15.1(3)T	
TP++	IP	39	TP++ Transport Protocol	tp++	15.1(3)T	
Trunk-1	IP	23	Trunk-1	trunk-1	15.1(3)T	
Trunk-2	IP	24	Trunk-2	trunk-2	15.1(3)T	
TTP	IP	84	TTP	ttp	15.1(3)T	
UDPLite	IP	136	UDPLite	udplite	15.1(3)T	
UTI	IP	120	UTI	uti	15.1(3)T	
VISA	IP	70	VISA Protocol	visa	15.1(3)T	
VMTP	IP	81	VMTP	vmtp	15.1(3)T	
VRRP	IP	112	Virtual Router Redundancy Protocol	vrrp	15.1(3)T	
WB-Expak	IP	79	WIDEBAND EXPAK	wb-expak	15.1(3)T	
WB-Mon	IP	78	WIDEBAND Monitoring	wb-mon	15.1(3)T	

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
WSN	IP	74	Wang Span Network	wsn	15.1(3)T	
XNET	IP	15	Cross Net Debugger	xnet	15.1(3)T	
XNS-LDP	IP	22	XEROX NS IDP	xns-idp	15.1(3)T	
XTP	IP	36	XTP	xtp	15.1(3)T	
Voice	H.323	TCP	Dynamically Assigned	H.323 Teleconferencing Protocol	h323	12.3(7)T 12.2(18)ZYA1 15.1(2)T
	RTCP	TCP/ UDP	Dynamically Assigned	Real-Time Control Protocol	rtcp	12.1E 12.2T 12.2(18)ZYA1 12.3 12.3T 12.3(7)T 15.1(2)T
	RTP	TCP/ UDP	Dynamically Assigned	Real-Time Transport Protocol Payload Classification	rtp	12.2(8)T 12.2(18)ZYA1 15.1(2)T
	Cisco-phone[5]	UDP	5060	Cisco IP Phones and PC-Based Unified Communicators	cisco-phone	12.2(18)ZYA 12.2(18)ZYA1 15.1(2)T
	SIP	TCP/UPD	5060	Session Initiation Protocol	sip	12.3(7)T 12.2(18)ZYA1 15.1(2)T
	SCCP/ Skinny	TCP	2000, 2001, 2002	Skinny Client Control Protocol	skinny	12.3(7)T 12.2(18)ZYA1 15.1(2)T
	Skype[6]	TCP/UDP	Dynamically Assigned	Peer-to-Peer VoIP Client Software	skype	12.4(4)T

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.

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
	TelePresence	TCP/UDP	Dynamically Assigned	Cisco TelePresence System	telepresence-media telepresence-control	12.2(18)ZYA2 15.1(2)T
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 15.1(2)T
	Direct Connect	TCP/ UDP	411	Direct Connect File Transfer Traffic	directconnect	12.4(4)T 12.2(18)ZYA1 15.1(2)T
	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 15.1(2)T
	FastTrack	N/A	Dynamically Assigned	FastTrack	fasttrack	12.1(12c)E 12.2(18)ZYA1 15.1(2)T
	Gnutella	TCP	Dynamically Assigned	Gnutella	gnutella	12.1(12c)E 12.2(18)ZYA1 15.1(2)T
	KaZaA	TCP/ UPD	Dynamically Assigned	KaZaA Note that earlier KaZaA version 1 traffic can be classified using FastTrack.	kazaa2	12.2(8)T 12.2(18)ZYA1 15.1(2)T
	WinMX	TCP	6699	WinMX Traffic	winmx	12.3(7)T 12.2(18)ZYA1 15.1(2)T

NBAR Memory Management

NBAR uses approximately 150 bytes of DRAM for each traffic flow that requires stateful inspection. (See NBAR Memory Management, page 70 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, page 71

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 some how 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

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*
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 *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide* , Release 12.2ZY
Classifying network traffic if not using NBAR	"Classifying Network Traffic" module

Related Topic	Document Title
FWSM and its connection features	"Configuring Advanced Connection Features" module of the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
FWSM commands	"Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Service Module Command Reference Guide
IDSM	"Configuring IDSM-2" module of the *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
SPAN or RSPAN	"Configuring SPAN and RSPAN" module of the *Catalyst 6500 Series Software Configuration Guide*
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 *Catalyst 6500 Series Software Configuration Guide*
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 of the *Cisco IOS Security Configuration Guide*
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
AutoQoS, [7] 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
Adding application recognition modules (also known as PDLMs)	"Adding Application Recognition Modules" module

7 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.

Related Topic	Document Title
Creating a custom protocol	"Creating a Custom Protocol" module
Configuring Flexible NetFlow for Network Based Application Recognition	"Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors" module

Standards

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

MIBs

MIB	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	*NAME/FINGER Protocol*
RFC 759	*Internet Message Protocol*
RFC 768	*User Datagram Protocol*
RFC 792	*Internet Control Message Protocol*
RFC 793	*Transmission Control Protocol*
RFC 821	*Simple Mail Transfer Protocol*
RFC 827	*Exterior Gateway Protocol*
RFC 854	*Telnet Protocol Specification*
RFC 888	*"STUB" Exterior Gateway Protocol*

RFC	Title
RFC 904	*Exterior Gateway Protocol Formal Specification*
RFC 951	*Bootstrap Protocol*
RFC 959	*File Transfer Protocol*
RFC 977	*Network News Transfer Protocol*
RFC 1001	*Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods*
RFC 1002	*Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications*
RFC 1057	*RPC: Remote Procedure Call*
RFC 1094	*NFS: Network File System Protocol Specification*
RFC 1112	*Host Extensions for IP Multicasting*
RFC 1157	*Simple Network Management Protocol*
RFC 1282	*BSD Rlogin*
RFC 1288	*The Finger User Information Protocol*
RFC 1305	*Network Time Protocol*
RFC 1350	*The TFTP Protocol (Revision 2)*
RFC 1436	*The Internet Gopher Protocol*
RFC 1459	*Internet Relay Chat Protocol*
RFC 1510	*The Kerberos Network Authentication Service*
RFC 1542	*Clarifications and Extensions for the Bootstrap Protocol*
RFC 1579	*Firewall-Friendly FTP*
RFC 1583	*OSPF Version 2*
RFC 1657	*Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol*
RFC 1701	*Generic Routing Encapsulation*
RFC 1730	*Internet Message Access Protocol--Version 4*
RFC 1771	*A Border Gateway Protocol 4 (BGP-4)*
RFC 1777	*Lightweight Directory Access Protocol*

RFC	Title
RFC 1831	*RPC: Remote Procedure Call Protocol Specification Version 2*
RFC 1889	*A Transport Protocol for Real-Time Applications*
RFC 1890	*RTP Profile for Audio and Video Conferences with Minimal Control*
RFC 1928	*SOCKS Protocol Version 5*
RFC 1939	*Post Office Protocol--Version 3*
RFC 1945	*Hypertext Transfer Protocol--HTTP/1.0*
RFC 1964	*The Kerberos Version 5 GSS-API Mechanism*
RFC 2045	*Multipurpose Internet Mail Extension (MIME) Part One: Format of Internet Message Bodies*
RFC 2060	*Internet Message Access Protocol--Version 4 rev1*
RFC 2068	*Hypertext Transfer Protocol--HTTP/1.1*
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2205	*Resource ReSerVation Protocol (RSVP)--Version 1 Functional Specification*
RFC 2236	*Internet Group Management Protocol, Version 2*
RFC 2251	*Lightweight Directory Access Protocol (v3)*
RFC 2252	*Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*
RFC 2253	*Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*
RFC 2326	*Real Time Streaming Protocol (RTSP)*
RFC 2401	*Security Architecture for the Internet Protocol*
RFC 2406	*IP Encapsulating Security Payload*
RFC 2453	*RIP Version 2*
RFC 2616	*Hypertext Transfer Protocol--HTTP/1.1* **Note** This RFC updates RFC 2068.

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 2: Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
NBAR - Network-based Application Recognition	12.1(5)T 12.1(1)E 12.2(11)YT 12.2(18)ZY	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. The following sections provide information about this feature: The following commands were introduced or modified: **match protocol http**, **match protocol citrix**, **match protocol gnutella**, **match protocol fasttrack**, **ip nbar protocol-tagging**,, **show ip nbar protocol-tagging**.

Feature Name	Releases	Feature Information
Additional PDL Support for NBAR	15.1(2)T	The Additional PDL Support for NBAR feature provides addtional PDLs as part of feature parity between Cisco IOS Release 12.2(18)ZY and Cisco IOS Release 15.1(2)T. The following section includes information about this PDL support extended to Cisco IOS Release 15.1(2)T:
Distributed Network-based Application Recognition (dNBAR)	12.2(4)T 12.2(18)SXF 12.1(6)E	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. The following sections provide information about this feature:
nBAR: IANA Protocol Extensions Pack1	15.1(3)T	The nBAR: IANA Protocol Extensions Pack1 feature allows NBAR to detect and classify a set of protocols and applications standardized by IANA. The following section includes information about this feature:

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 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.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface ethernet 2/4`	Configures an interface type and enters interface configuration mode. • 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. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show policy-map interface** *type number* **Example:** `Router# show policy-map interface Fastethernet 6/0`	(Optional) Displays the packet and class statistics for all policy maps on the specified interface. • Enter the interface type and the interface number.
Step 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*] **Example:** `Router# show ip nbar protocol-discovery interface Fastethernet 6/0`	Displays the statistics gathered by the NBAR Protocol Discovery feature. • (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
```

```
                            Input                    Output
                            -----                    ------
  Protocol                  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	*Cisco IOS Quality of Service Solutions Command Reference*
Concepts and information about NBAR	"Classifying Network Traffic Using NBAR" 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

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 3: Feature Information for Enabling Protocol Discovery

Feature Name	Releases	Feature Information
NBAR--Network-Based Application Recognition	12.2(18)ZYA	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). The following commands were modified: **ip nbar protocol-discovery, show ip nbar protocol-discovery**.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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, page 90.

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 4: match protocol Commands and Corresponding Protocol or Traffic Type

match protocol Command[8]	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

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.

8 **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.**

Note The **match protocol citrix**command is shown in Step Configuring a Traffic Class, page 91 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. • 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**] *class-map-name* **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. • Enter the name of the class map.
Step 4	**match protocol citrix**	Configures NBAR to match Citrix traffic.

	Command or Action	Purpose
	Example: `Router(config-cmap)# match protocol citrix`	**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:** `Router(config-cmap)# end`	(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, page 93 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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **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. • Enter the name of the policy map.
Step 4	**class** {*class-name* | **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. • Enter the specific class name or enter the **class-default**keyword.
Step 5	**bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*} **Example:** `Router(config-pmap-c)# bandwidth percent 50` **Example:**	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. **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. **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.
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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface ethernet 2/4`	Configures an interface type and enters interface configuration mode. • Enter the interface type and the interface number.
Step 4	**pvc** [*name*] *vpi* / *vci* [**ilmi**| **qsaal**| **smds**| **l2transport**] **Example:** `Router(config-if)# pvc cisco 0/16`	(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. • Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. **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, page 94.
Step 5	**exit** **Example:** `Router(config-atm-vc)# exit`	(Optional) Returns to interface configuration mode. **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, page 94. If you are not attaching the policy map to an ATM PVC, advance to Attaching a Traffic Policy to an Interface or Subinterface, page 94.
Step 6	**service-policy** {**input**	**output**} *policy-map-name*	Attaches a policy map (traffic policy) to an input or output interface. • Specify either the **input** or **output** keyword, and enter the policy map name.

	Command or Action	Purpose

	Example:
	`Router(config-if)# service-policy input policy1`
		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.
		Note After you use the **service-policy** command, you may see two messages similar to the following:
		`%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`
		While both of these messages appear, NBAR is enabled in the direction specified by the **input** or **output** keyword only.

Step 7	**end** **Example:** `Router(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Verifying NBAR Using the MCQ

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**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Example: `Router> enable`	
Step 2	**show class-map** [*class-map-name*] **Example:** `Router# show class-map`	(Optional) Displays all class maps and their matching criteria. • (Optional) Enter the name of a specific class map.
Step 3	**show policy-map** [*policy-map*] **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. • (Optional) Enter the name of a specific policy map.
Step 4	**show policy-map interface** *type number* **Example:** `Router# show policy-map interface Fastethernet 6/0`	(Optional) Displays the packet and class statistics for all policy maps on the specified interface. • Enter the interface type and the interface number.
Step 5	**show ip nbar port-map** [*protocol-name*] **Example:** `Router# show ip nbar port-map`	(Optional) Displays the current protocol-to-port mappings in use by NBAR. • (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	*Cisco IOS Quality of Service Solutions Command Reference*
QoS features and functionality on the Catalyst 6500 series switch	"Configuring PFC QoS" chapter of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide* , 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

Related Topic	Document Title
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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	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 5: 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.

Feature Name	Releases	Feature Information
		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:
NBAR--Citrix ICA Published Applications	12.4(2)T	Enables NBAR to classify traffic on the basis of the Citrix Independent Computing Architecture (ICA) published application name and tag number. The following sections provide information about the NBAR-Citrix ICA Published Applications feature:
NBAR--Multiple Matches Per Port	12.4(2)T	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. The following sections provide information about the NBAR-Multiple Matches Per Port feature:
NBAR Extended Inspection for HTTP Traffic	12.3(4)T	Allows NBAR to scan TCP ports that are not well known and identify HTTP traffic that traverses these ports. The following sections provide information about the NBAR

Feature Name	Releases	Feature Information
		Extended Inspection for HTTP Traffic feature:
NBAR Real-Time Transport Protocol Payload Classification	12.2(15)T	Enables stateful identification of real-time audio and video traffic. The following section provides information about the NBAR Real-Time Transport Protocol Payload Classification feature:
NBAR--Network-Based Application Recognition	12.2(18)ZYA	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. The following sections provide information about the NBAR feature: The following command was modified: **match protocol (NBAR)**.
NBAR--Network-Based Application Recognition (Hardware Accelerated NBAR)	12.2(18)ZY	Enables NBAR functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA). The following section provides information about the NBAR--Network-Based Application Recognition (Hardware Accelerated NBAR) feature:

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.