

CiscoWorks QoS Policy Manager 3.2

The need for high availability and predictable performance for business-critical applications, combined with the demand for voice and video services, mandates differentiated handling of network traffic. CiscoWorks QoS Policy Manager (QPM) 3.2 is a secure, Web-based tool that enables end-to-end quality of service (QoS) for converged data, voice, and video networks. As part of the CiscoWorks solution family, QPM 3.2 combines traffic monitoring with configuration of Differentiated Services (DiffServ) across the IP infrastructure by taking advantage of the Cisco IOS[®] Software and Cisco[®] Catalyst[®] Operating System (CatOS) QoS mechanisms built into LAN and WAN switching and routing equipment.

Features

- *Traffic monitoring for setting and validating QoS*—Users can measure traffic throughput for top applications and service classes plus troubleshoot problems with real-time and historical QoS feedback.
- *Advanced user administration and security*—Users can centrally define roles and permissions and take advantage of Cisco Secure Access Control Server (ACS) to control privileges for policy view, modification, and deployment for different device groups.
- *Support for large-scale QoS deployments*—Users can partition the network into administrative and deployment domains and use policy libraries for global QoS configuration.
- *Centralized Web-based control*—The secure, Web-based GUI provides accurate, end-to-end QoS configuration and automated, reliable policy deployment, while eliminating device-by-device command streams.
- *Automated QoS provisioning for voice over IP (VoIP)*—Users can use a setup wizard to intelligently determine QoS policies and properties at each network point that requires IP telephony QoS configuration based on Cisco AVVID (Architecture for Voice, Video and Integrated Data) design recommendations.
- *DiffServ for various types of traffic*—Business-driven service levels are achieved across the enterprise network by configuring traffic classification and allowing QoS policy enforcement through Cisco devices.
- *Extensive application-level classification*—An integral part of Cisco content networking, CiscoWorks QPM 3.2 delivers the appropriate service levels to business-critical applications by supporting the extension of IP packet classification to include application signature, Web URLs, and negotiated ports..



- *Structured traffic management*—This feature enables congestion management, congestion avoidance, and bandwidth control by selectively activating QoS mechanisms on intelligently grouped LAN and WAN interfaces and providing support for external application programming interfaces (APIs) to trigger event-based policy distribution.
- *Access control*—Users can extend security by defining access control policies to permit or deny transport of packets into or out of device interfaces.
- *Advanced QoS policy administration*—This feature exposes QoS policy conflicts, uploads existing device configurations, presents command-line interface (CLI) syntax that corresponds to policies, allows previewing configuration changes before deployment, supports incremental access-control-list (ACL) updates, defines ACL ranges, and restores or applies a previous version of a policy database and backup to a remote server.
- *Comprehensive device and Cisco IOS Software support*—Only CiscoWorks QPM 3.2 can be used with hundreds of different Cisco routers and switches as well as a broad range of Cisco IOS Software and Cisco CatOS software versions.
- *CiscoWorks integration*—Device inventory import from CiscoWorks Resource Manager Essentials (RME) shortens configuration time for devices targeted for policy enforcement and QoS monitoring.
- *Web-based reporting*—This feature enables a user to quickly view and analyze QoS policy management.

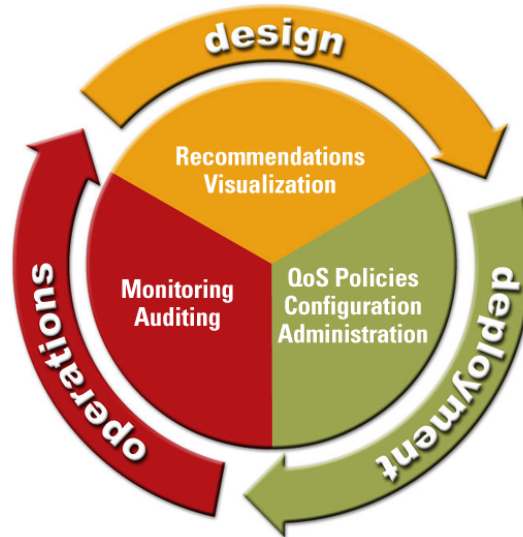
CiscoWorks QPM 3.2 Benefits

- CiscoWorks QPM is a scalable QoS policy system that makes it easy to:
- Baseline monitor critical traffic flows to define policies
- Classify applications into service classes
- Provision QoS with network-wide enforcement
- Validate QoS settings and results

With CiscoWorks QPM 3.2, users can gain visibility into network operations with traffic monitoring, configure policies critical to application performance, and automate multiple service levels across any network topology (refer to Figure 1). It provides centralized QoS analysis and policy control for voice, video, and data networks, and enables network-wide, content-based DiffServ and campus-to-WAN automated QoS configuration and deployment.



Figure 1
Complete QoS Management Life-Cycle Coverage with CiscoWorks QPM



Centralized, Multidevice Management

CiscoWorks QPM 3.2 uses the common CiscoWorks foundation and implements a structured workflow, making it easier to scale management to many devices and improve productivity when it comes to policy configuration, deployment, and analysis (refer to Figure 2). It provides network administrators with a secure HTML-based GUI, authentication, roles definitions and permissions, database engine, extensive support for Cisco IOS routers and Cisco Catalyst switches, access to Cisco and user-defined policy templates, and more.

Figure 2
Secure, Web-Based QoS Policy Manager Integrated Into the CiscoWorks Desktop





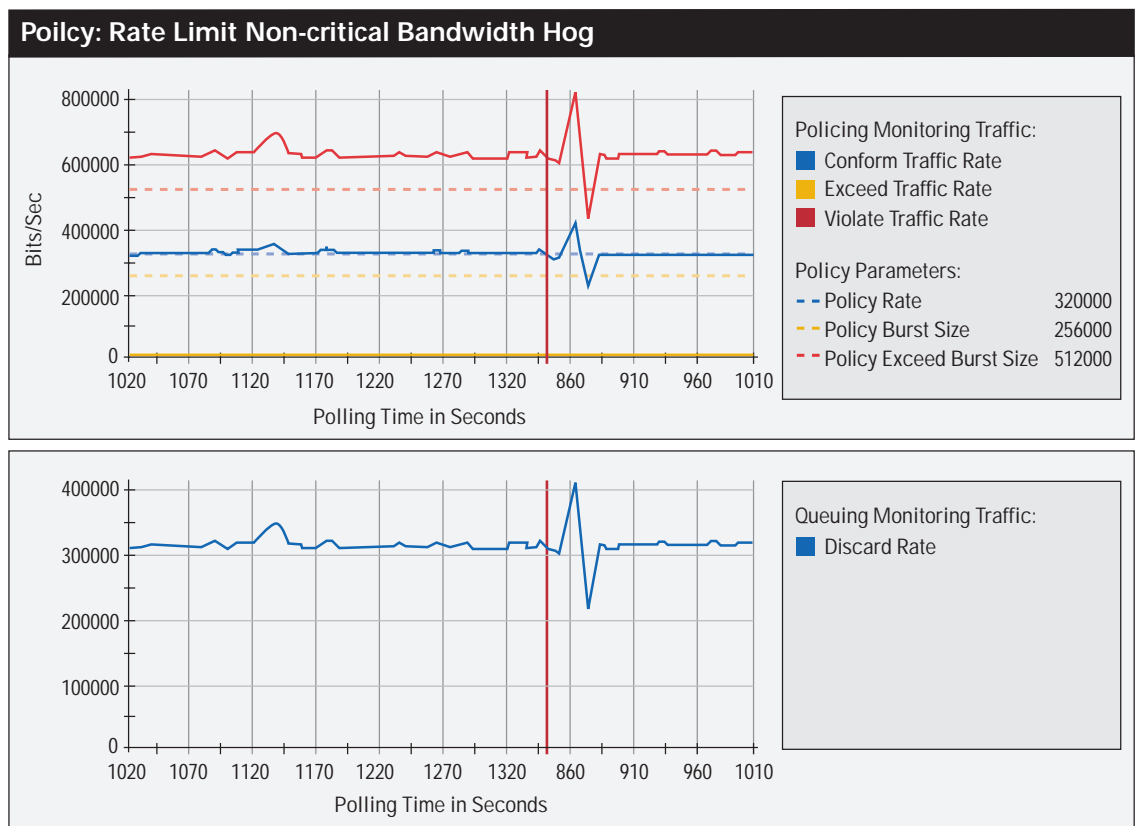
Traffic Monitoring

Traffic monitoring is fundamental to QoS provisioning in the IP infrastructure, ensuring critical application performance and achieving the best possible bandwidth usage. With CiscoWorks QPM 3.2 it is possible to obtain QoS feedback from central and remote routers, including WAN interfaces along a multihop path. CiscoWorks QPM 3.2 takes advantage of the Cisco intelligent infrastructure by displaying statistics collected from the Cisco IOS router class-based QoS MIB or committed-access-rate (CAR) MIB. Network administrators can use QPM monitoring to establish a reference point for current and historical network conditions, gaining insight into traffic throughput for top applications (for example, SAP, PeopleSoft, and SNA) or traffic distribution by service class (for example, real time, business critical, and best effort). This baseline traffic information is then used as input into QoS policy creation or modification.

After QoS deployment, CiscoWorks QPM 3.2 monitoring helps determine if policies are having the desired impact by providing packet or bit rate measurements at WAN interfaces for inbound and outbound traffic. And network administrators can view QoS graphs, including line and bar charts, next to policy descriptions.

Administrators troubleshoot performance problems by examining traffic patterns relative to QoS enforcement mechanisms, including policing, queuing, shaping, and dropping (refer to Figure 3). A date and time "zoom" function is available to scan QoS data over different time periods, and a file export function allows for additional analysis by other tools.

Figure 3
QoS Policy Manager Traffic Monitoring



Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

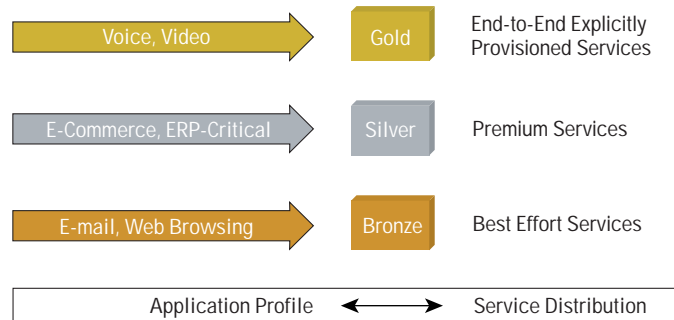


Deliver Network-Wide DiffServ

Provisioning network resources based on the relative importance of application traffic is the most effective way to deliver differentiated QoS. Packet classification is key in allowing selection of the appropriate packets for a specific level of service. By automating the process of translating application performance requirements into QoS policy, CiscoWorks QPM 3.2 helps ensure reliable performance for Internet business applications and voice traffic that contend with noncritical traffic. A network administrator can quickly construct rules-based QoS policies that identify and partition application traffic into multiple levels of service, ensuring that the most important applications receive priority service (refer to Figure 4).

For example, a business might establish differentiated gold, silver, and bronze levels of IP services. A gold service would guarantee latency and delivery for the transport of SNA or real-time traffic such as VoIP. A silver service would guarantee delivery for business-critical applications that require certain response times but are not as latency-sensitive, such as enterprise resource planning (ERP) or e-commerce. And a bronze service could be used to support certain Web and e-mail sessions, while other traffic is treated on a best-effort basis.

Figure 4
Establish DiffServ with CiscoWorks QPM



Edge and Backbone QoS Policy Control and Enforcement

CiscoWorks QPM 3.2 allows a user to build a network-wide QoS policy architecture that prioritizes applications by level of service at the perimeter of the network and then provides policy enforcement in the backbone (or core) using congestion-management, congestion-avoidance, and traffic-shaping techniques. This architecture improves network operation by performing traffic classification, marking or coloring packets, and scheduling on the campus edge while eliminating the need to classify traffic at each WAN interface in the backbone. In addition, Cisco IOS QoS services provide the means for distributing network functionality and responsibility between edge functions and backbone functions. This distribution of functions enables simultaneous performance and services scalability.

At the edge of the network, CiscoWorks QPM 3.2 is used to:

- Specify policies that establish traffic classes and related service levels
- Specify policies that define how network resources are allocated and controlled per traffic class and service level
- Enable efficient mapping of applications into service levels
- Apply policies to meet business requirements



After packets have been marked or colored according to the defined service level, the QoS policy is enforced in the network core or WAN backbone. For the network backbone, CiscoWorks QPM 3.2 enables policy enforcement through an extensive set of QoS mechanisms that are used for congestion management, such as Class-Based Weighted Fair Queuing (CBWFQ); congestion control, including Weighted Random Early Detection (WRED); and traffic shaping.

To effectively provide end-to-end QoS, network signaling requires that network devices share the responsibility of delivering priority traffic. Today, Cisco IOS Software supports a rich set of QoS features with campus and backbone switches and routers, each performing separate but cooperative QoS functions. Using CiscoWorks QPM 3.2, administrators can define QoS policy groups within a network to control distinct QoS classification and enforcement roles. Taking advantage of newly integrated QoS functions delivered in the Cisco Catalyst 3550, Catalyst 4500, and Catalyst 6000 switches, CiscoWorks QPM 3.2 extends policy control and enforcement across the enterprise, from headquarters campus to small or large remote offices.

QoS for IP Telephony

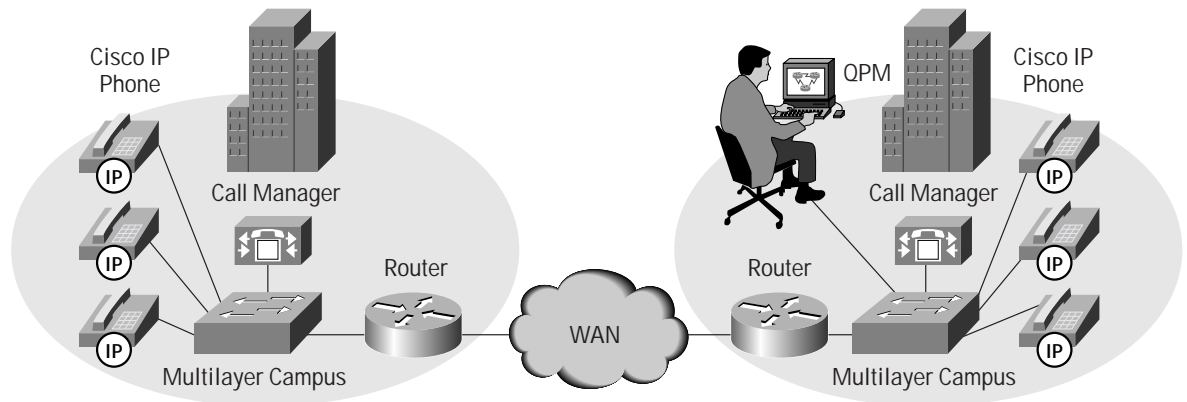
One of the most promising uses for IP networks is to allow sharing of voice traffic with the traditional data and LAN-to-LAN traffic. Typically, sharing can help reduce transmission costs by reducing the number of network connections as well as sharing existing connections and infrastructure. By deploying VoIP networks, businesses today can reduce some of their voice costs by combining voice traffic onto their existing IP networks. To provide the required voice quality, however, QoS must be part of the network. CiscoWorks QPM 3.2, along with Cisco IOS and Cisco CatOS QoS mechanisms in a Cisco AVVID network, gives VoIP traffic the priority service it needs, while providing the required service levels for data traffic (refer to Figure 5).

CiscoWorks QPM 3.2 enables optimal voice quality in enterprise IP networks. The QPM 3.2 management tool contains a step-by-step wizard that guides administrators through the process of configuring QoS for voice in the network, QoS monitoring for voice traffic, and reports, including network voice readiness (devices that have all the required software and hardware to support QoS for voice) and deployment audit. The IP telephony wizard can identify potential network points (device interfaces) where QoS needs to be configured, and select and assign the appropriate QoS policies for each interface on the voice path. QoS policies and properties for voice, included with CiscoWorks QPM 3.2 in a template library, are defined according to the Cisco IP Telephony design recommendations. A user can easily modify these predefined templates or reassign default policy assignments as needed to fit an organization's IP network.

With CiscoWorks QPM 3.2, a user can monitor for troubleshooting (for example, to determine whether voice packets are being dropped at headquarters and remote WAN interfaces) and provide network-wide QoS to expedite the transmission of voice packets while reducing jitter.



Figure 5
CiscoWorks QoS Policy Manager Delivers Centralized, Comprehensive QoS Management for Voice



Identify Traffic Flows	Establish/mark Service Classes	Enforce
<ul style="list-style-type: none"> • Subnet/IP Address • UDP Port Range • IP ToS Marking • Trust Settings • RSVP Policy Control • VLAN • RTP Payload Type 	<p>Voice → Gold</p>	<ul style="list-style-type: none"> • CBWFQ • LLQ • IP RTP Priority • RSVP Priority and WAN Devices • Cat 6K 1P2Q2T • CRTP • Link Fragmentation and Interleaving (LFI) • Enhanced FRTS with FRF.12 and FR Fair Queue and FR Voice Bandwidth

Secure, Automated QoS Management

Even with intelligent network devices, the task of manually configuring and deploying QoS policies on a network-wide basis can be error-prone. CiscoWorks QPM 3.2 automates many of the steps associated with policy definition, validation, configuration, and deployment. During policy definition, CiscoWorks QPM 3.2 queries devices to determine the device class, interface type, software version, and supported QoS features required to build a rules database. Using this rules database, QPM 3.2 guides the user through valid policy definitions, without requiring an understanding of QoS mechanism command-line language or device syntax. CiscoWorks QPM 3.2 eliminates tedious device-by-device configuration tasks, improving policy consistency and reducing the amount of time it takes to implement QoS policies. QPM allows a user to:

- Use secure HTML communications between client and application server plus Secure Shell (SSH) Protocol for policy distribution to Cisco routers
- Query device roles specifying the network point for a device in the Cisco AVVID network (for example, campus access, campus distribution, or WAN aggregation)
- Generate policy and CLI conflict reports
- View CLI translation for policies and preview device-level changes (CLI additions and deletions) before deployment
- Create powerful policies that combine static and dynamic port applications and host-system traffic filters
- Activate a rich set of QoS services through queuing, shaping, policing, and congestion-avoidance mechanisms
- Organize large network device inventory into logical folders for better manageability



- Upload existing device QoS configurations and validate policies prior to deploying them to the network
- Roll back to a previous QoS implementation by redeploying a historical version of the deployment group
- Generate Web-based reports on QoS policies deployed in the network

Support for Large-Scale QoS Deployments

CiscoWorks QPM 3.2 allows partitioning of the network into QoS administrative and deployment domains. With possibly hundreds or thousands of devices in a network to be managed, QPM 3.2 allows for one or more deployment groups with integrated policy groups and device groups. CiscoWorks QPM 3.2 provides a QoS capabilities report for any policy group, allowing users to see exactly what QoS functions are common or different across like and unlike network devices and OS versions. To ensure QoS consistency and streamline configuration in large networks, users can build libraries containing policy templates. These templates can be copied and then modified or attached globally, enabling many policies to "inherit" a common set of QoS attributes. Network administrators are also now able to implement best practices for phased deployments, considering the number of devices requiring QoS configuration per concurrent deployment versus time to deploy guidelines. CiscoWorks QPM 3.2 supports role-based permissions to view, modify, and deploy QoS policies and monitoring tasks, enabling organizations to scale access privileges. It conveniently uses the CiscoWorks Desktop user authentication at logon and then automatically applies user permissions as defined through the common management framework. In CiscoWorks QPM 3.2 network managers can restrict QoS policy management rights for users or user groups for different devices based on Cisco Secure ACS roles, permissions, and administrative device groups.

With CiscoWorks QPM 3.2, QoS policies are distributed to network devices after being converted into specific classification, queuing, policing, and shaping configuration commands, reducing the complexity of configuring a mix of QoS features across different devices and Cisco IOS and Cisco CatOS versions. In addition, QPM 3.2 ensures the success of each policy distribution by monitoring the status of a multidevice distribution, logging all interface configuration changes, and maintaining a policy audit trail.

CiscoWorks QPM 3.2 Feature Details

CiscoWorks QPM 3.2 comprises multiple tools in a single application: analysis, policy configuration, deployment control, device management, reporting, and general administration. The following sections describe the various features related to these tools.

QoS Monitoring

QoS monitoring in CiscoWorks QPM 3.2 is a combination of defining and executing tasks, collecting data from the Cisco IOS class-based QoS MIB or CAR MIB on Cisco routers, and viewing charts and graphs with traffic and QoS statistics.

CiscoWorks QPM 3.2 allows the user to build real-time and historical monitoring tasks specific to devices, interfaces, and QoS policies. The polling interval ranges from 10 seconds to 60 minutes. The maximum length of time a monitoring task can run is 6 months. It is possible to run multiple tasks comprising hundreds of elements and for different purposes, such as profiling current traffic throughput for top applications, and determining distribution of traffic for different service classes. Data collected is stored in a database, and a file can be exported for additional analysis.



Traffic and QoS statistics are displayed as line or bar charts in bits or packets per second, per interface or policy. CiscoWorks QPM 3.2 allows a user to view reports showing traffic throughput before and after QoS, as well as impact on traffic due to QoS policy actions.

With CiscoWorks QPM 3.2, users can view:

- Statistics matching policies and specific filters, including network-based application recognition (NBAR) application filters
- Traffic rate before any QoS policy actions, traffic transmitted after QoS policy actions, and dropped—not transmitted—traffic that is dropped because of QoS policy drop actions
- QoS action statistics: WRED, policing, traffic shaping, and queuing

Secure HTML-Based Policy Administration

CiscoWorks QPM 3.2 integrates with the CiscoWorks Web-based desktop, making it easy to share information and move among other CiscoWorks applications. The policy system maintains a knowledge base that stores attribute information about the QoS capabilities of each device. This knowledge base automatically validates policies to ensure that users define QoS policies only for QoS mechanisms supported by target devices and then translates these QoS policies into configuration commands specific to each interface, which users can view in QPM 3.2 with the click of a mouse. CiscoWorks QPM 3.2 policy abstraction and automation reduces repetitive tasks associated with defining policies for multiple devices and software releases, ensuring QoS policy integrity.

Rules-Based Policy Filters

CiscoWorks QPM 3.2 allows a user to build flexible, rules-based QoS policies that filter traffic based on source or destination IP address or port, protocol, IP type of service (ToS), Domain Name System (DNS) host name, as well as user-defined macro filters. Filter expressions improve the accuracy and consistency of configuration commands deployed to the network.

Application-Level Packet Classification

An integral part of Cisco content networking, CiscoWorks QPM 3.2 enables configuration of NBAR and distributed NBAR features available in Cisco IOS Software that extend packet classification to content-based application signature, Web URLs, and recognition of dynamic protocols.

In addition, CiscoWorks QPM 3.2 now takes advantage of NBAR for packet coloring or marking and rate limiting. Through simple dialog boxes and scrolling, users can apply powerful rules-based policies, combining application and host-system filters, including mapping NBAR protocol numbers, to achieve granular service differentiation. The packet inspection engine of NBAR provides classification of applications that rely on dynamic TCP/User Datagram Protocol (UDP) port assignments and classification of HTTP traffic by URL and Multipurpose Internet Mail Extensions (MIME) types. Additional packet content-based application signatures also can be recognized, including Real-Time Transport Protocol (RTP) payload type and Gnutella (a peer-to-peer file-sharing application).



Application Service Profiles

Users can define application-service profiles based on application port, protocol, and TCP/UDP socket address. CiscoWorks QPM 3.2 has well-known TCP and UDP applications predefined in the system, and it allows the user to create a library of customized application profiles.

Host Groups

Host groups based on IP address, IP address range, DNS name, or IP address and mask combination can be created. When defining QoS policies, the user can use these host groups instead of specifying individual end user, server, or network address. As new hosts are added or removed, users simply update and reapply the host group to the network instead of reconfiguring the ACLs of multiple devices.

Policy Libraries

Policy libraries in CiscoWorks QPM 3.2 contain either Cisco or user-defined policy templates that can be used to create and share policy groups across deployment groups and device groups. Templates contain predefined QoS properties with specific device constraints that can be customized. It is also possible to attach a policy template to policy groups, enabling “one-stop” global policy configuration.

Administrative and Deployment Domains

With CiscoWorks QPM 3.2 it is possible to have one or more deployment groups with integrated policy groups and device groups. The intelligent grouping feature of QPM 3.2 for structured QoS management ensures policy accuracy and consistency across multiple interfaces and device types. For example, deployment groups can be according to regions or by policy groups by roles (such as access, distribution, and core), with policies assigned to a specific set of devices and interface types. CiscoWorks QPM 3.2 includes a QoS capabilities report during policy configuration, so it is possible to see exactly which QoS mechanisms are available across different devices and OS versions in the same group. Network administrators can divide the network into groups for purposes of controlling who can do what with which devices: view only, modify, or deploy. A user can create role-based user permissions or allow QPM to inherit privileges for different device groups created in Cisco Secure ACS 3.2 or later.

Access Control

CiscoWorks QPM 3.2 extends network security by allowing QoS policies to permit or deny transport of packets through interfaces. Access control policies can be enabled or disabled globally or specified on a per-device basis. Further, QPM provides QoS policy filtering to exclude specific traffic from defined service levels.

Consistent DiffServ

Up to 64 classes of DiffServ can be defined, into which all traffic can be classified based on network session to application-layer filters. These classes can be identified network-wide with IP Precedence or differentiated-services-code-point (DSCP) value without changes to existing applications, devices, or complicated network signaling requirements.



QoS Enforcement

CiscoWorks QPM 3.2 supports enforcing DiffServ by utilizing extended ACLs to define network policies for congestion handling and bandwidth allocation. QPM 3.2 supports congestion management using CBWFQ, Weighted Round Robin (WRR), priority queuing, custom queuing, and Weighted Fair Queuing (WFQ); congestion avoidance using WRED, including DSCP-based WRED; ingress and egress bandwidth limitations using CAR; and traffic shaping using generic traffic shaping (GTS) and Frame Relay traffic shaping (FRTS).

Campus and Remote-Office QoS

CiscoWorks QPM 3.2 extends policy control across campus and WAN environments by supporting the latest Cisco Catalyst switches.

Integrated campus QoS features include:

- IP packet classification, which enables network-wide differentiated service of traffic on an ingress port basis
- Classification by VLAN
- Bandwidth policy, which enables traffic rate limiting on a per-port basis
- Drop threshold management, which gives preference to higher-priority traffic
- Traffic scheduling, which allocates traffic to outbound transmit queues according to IP Precedence or DSCP value

Voice QoS

CiscoWorks QPM 3.2 comes with an IP telephony wizard that walks the user through configuration of QoS for voice. The wizard automatically maps device inventory to policy templates that contain predefined QoS mechanisms for voice traffic. These templates are based on the Cisco IP Telephony QoS design recommendations for switches and routers, yet can be modified as needed or easily updated through Cisco.com. The wizard presents the policy group associated with different types of devices, interfaces (for example, WAN-FR-DLCI-Slow versus WAN-FR-DLCI-High), and roles (for example, Access6K versus Dist6K). QoS mechanisms supported for voice include:

- CBWFQ with
 - Low-latency queuing (LLQ) for strict priority
 - IP RTP priority and payload type
 - GTS
 - FRTS on subinterface or data-link connection identifier (DLCI)
 - Distributed traffic shaping (DTS)
 - Distributed Frame Relay fragmentation (DFRF)
 - Rate limiting
- Compressed RTP (cRTP) header
- Link fragmentation and interleaving (LFI) for point-to-point connections
- Enhanced FRTS with Frame Relay Fragmentation (FRF12) and Frame Relay fair queue and Frame Relay voice bandwidth
- Cisco Catalyst trust properties, including boundary extension and marking
- Cisco Catalyst 6000 advanced traffic-scheduling capabilities, including 1P2Q2T



Policy Deployment

CiscoWorks QPM 3.2 has numerous advanced features to ensure that building QoS policies is accurate. This solution enables a user to:

- Set ACL numbers
- Revalidate DNS resolutions
- Upload existing device QoS configurations
- Detect device-based policy changes
- Detect Cisco IOS and Cisco Catalyst OS software versions

The distribution manager component of CiscoWorks QPM 3.2 controls and audits the distribution of QoS policies to network devices. The distribution control features of the system allow a user to:

- Preview all configuration changes, including the device and software version-specific CLI or modular CLI syntax
- Deploy policies to device groups running the same software image or different software images
- Stop a policy distribution if a failure occurs
- Track job progress and job history information
- Output a configuration file and Trivial File Transfer Protocol (TFTP) download to devices

Event-Driven Policy Distribution

CiscoWorks QPM 3.2 allows external applications to trigger the deployment of a deployment group, by issuing an HTTP request. This feature allows a user to securely activate event or time-based triggering of deployment, as required.

Reporting and Advanced Administration

CiscoWorks QPM 3.2 includes reports that provide a summary of all QoS policies deployed in the network, audit trails to see who did what and when concerning policies and deployments, backup schedules and backup history, as well as reports pertaining to policy conflicts after an administrative action, such as upload device configuration.

Comprehensive Device and Cisco IOS Software Support

CiscoWorks QPM 3.2 device support includes:

- Routers—Cisco 1600, 1700, 2500, 2600, 2600XM, 3200, 3600, 3700, 4000, 4500, 4700, 7100, 7200, 7300, 7401, and 7600 IR, Cisco 7500 Series with Versatile Interface Processor (VIP), Cisco ICS 7750, and Cisco AS5300 and AS5800
- Switches—Cisco Catalyst 2900, Catalyst 2950, Catalyst 3500, Catalyst 3550, Catalyst 3750, Catalyst 4000, Catalyst 4500, Catalyst 5000, Catalyst 6000, and Catalyst 8500 series; combination of policy feature card (PFC), Multilayer Switch Feature Card (MSFC), and FlexWAN module for the Cisco Catalyst 6000; Cisco Catalyst 2948G-L3 and Catalyst 4908G-L3; and the route switch module (RSM) for the Cisco Catalyst 5000
- Cisco IOS Software releases—11.1cc, 12.0, 12.1, 12.2, 12.2T, 12.3 and later, 12.2S, and 12.1E and later
- Cisco CatOS releases—5.5, 6.0, 7.0, and 8.0 and later

Additional information about CiscoWorks QPM 3.2 supported devices, device software, and related QoS functions is available at: http://cisco.com/en/US/products/sw/cscowork/ps2064/products_device_support_tables_list.html.



CiscoWorks Device Import

Device inventory information can be imported from CiscoWorks RME. CiscoWorks QPM 3.2 can import both the data-integration file and comma-separated-value file format generated by the export feature of CiscoWorks RME.

Server and Client Specifications (minimum requirements)

Server Hardware

- PC-compatible computer with 1-GHz or faster Pentium processor
- CD-ROM drive
- 10BASE-T or faster connection
- 1-GB RAM
- 9-GB available disk drive space
- 2-GB virtual memory
- Server Operating System

CiscoWorks QPM requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 or 4)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Ports Used by QPM

CiscoWorks QPM on Windows uses the following ports, in addition to the ports used by CiscoWorks Common Services:

- 51099 Java Naming and Directory Interface (JNDI) lookup port
- 51199 JRMP lookup port
- 51299 Admin page port
- 10033 (Windows) Database port
- 51899 Protocol Data Packet (PDP) port

Client Requirements

Hardware

- PC-compatible computer with 300-MHz or faster Pentium processor

Client Operating System

- Windows 2000 (Server or Professional Edition) with Service Pack 3 or 4, or Windows XP SP1 (Server or Professional)

Client Browser

Windows with SP 3 and Windows XP clients:

- Microsoft Internet Explorer 6.0 or Internet Explorer 6.0 with Service Pack 1
- Netscape Navigator 7.1



Windows clients with SP 4:

- Microsoft Internet Explorer 6.0 with Service Pack 1
- Netscape Navigator 7.1

Cisco recommends using CiscoWorks QPM 3.2 on its own server for optimal performance. CiscoWorks QPM 3.2 can be used with other CiscoWorks solutions, as follows:

- CiscoWorks VPN Security Management Solution (VMS) 2.2
- CiscoWorks LAN Management Solution (LMS) 2.2
- CiscoWorks Routed WAN Management Solution (RWAN) 1.3

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Support (SAS) program. This service program offers customers contract-based 24 x 7 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and minor software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks QoS Policy Manager is available for purchase through normal Cisco sales and distribution channels worldwide. CiscoWorks QPM includes all the necessary components needed for an independent installation on a Microsoft Windows workstation.

For More Information

For more information about CiscoWorks QoS Policy Manager 3.2, visit: <http://www.cisco.com/go/qpm>.

If you have further questions, e-mail the CiscoWorks team at: CiscoWorks@cisco.com.

GuestSearch:

CISCO SYSTEMS



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and Cisco IOS are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.
(0304R) ETMG 203185—LB 12.04