

Network-Based Application Recognition

Last updated: September 2008

Common questions and answers regarding Cisco® Network-Based Application Recognition (NBAR) follow.

Q. What is NBAR?

A. NBAR, an important component of the Cisco Content Networking architecture, is a new classification engine in Cisco IOS® Software that can recognize a wide variety of applications, including Web-based applications and client/server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality-of-service (QoS) features to help ensure that the network bandwidth is best used to fulfill your business objectives.

Q. Why would I want NBAR?

A. Today's applications require high performance to help ensure competitiveness in an increasingly fast-paced business environment. The network can provide a variety of services to help ensure that your mission-critical applications receive the bandwidth they need to provide this performance. The difficulty is that today's Internet-based and client-server applications make it difficult for the network to identify and provide the proper level of control you need. NBAR solves this problem by adding intelligent network classification to your infrastructure.

Q. How does NBAR fit into the Content Networking framework?

A. NBAR provides intelligent network classification that can be used to determine which services the network should provide. NBAR currently works with QoS features so that one can provide differentiated classes of service (CoSs) to different applications.

Q. What are some of the benefits of using NBAR?

- A.** The benefits include the following:
- **Help Ensure Performance for Mission-Critical Applications:** NBAR allows the network to provide differentiated services to each application. You can provide absolute priority and guaranteed bandwidth to your mission-critical applications such as Oracle or an application that runs on a particular Web page. At the same time you can limit the bandwidth consumed by the less essential applications. The end result is that users can access their mission-critical applications with minimal delay without the need to upgrade costly WAN links or cutting off access to commonly used, but not mission-critical, applications.
 - **Reduce WAN Expenses:** In many parts of the world, and especially between countries, telecommunications links can still be prohibitively expensive. This leads to a dilemma for the network manager: on the one hand you need to provide access to new client-server and Internet-enabled applications, while on the other hand you need to control WAN service costs. NBAR provides a solution to this problem by enabling you to intelligently

utilize WAN bandwidth so that you can provide acceptable service levels with the minimum possible bandwidth.

- **Manage Web Response:** The Web is now a critical business resource in many enterprises, for both internal and external communications. Employees, partners, and customers must have access to the Web pages they need without such problems as slow downloads or Web-based application failure. NBAR allows you to identify the Web pages and type of Web content that you deem critical.
- **Improve VPN Performance:** VPNs often reduce networking costs while providing increased flexibility. Unfortunately, the service quality in a VPN is often difficult to guarantee. Running NBAR and VPN concurrently in the same router solves this problem by identifying mission-critical traffic before it is encrypted, allowing the network to apply the appropriate QoS controls. By running both VPN and NBAR concurrently, we help ensure that the packets are processed in the correct order to achieve both maximum security and the appropriate QoS. NBAR can also mark the tunnel packet so that the service provider can provide differentiated service to different applications on the service provider's WAN.
- **Improve Multiservice Performance:** Multiservice networks allow you to combine your data, voice, and video requirements into one unified network. Unfortunately, each of these services requires different network characteristics. NBAR is able to intelligently identify the type of each packet and provide the proper network characteristics.

Q. What distinguishes the Cisco NBAR offering?

A. Enterprises that implement Cisco NBAR will be able to intelligently classify network traffic without the need for costly additions to the network infrastructure. Other solutions require the addition of an exterior device for each and every WAN link. The Cisco solution requires a simple software upgrade to your network's existing routers.

Q. Will NBAR be able to support new and emerging applications?

A. Cisco Systems® created NBAR to be extremely flexible. Cisco can deliver new application support easily through a protocol description language module (PDLM). PDLMs contain the rules used by NBAR to recognize an application and can usually be loaded without the need for a Cisco IOS Software upgrade or router reboot.

Details

Q. What platforms and Cisco IOS® Software releases support NBAR?

- A.** NBAR is supported on the following platforms:
- Cisco 800 Series Routers
 - Cisco 1700 Series Modular Access Routers
 - Cisco 1800 Series Integrated Services Routers
 - Cisco 2600XM Series Router
 - Cisco 2800 Series Integrated Services Routers
 - Cisco 3700 Series Multiservice Access Routers
 - Cisco 3800 Series Integrated Services Routers
 - Cisco 7100 Series VPN Routers
 - Cisco 7200 Series Routers

- Cisco 7300 Series Routers
- Cisco 7500 Series Routers

Please refer to the link below for Cisco IOS Software releases for NBAR support:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455985.html

Q. Which protocols can NBAR classify?

A. NBAR supports a wide range of network protocols, including the stateful protocols that were difficult to classify before NBAR. Tables 1 through 5 show some of the supported protocols and descriptions.

Table 1. Peer-to-Peer Protocols

Peer-to-Peer Protocol	Type	Description
BitTorrent	TCP	File-sharing application
Gnutella	TCP	File-sharing application
Kazaa2	TCP	File-sharing application
eDonkey	TCP	File-sharing application
Fasttrack	TCP	File-sharing application
Napster	TCP	File-sharing application

Table 2. VoIP Protocols

VoIP Protocol	Type	Description
SCCP	TCP	Skinny Call Control Protocol
SIP	TCP and UDP	Session Initiation Protocol
MGCP	TCP and UDP	Media Gateway Control Protocol
H.323	TCP and UDP	An ITU-T standard for digital videoconferencing over TCP/IP networks
SKYPE ¹	TCP and UDP	Application allowing telephone conversation over the Internet

Table 3. TCP and UDP Stateful Protocols

TCP or UDP Stateful Protocol	Type	Description
FTP	TCP	File Transfer Protocol
Exchange	TCP	MS-RPC for Exchange
HTTP	TCP	HTTP with URL, host, or MIME classification
Citrix	TCP	Citrix published application
Netshow	TCP/UDP	Microsoft Netshow
RealAudio	TCP/UDP	RealAudio Streaming Protocol
r-commands	TCP	rsh, rlogin, rexec
StreamWorks	UDP	Xing Technology Stream Works audio/video
SQL*NET	TCP/UDP	SQL*NET for Oracle
SunRPC	TCP/UDP	Sun Remote Procedure Call
TFTP	UDP	Trivial File Transfer Protocol
VDOLive	TCP/UDP	VDOLive streaming video

¹ Currently, Cisco only supports Skype version 1

Table 4. Non-UDP and Non-TCP Protocols

Non-UDP or Non TCP Protocol	Type	Well-Known Port Number	Description
EGP	IP	8	Exterior Gateway Protocol
GRE	IP	47	Generic Routing Encapsulation
ICMP	IP	1	Internet Control Message Protocol
IPINIP	IP	4	IP in IP
IPsec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol

Table 5. TCP and UDP Static Port Protocols

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
BGP	TCP/UDP	179	Border Gateway Protocol
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing
CU-SeeMe	UDP	24032	Desktop videoconferencing
DHCP/Bootp	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol
DNS	TCP/UDP	53	Domain Name System
Finger	TCP	79	Finger User Information Protocol
Gopher	TCP/UDP	70	Internet Gopher Protocol
HTTP	TCP	80	Hypertext Transfer Protocol
HTTPS	TCP	443	Secured HTTP
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol
IRC	TCP/UDP	194	Internet Relay Chat
Kerberos	TCP/UDP	88, 749	The Kerberos Network Authentication Service
L2TP	UDP	1701	L2F/L2TP Tunnel
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol
MS-SQLServer	TCP	1433	Microsoft SQL Server
NetBIOS	TCP	137, 139	NetBIOS over IP (Microsoft Windows)
NetBIOS	UDP	137, 138	NetBIOS over IP (Microsoft Windows)
NFS	TCP/UDP	2049	Network File System
NNTP	TCP/UDP	119	Network News Transfer Protocol
Notes	TCP/UDP	1352	Lotus Notes
NTP	TCP/UDP	123	Network Time Protocol
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere
POP3	TCP/UDP	110	Post Office Protocol
PPTP	TCP	1723	Point to Point Tunneling Protocol
RIP	UDP	520	Routing Information Protocol
RSVP	UDP	1698,1699	Resource Reservation Protocol
SFTP	TCP	990	Secure FTP
SHTTP	TCP	443	Secure HTTP
SIMAP	TCP/UDP	585, 993	Secure IMAP
SIRC	TCP/UDP	994	Secure IRC
SLDAP	TCP/UDP	636	Secure LDAP
SNNT	TCP/UDP	563	Secure NNTP

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
SMTP	TCP	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol
SOCKS	TCP	1080	Firewall security protocol
SPOP3	TCP/UDP	995	Secure POP3
SSH	TCP	22	Secured Shell
STELNET	TCP	992	Secure TELNET
Syslog	UDP	514	System Logging Utility
Telnet	TCP	23	Telnet Protocol
X Windows	TCP	6000-6003	X11, X Windows

Q. How do I classify HTTP traffic?

A. You can classify HTTP traffic by URL, host, or MIME type. When classifying by URL and host, you can use full regular expressions to define the class. For example, you could put everything under the /stock/ directory into a single class.

Q. Can NBAR provide smaller granularity than just by application?

A. The packet description language allows NBAR to classify not just the application, but also subprocesses within an application. This is what NBAR uses for HTTP classification today.

Q. How do I add support for a new application?

A. Cisco will provide new PDL files to describe new and requested applications. The PDL can usually be loaded without changing the Cisco IOS Software image and without a reload.

Q. Which services can be used with NBAR?

A. The following are the services that can be used with NBAR:

- Guaranteeing bandwidth with Class-Based Weighted Fair Queuing (CBWFQ)
- Policing and limiting bandwidth
- Marking for differentiated service downstream or from the service provider (ToS or Diff Serv code points [DSCP])
- Drop policy to avoid congestion (Weighted Random Early Detection [WRED])

Q. Which switching paths will NBAR support on Cisco IOS Software?

A. NBAR supports the Cisco Express Forwarding switching path.

Q. What type of performance can I expect with NBAR?

A. NBAR can classify stateful protocols with 300-byte packets with average flow lengths at 90 Mbps with just a 15 percent increase in CPU. For protocols classified by static port numbers, NBAR performs about the same as traditional access control lists (ACLs).

Q. How do I configure NBAR?

A. NBAR can be configured by the command-line interface (CLI) as part of the new modular CLI for QoS. The modular CLI separates the configuration process into two parts: the definition of classes and then the application of QoS mechanisms to each class. NBAR can be used to define to which class a given application belongs.

Q. How do I manage NBAR with an application other than the CLI?

A. QoS Policy Manager (QPM) 1.1 will be able to manage NBAR. QPM provides an enterprise-wide QoS policy management system that can provide policy for many devices within the network. QoS Device Manager, also known as QDM, is a network management application used for configuring and monitoring QoS functionality within Cisco routers and supports NBAR.

Q. Is a MIB available to monitor NBAR?

A. Yes. The CISCO-NBAR-PROTOCOL-DISCOVERY MIB is available for monitoring NBAR. This MIB contains information such as input and output byte and packet counts.

Q. What information is provided by the protocol discovery feature?

A. Protocol discovery shows you the mix of applications currently running on the network. This helps you define QoS classes and policies, such as how much bandwidth to provide to mission-critical applications and how to determine which protocols should be policed. The following per-protocol, bidirectional statistics are available:

- Packet and byte counts
- Bit rates

Q. How much memory does NBAR use?

A. NBAR uses 150 bytes of DRAM to track each stateful protocol flow. By default, NBAR allocates 1 MB of memory for flow resources, allowing NBAR to track about 5000 stateful flows without allocating more memory. NBAR will automatically allocate additional memory if needed.

Q. Can NBAR classify IPX traffic?

A. IPX traffic is currently not being classified by NBAR.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)