Network-Based Application Recognition

Last Updated: March 2009

Cisco® Content Networking delivers the network agility required by the enterprise to deploy new Internet business applications critical to securing competitive advantage by increasing revenue while reducing operating costs. By creating end-to-end intelligent network services required for Internet business applications such as e-commerce, supply chain management, and workforce optimization, Cisco Content Networking integrates the enterprise with customers, suppliers, and business partners.

Content Networking

Cisco Content Networking is an intelligent network architecture that dynamically recognizes Internet business applications and engages network services to achieve end-to-end security, performance, and availability. This architecture has three components:

- Intelligent network classification and network services delivered through Cisco IOS® Software
- Intelligent network devices that integrate Internet business applications with network services
- An intelligent policy management framework for configuration, monitoring, and accounting

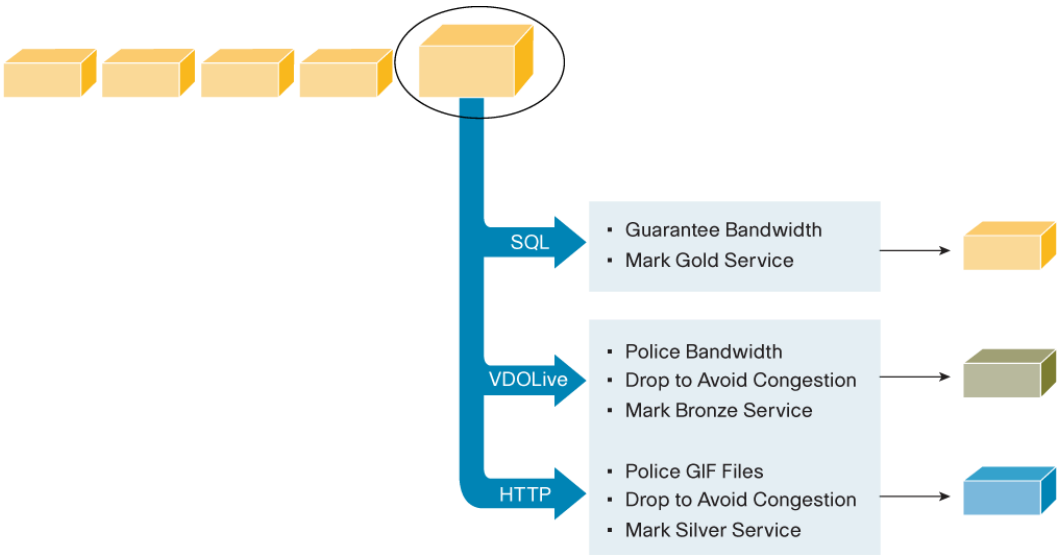
With these three components, the dynamic architecture of Cisco Content Networking delivers the intelligent network services required to promote the next-generation Internet business model.

Network-Based Application Recognition Overview

Network-Based Application Recognition (NBAR), a feature first available in Cisco IOS Software Release 12.0(5)XE2, provides intelligent network classification for network infrastructure. NBAR is a classification engine 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 the company's objectives. These features include the ability to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and mark packets appropriately so that the network and the service provider's network can provide QoS from end to end.

For example, your customer service representatives require a fast response when they query for an order status in the corporate data warehouse hosted on an Oracle database server. Unfortunately, if others on the network are using high-bandwidth applications, such as VDOLive, or viewing large GIF files, then the SQL*NET transaction to the Oracle database may be delayed. NBAR addresses this problem by properly classifying the applications and then providing guaranteed bandwidth to the SQL*NET queries while simultaneously policing the other applications. Figure 1 illustrates this solution.

Figure 1. NBAR Provides Intelligent Network Classification



Features at a Glance

NBAR intelligently classifies and allows you to enforce QoS policy on today's mission-critical applications.

- NBAR supports a wide range of network protocols, including some of these stateful protocols that were difficult to classify before NBAR:
  - HTTP classification by URL, host, and Multipurpose Internet Mail Extensions (MIME) type
  - Oracle SQL*Net
  - Sun RPC
  - Microsoft Exchange
  - UNIX r commands
  - VDOLive
  - RealAudio
  - Microsoft Netshow
  - FTP
  - StreamWorks
  - Trivial File Transfer Protocol (TFTP)
- NBAR also classifies traditional static port protocols for supporting a wide range of solutions. The complete list is given at the end of this document.
- Support for new protocols can be easily and quickly added using packet description language modules (PDLMs) from Cisco Systems®. PDLMs contain the rules used by NBAR to recognize an application and in most cases can be loaded without the need for a new Cisco IOS Software image or even a reboot.
- Protocol discovery shows you the mix of applications currently running on the network. This helps you define QoS classes and polices, 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

- After applications are intelligently classified, the network can apply the following QoS features:
  - Guaranteed bandwidth with Class-Based Weighted Fair Queuing (CBWFQ)
  - Enforce bandwidth limits using policing
  - Marking for differentiated service downstream or from the service provider using type of service (ToS) bits or Diff Serv code points (DSCPs) in the IP header
  - Drop policy to avoid congestion (Weighted Random Early Detection [WRED])

Benefits and Applications

Help Ensure Performance for Mission-Critical Applications

Mission-critical applications, such as Oracle, Citrix, Microsoft Exchange, or the new breed of Web-based applications, must perform well to help ensure your success in today's fast-paced e-business environment. Bottlenecks can occur in many places, including the network. These bottlenecks often occur even though you have budgeted what you thought was more than adequate bandwidth for each application.

What often happens is that employees take advantage of new Internet applications, such as streaming audio and video or downloading of new programs. All of these applications can quickly consume your WAN bandwidth. Unfortunately, these are not typically the mission-critical applications to which you want to give network priority.

By intelligently classifying applications, NBAR allows the network to provide differentiated services to each application. You can provide absolute priority and a guaranteed amount of 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 less critical 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

The cost of WAN bandwidth has decreased significantly over the last decade, especially in deregulated markets. However, 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.

NBAR will identify your mission-critical applications so that you can assign them higher priority or guaranteed bandwidth on the link. This helps ensure that the noncritical applications do not overwhelm these slower international links and bring your mission-critical traffic to a halt.

Improve 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. For example:

- Customers accessing the sales ordering page would be given priority. This prevents the customer from getting frustrated at the point of sale.
- Sales tools can be given absolute priority and guaranteed bandwidth, helping ensure that your sales force is never forced to wait for a price quote because another employee is browsing the latest version of the firm's new television commercial on streaming video.
- Web-based applications often load slowly. With NBAR, applications can be identified by MIME type and be given priority in the network.
- Some classes of content, such as JPEG pictures, consume large amounts of bandwidth, but may not be considered critical Web-based information. In such cases, you can control the amount of bandwidth consumed by such types of content.

Improve VPN Performance

VPNs often reduce networking costs while providing increased flexibility. Unfortunately, the service quality in a VPN is difficult to guarantee. Running NBAR and a 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 a 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.

If a remote employee accesses a critical enterprise resource planning (ERP) application, NBAR will identify the packet, mark it as a "gold-service" packet, and place it into a priority queue. The VPN processes will then tunnel and encrypt the packet while maintaining the "gold-service" marking on the new packet. When used with service providers that offer differentiated services on their networks, the ERP application will receive priority treatment as it travels through the VPN. Other, less-critical applications accessed by the same employee may be given lower-priority service.

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.

For example, if you deploy a training system that utilizes streaming video, such as the Cisco IP/TV® solution, you will want to try to ensure that employees see a clean picture, not one that is choppy and hard to understand. With NBAR, the network can easily recognize the streaming video traffic and assign it to a higher priority class of traffic that receives a minimum guaranteed bandwidth. Other traffic, such as e-mail, can be assigned to a lower priority class, because e-mail must be delivered, but it does not have the latency and bandwidth constraints of the streaming video. The end result is that trainees receive their video training on demand with high quality while the network concurrently serves other applications.

Availability and Orderability

NBAR is a component of Cisco IOS Software and is available in most software platforms. Please refer to the Feature Navigator link in the reference section of this document for supported hardware and software versions.

Table 1 shows a summary of NBAR features and benefits.

Table 1. NBAR Features and Benefits Summary

Feature	Comment/Description	Benefit
Intelligently Classify Applications	Web-based and client/server applications cannot be recognized by traditional classification technologies, such as access control lists (ACLs). NBAR adds intelligent classification to recognize these applications.	Mission-critical applications can be given priority by the network to help ensure that they can be used without network-induced delay.
New Protocols Can Be Quickly Added to NBAR	NBAR uses a flexible packet description language that allows Cisco to easily and quickly add support for new applications. The new PDLM can be loaded without changing Cisco IOS Software releases and without rebooting the router.	In today's rapidly changing environment, it is impossible to predict the next critical application. NBAR provides the flexibility so that you can be sure Cisco will be able to support these new applications in a timely way.
Protocol Discovery	NBAR can determine which protocols and applications are currently running on your network.	Before creating a QoS policy, you must first understand your current traffic mix and application requirements. Protocol discovery provides the information to make this critical first step.
Support for QoS	After intelligently classifying the packet by NBAR, the router will utilize an underlying QoS service to provide differentiated services. The following services are supported: Guaranteed bandwidth with CBWFQ Policing and limiting bandwidth Marking for differentiated service downstream or from the service provider (ToS or DSCP) Drop policy to avoid congestion (WRED)	The underlying QoS features are what provide the differentiated services to the network, enabling you to help ensure your mission-critical applications receive priority and are not slowed down by noncritical traffic.

Protocols Supported by NBAR

NBAR supports the protocols listed in Tables 2 through 4.

Table 2. Non-UDP and Non-TCP Protocols

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Software Release
EGP	IP	8	Exterior Gateway Protocol	egp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
GRE	IP	47	Generic Routing Encapsulation	gre	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
ICMP	IP	1	Internet Control Message Protocol	icmp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
IPINIP	IP	4	IP in IP	ipinip	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
IPsec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header	ipsec	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T

Table 3. TCP and UDP Static Port Protocols

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Software Release[1]
BGP	TCP/UDP	179	Border Gateway Protocol	bgp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Software Release[1]
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing	cuseeme	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
CU-SeeMe	UDP	24032	Desktop videoconferencing	cuseeme	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
DHCP/BOOTP	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol	dhcp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
DNS	TCP/UDP	53	Domain Name System	dns	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Finger	TCP	79	Finger user information protocol	finger	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Gopher	TCP/UDP	70	Internet Gopher Protocol	gopher	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
HTTP	TCP	80	Hypertext Transfer Protocol	http	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
HTTPS	TCP	443	Secured HTTP	secure-http	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol	imap	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
IRC	TCP/UDP	194	Internet Relay Chat	irc	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Kerberos	TCP/UDP	88, 749	Kerberos Network Authentication Service	kerberos	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
L2TP	UDP	1701	L2F/L2TP tunnel	l2tp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
MS-PPTP	TCP	1723	Microsoft Point-to-Point Tunneling Protocol for VPN	pptp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
NetBIOS	TCP	137, 139	NetBIOS over IP (MS Windows)	netbios	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
NetBIOS	UDP	137, 138	NetBIOS over IP (MS Windows)	netbios	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
NFS	TCP/UDP	2049	Network File System	nfs	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
NNTP	TCP/UDP	119	Network News Transfer Protocol	nntp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Notes	TCP/UDP	1352	Lotus Notes	notes	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Novadigm	TCP/UDP	3460-3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	Release 12.1(2)E and 12.1(5)T
NTP	TCP/UDP	123	Network Time Protocol	ntp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere	pcanywhere	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere	pcanywhere	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
POP3	TCP/UDP	110	Post Office Protocol	pop3	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Printer	TCP/UDP	515	Printer	printer	Release 12.1(2)E and 12.1(5)T
RIP	UDP	520	Routing Information Protocol	rip	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Software Release[1]
RSVP	UDP	1698, 1699	Resource Reservation Protocol	rsvp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SFTP	TCP	990	Secure FTP	secure-ftp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SHTTP	TCP	443	Secure HTTP	secure-http	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SIMAP	TCP/UDP	585, 993	Secure IMAP	secure-imap	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SIRC	TCP/UDP	994	Secure IRC	secure-irc	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SLDAP	TCP/UDP	636	Secure LDAP	secure-ldap	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SMTP	TCP	25	Simple Mail Transfer Protocol	smtp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol	snmp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SNNTP	TCP/UDP	563	Secure NNTP	secure-nntp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SOCKS	TCP	1080	Firewall security protocol	socks	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SPOP3	TCP/UDP	995	Secure POP3	secure-pop3	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SSH	TCP	22	Secured Shell	ssh	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
STELNET	TCP	992	Secure Telnet	secure-telnet	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Syslog	UDP	514	System Logging Utility	syslog	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Telnet	TCP	23	Telnet Protocol	telnet	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
X Windows	TCP	6000-6003	X11, X Windows	xwindows	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T

Table 4. TCP and UDP Stateful Protocols

Protocol	Type	Description	Syntax	Cisco IOS Software Release
Citrix ICA	TCP/UDP	Citrix ICA traffic by application name	citrix app	Release 12.1(2)E and 12.1(5)T
FTP	TCP	File Transfer Protocol	ftp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
Exchange	TCP	MS-RPC for Exchange	exchange	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
FastTrack		FastTrack For a list of common FastTrack applications, go to: Classification of Peer-to-Peer File-Sharing Applications	fasttrack	Release 12.1(12c)E
Gnutella	TCP	Gnutella For a list of common Gnutella applications, go to: Classification of Peer-to-Peer File-Sharing Applications	gnutella	Release 12.1(12c)E
HTTP	TCP	HTTP with URL, MIME, or host classification	http	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T (HTTP host classification is not available on the 12.0 XE release train)
Napster	TCP	Napster traffic	napster	Release 12.1(5)T
Netshow	TCP/UDP	Microsoft Netshow	netshow	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T

Protocol	Type	Description	Syntax	Cisco IOS Software Release
R-Commands	TCP	rsh, rlogin, rexec	Rcmd	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
RealAudio	TCP/UDP	RealAudio Streaming Protocol	realaudio	Release 12.0(5)XE2,12.1(1)E and 12.1(5)T
RTP	TCP/UDP	Real-Time Transport Protocol Payload Classification	rtp	Release 12.2(8)T
SQL*NET	TCP/UDP	SQL*NET for Oracle	sqlnet	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
StreamWorks	UDP	Xing Technology Stream Works audio and video	streamwork	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
SunRPC	TCP/UDP	Sun Remote Procedure Call	sunrpc	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
TFTP	UDP	Trivial File Transfer Protocol	tftp	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T
VDOLive	TCP/UDP	VDOLive Streaming Video	vdolive	Release 12.0(5)XE2, 12.1(1)E and 12.1(5)T

References

- Configuring Network-Based Application Recognition: http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfnbar.pdf
- NBAR Packet Description Language Modules: http://www.cisco.com/cgi-bin/tablebuild.pl/pdlm
- Feature Navigator: http://www.cisco.com/go/fn

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.

Printed in USA C36-495722-01 03/09