



DATA SHEET

AUTOMATION FOR QUALITY OF SERVICE DEPLOYMENTS: CISCO AUTOQOS

Last Updated: September 2005

Cisco® AutoQoS represents innovative technology that simplifies a network administrator's challenges by reducing Quality-of-Service (QoS) complexity and deployment time and cost in Enterprise networks. Cisco AutoQoS incorporates value-added intelligence in Cisco IOS® Software and Cisco Catalyst® OS software to provision and manage large-scale QoS deployments.

The first phase of Cisco AutoQoS offers straightforward capabilities to automate Voice-over-IP (VoIP) deployments for customers who want to deploy IP telephony, but who lack the expertise and/or staffing to plan and deploy IP QoS and IP services.

Customers can more easily provision and manage successful QoS deployments using Cisco AutoQoS together with CiscoWorks QoS Policy Manager (Cisco QPM). Cisco AutoQoS provides QoS provisioning for individual routers and switches, simplifying deployment and reducing human error. Cisco QPM provides centralized QoS design, administration, and traffic monitoring that scales to large QoS deployments.

QUALITY-OF-SERVICE DEPLOYMENT OVERVIEW

Cisco AutoQoS simplifies and shortens the QoS deployment cycle. The five major aspects of successful QoS deployments are:

1. Application classification
2. Policy generation
3. Configuration
4. Monitoring and reporting
5. Consistency

Each aspect presents challenges to the network manager.

Application Classification

The first step in deploying QoS is identifying and categorizing the network traffic generated by each application. Access control lists (ACLs) are the most commonly used tools for identifying traffic. ACLs use information from Layer 3 (IP addresses) and Layer 4 (TCP/User Datagram Protocol [UDP] port numbers) to identify traffic. However, using ACLs alone to deploy QoS rapidly increases the size and number of ACLs required in a network. Furthermore, they cannot easily identify all applications (that is, various kinds of HTTP traffic).

Policy Generation

Developing the initial QoS policy often challenges customers, who must balance QoS policy variables (bandwidth, delay, jitter, and packet loss) to achieve the desired application performance. Cisco QoS empowers the network manager to set policies for delivering the desired application performance for the business; however, many customers lack the required expertise to arrive at a starting point for their QoS policies.



Configuration

Network devices need to be programmed with the right set of features and parameters to implement the policy. Although QoS is rich in features, the process of effective implementation is time-consuming. Without automation, the QoS configuration challenge can be very complex.

Monitoring and Reporting

Customers are often deluged with large quantities of data, but very little relevant information that helps them to identify the cause of a problem or any important trends (for example, traffic patterns and exceptions). Obtaining the right information can be quite expensive, and it often arrives too late to be useful. A typical example is finding out “who” (that is, which user or IP address) is causing congestion or creating abnormal loads on a link. Without automation, establishing an efficient monitoring process can take many months.

Consistency

Customers are faced with managing QoS policies consistently across multiple kinds of devices in the network, including IP phones, switches, and routers. Different devices and vendors often implement QoS functionality differently, creating a challenge for the network manager.

CISCO AUTOQOS: A NEW PARADIGM FOR SIMPLIFYING QUALITY OF SERVICE

Cisco AutoQoS provides a new paradigm for automating the delivery of network QoS. It simplifies the provisioning of network QoS with intelligence and shortens the QoS deployment cycle.

Customers can use Cisco AutoQoS to:

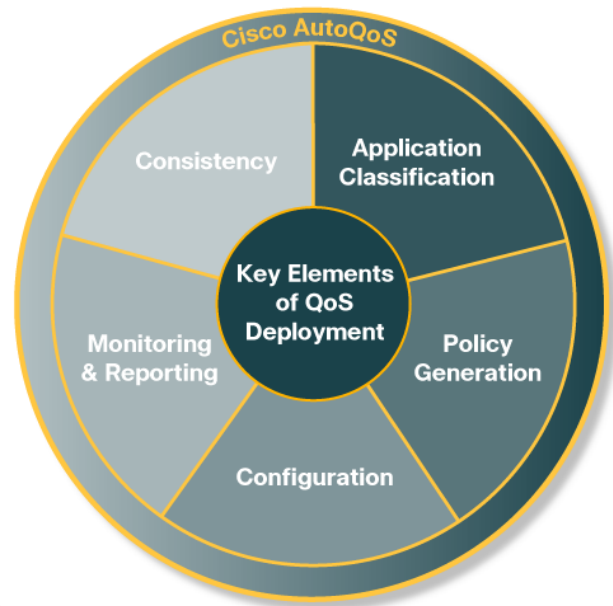
- Get a quick start on QoS deployment
- Automate the most common deployment scenarios
- Identify and classify applications
- Establish alert conditions

Cisco AutoQoS addresses the major elements of end-to-end QoS deployments, using decades of networking experience, extensive lab performance testing, and input from a broad base of customer AVVID (Architecture for Voice, Video and Integrated Data) installations to determine the optimal QoS configuration for typical VoIP deployments. (See Figure 1.)

Figure 1. Cisco AutoQoS: Simplifying QoS Deployment

Agile QoS Deployment for VoIP Using Cisco AutoQoS-VoIP and CiscoWorks QPM

- **Application Classification**
 - AutoQoS identifies VoIP bearer and control traffic
- **Policy Generation**
 - AutoQoS evaluates the network environment and generates initial policy on a given Port, Interface or PVC
- **Configuration**
 - AutoQoS provides a single command to enable QoS on each interface/PVC
 - QPM provides centralized network-wide configuration, management and monitoring
- **Monitoring & Reporting**
 - Traps issued on VoIP packet drops
 - QPM uses data received from network devices to generate QoS reports
- **Consistency**
 - AutoQoS is fully inter-operable between LAN & WAN devices



Cisco AutoQoS—Simplifying QoS Deployment

Cisco AutoQoS addresses the five key elements of QoS deployment.

Application Classification

Cisco AutoQoS uses intelligent classification on routers, utilizing Cisco Network-Based Application Recognition (NBAR) to provide deep and stateful packet inspection. Cisco AutoQoS uses Cisco Discovery Protocol for voice packets, helping ensure that the device attached to the LAN is really an IP phone.

Policy Generation

Cisco AutoQoS evaluates the network environment and generates an initial policy. It automatically determines WAN settings for fragmentation, compression, encapsulation, and Frame Relay-ATM interworking, eliminating the need to understand QoS theory and design practices in various scenarios. Customers can meet additional or special requirements by modifying the initial policy as they normally would.

The first release of Cisco AutoQoS provides the necessary AutoQoS-VoIP feature to automate QoS settings for VoIP deployments. This feature automatically generates interface configurations, policy maps, class maps, and ACLs. AutoQoS-VoIP will automatically employ Cisco NBAR to classify voice traffic and mark it with the appropriate differentiated services code point (DSCP) value. AutoQoS-VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.

Configuration

With one command, Cisco AutoQoS configures the port to prioritize voice traffic without affecting other network traffic, while still offering the flexibility to adjust QoS settings for unique network requirements.

Not only will Cisco AutoQoS automatically detect Cisco IP phones and enable QoS settings; it also will disable the QoS settings when a Cisco IP Phone is relocated or moved to prevent malicious activity.

Monitoring and Reporting

Cisco AutoQoS provides visibility into the classes of service deployed using system logging and Simple Network Management Protocol (SNMP) traps, with notification of abnormal events (for example, VoIP packet drops).

Cisco QPM uses the Cisco Systems® intelligent IP network to provide visibility into network operations. Users can measure traffic throughput for top applications and service classes; they can also troubleshoot problems with real-time and historical QoS feedback. Traffic and QoS statistics can be displayed as line or bar charts in bits or packets per second, per interface or policy. Cisco QPM enables a user to view graphs before and after QoS deployment, tied to traffic filters and policies, as well as results from QoS policy actions.

Consistency

Cisco AutoQoS policies are designed to work together across Cisco devices, helping ensure consistent end-to-end QoS.

Cisco QPM enables users to view:

- Statistics matching policies and specific filters, including Cisco NBAR application filters
- Traffic rate before any QoS policy actions, traffic transmitted after QoS policy actions, and traffic dropped (rather than transmitted) because of QoS policy drop actions
- QoS action statistics: Weighted Random Early Detection (WRED), policing, traffic shaping, queuing

For additional information, please visit <http://www.cisco.com/en/US/products/sw/cscowork/ps2064/index.html>.

FEATURES AND BENEFITS

Cisco AutoQoS simplifies deployment and speeds provisioning of QoS technology over a Cisco network infrastructure. It reduces human error and lowers training costs. With AutoQoS-VoIP, you use just one command to enable QoS for VoIP across every Cisco router and switch. You can also modify an AutoQoS-generated policy to meet your specific requirements.

Tables 1 and 2 detail the initial Cisco AutoQoS features for Cisco IOS Software and Cisco Catalyst OS software.

Table 1. Cisco AutoQoS for VoIP in the WAN

Feature	Benefit
Autodetermination of WAN Settings	Automatic determination of WAN settings for fragmentation and interleaving, compression, encapsulation, and Frame Relay-ATM interworking. Eliminates the need to understand QoS theory and design practices in common deployment scenarios.
Initial Policy Generation	Initial policy generation provides users an advanced starting point for VoIP deployments. This reduces the time needed to establish an initial, feasible QoS policy solution that includes providing QoS to VoIP bearer traffic, signaling traffic, and best-effort data. The initial policy can be modified to meet additional or special requirements.
Traps and Reporting	Syslog and SNMP traps provide visibility into the classes of service deployed and notification of abnormal events such as VoIP packet drops.
Intelligent Classification of Network Traffic	Using Cisco NBAR for deep and stateful packet inspection, this feature can identify VoIP bearer and control traffic. Simplifies QoS configurations by reducing, and in some cases eliminating, the need for ACLs.

Table 2. Cisco AutoQoS for VoIP in the LAN

Feature	Benefit
Simplified Configuration	<ul style="list-style-type: none">• In one command, AutoQoS configures the port to prioritize voice traffic without affecting other network traffic.• Includes the flexibility to tune AutoQoS settings for unique network requirements.
Automated and Secure	<ul style="list-style-type: none">• Automatically detects Cisco IP phones and enables AutoQoS settings (Cisco Catalyst 2900 and 3750 Series Switches and Cisco Catalyst 3500 XL Series Switches).• Prevents malicious activity by disabling QoS settings when a Cisco IP Phone is relocated/moved.
Optimal VoIP Performance	<ul style="list-style-type: none">• Uses decades of networking experience, extensive lab performance testing, and input from a broad base of customer AVVID installations to determine the optimal QoS configuration for typical VoIP deployments.• Uses all advanced QoS capabilities of the Cisco Catalyst switches.
End-to-End Interoperability	<ul style="list-style-type: none">• Designed to work well with the AutoQoS settings on all other Cisco switches and routers, helping ensure consistent end-to-end QoS.

CiscoWorks QoS Policy Manager

Although Cisco AutoQoS allows a user to configure QoS at the device level, enterprises will use Cisco QPM to cost-effectively manage QoS in their IP network. This enables in-depth analysis, intelligent QoS design, and scalable deployment. (See Table 3.)

Table 3. CiscoWorks QPM Features and Benefits

Feature	Benefit
Policy Configuration Wizards	CiscoWorks QPM wizards intelligently guide users through campus-to-WAN QoS policy configuration, while Cisco-defined and customer-defined policy libraries simplify global QoS configuration for voice, video, and data.
Traffic Throughput Measurement and QoS Feedback	CiscoWorks QPM enables the user to measure traffic throughput for top applications, including IP telephony, and service classes; they can also troubleshoot problems with real-time and historical QoS feedback.

For additional information about CiscoWorks QoS Policy Manager 3.2, please visit

http://cisco.com/en/US/products/sw/cscowork/ps2064/products_data_sheet09186a0080091bcf.html.

PLATFORM SUPPORT

Table 4 details platform support for the initial release of Cisco AutoQoS, which provides automatic, end-to-end QoS provisioning for VoIP traffic.

Table 4. Cisco AutoQoS Platform Support

	Platforms	Software
Switches	Cisco Catalyst 2970 Series Switch	Cisco IOS Software Release 12.2(25)SE
	Cisco Catalyst 3560 Series Switch	Release 12.2(25)SE
	Cisco Catalyst 3750 Series Switch	Release 12.2(20)EX
	Cisco Catalyst 4500 Series Switch	Release 12.1(19)E
	Cisco Catalyst 6500 Series Switch	Cisco Catalyst Operating System 7.5.1
Routers	Cisco 800 Series Router	Release 12.4(2)T
	Cisco 1700 Series Modular Access Router	Release 12.3(14)T
	Cisco 1800 Series Integrated Services Router	Release 12.3(8)T
	Cisco 2600XM Series Router	Release 12.2(15)T
	Cisco 2800 Series Integrated Services Router	Release 12.3(11)T
	Cisco 3700 Series Multiservice Access Router	Release 12.2(15)T
	Cisco 3800 Series Integrated Services Router	Release 12.3(11)T
	Cisco 7200 Series Router	Release 12.2(15)T
	Cisco 7301 Series Router	Release 12.3(7)T

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)

205393.F_ETMG_PI_9.05