Q&A

CISCOWORKS QOS POLICY MANAGER 3.2

GENERAL

Q. What is CiscoWorks QoS Policy Manager (QPM)?

A. CiscoWorks QPM is an important enabler of end-to-end quality of service (QoS) for IP networks. CiscoWorks QPM 3.2 is a secure, Web-based, QoS management tool that combines centralized traffic monitoring with networkwide configuration of Differentiated Services (DiffServ) for data, voice, and video applications, simply by taking advantage of the Cisco® intelligent infrastructure.

Q. What are the benefits of CiscoWorks QPM?

A. CiscoWorks QPM can improve converged network operations by providing a centralized, intelligent, and cost-effective way to manage traffic according to enterprise requirements. Network administrators can take full advantage of built-in Cisco IOS® Software and Cisco Catalyst® Operating System (Catalyst OS) QoS mechanisms, gain visibility into traffic throughput at different points in the network, and enable networkwide performance protection for voice, video, and critical data. Improved productivity is gained through QoS management that spans from baseline profiling of traffic by top applications and distribution of traffic by service classes to networkwide QoS provisioning and monitoring for QoS policy validation.

NEW FEATURES

Q. What features are new to CiscoWorks QPM 3.2?

A. Table 1 describes the new features included in CiscoWorks QPM 3.2.

Table 1. CiscoWorks QPM 3.2 Features

Features
Enhanced QoS management reliability and performance
Includes CiscoWorks Common Services Software 2.2
Explicit support for the following device operating systems: • Cisco IOS Software Release 12.3 • Cisco Catalyst OS 7.2 and Catalyst OS 8.1
Support for QoS on tunnel interfaces
New device support: • Cisco Catalyst 2948 Switch • Cisco Catalyst 3750 Series switches with support for class of service (CoS)/differentiated services code point (DSCP) mappings, marking, and policing • Cisco Catalyst 6500 Series Policy Feature Card 3 (PFC3) and Multilayer Switch Feature Card 3 (MSFC3)
Japanese-OS on Windows
Netscape Navigator browser 7.1

For more information about device and software support, please visit

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

Use CiscoWorks QPM on its own server (recommended for optimal performance), or in conjunction 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

Q. Is CiscoWorks QPM 3.2 compatible with CiscoWorks QPM 3.1, 3.0, or 2.1?

A. Yes. Please note that there is a policy-conversion utility for CiscoWorks QPM 2.1 to QPM 3.2. If you are a QPM 2.1 user, it is recommended to first become familiar with the CiscoWorks QPM 3.2 user interface, workflow, and product features before converting QPM 2.1 policies. This will allow you to plan in advance how you want CiscoWorks QPM 2.1 policies to be structured within the CiscoWorks QPM 3.2 management tool.

MONITORING

Q. Is it possible to use QoS monitoring without CiscoWorks QPM 3.2 policy deployment?

A. No. QoS policies must be deployed to the network using CiscoWorks QPM 3.2 to enable QoS monitoring and reporting in the management tool.

Q. Can I use CiscoWorks QPM 3.2 monitoring with Cisco routers and switches?

A. It is possible to use CiscoWorks QPM 3.2 monitoring with central and remote Cisco routers only (Cisco 2500, 2600, 3600, 3700, 4000, 7000, and 7500 series). Enterprises will use CiscoWorks QPM 3.2 monitoring to collect QoS statistics from items listed in Table 2:

Table 2. CiscoWorks QPM 3.2 Monitoring of QoS Statistics

MIB Type	Cisco IOS Software Release
Class-Based QoS (CBQoS) MIB used for modular QoS-defined policies	Cisco IOS Software releases 12.2, 12.2T, and 12.3
Committed access rate (CAR) MIB used for non-modular, QoS-defined policies	Cisco IOS Software releases 11.1cc, 12.0, 12.1, 12.2, 12.2T, and 12.3

Q. What kind of QoS feedback is possible with CiscoWorks QPM 3.2?

A. CiscoWorks QPM 3.2 monitoring is used to baseline profile traffic for top applications (for example, SAP, Oracle, PeopleSoft, custom applications) and DiffServ classes (for example, real-time, business-critical, best-effort) and to validate QoS settings and results (for example: Is the “silver” service class for business-critical applications getting 40 percent of the link? Are rate-limiting bandwidth applications such as Gnutella working?). Historical analysis monitors traffic, with a start and end time, for all policies on one or more interfaces, polling on a regular basis and storing the gathered data. Real-time analysis monitors traffic for all policies on one interface continuously, in real time (no data is stored). Information is presented in bits or packets per second and graphed as a line or bar chart. Analysis includes displaying traffic statistics (including network-based application recognition [NBAR] filters) before and after QoS policy deployment and charting QoS action statistics. The following statistics can be graphed:

- Policies
  - Traffic matched per class prior to QoS actions
  - Traffic matched per class after QoS actions
  - Traffic matched per class discarded by QoS
- Filters—distribution of matching traffic by policy filter statements

- QoS actions—Queuing, Weighted Random Early Detection (WRED), traffic shaping, and policing

Q. Can I do further analysis with a third-party application such as Microsoft Excel or Concord Communications eHealth?

A. Yes. CiscoWorks QPM 3.2 has an export option that generates an Extensible Markup Language (XML) formatted file that contains monitoring statistics that can be imported into third-party applications for further analysis.

Q. How does CiscoWorks QPM 3.2 monitoring fit with the Cisco Network Analysis Module (NAM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series in a CiscoWorks traffic-management solution?

A. You can use the Cisco NAM with CiscoWorks QPM 3.2 for complete LAN and WAN traffic management. The Cisco NAM can characterize traffic patterns on the LAN by automatically detecting known and unknown applications, categorized by hosts and conversations. Cisco NAM has onboard instrumentation, including NetFlow support, for traffic management. When used with CiscoWorks QPM 3.2, the Cisco NAM gives network administrators a complete Cisco solution for traffic analysis and LAN and WAN troubleshooting.

Q. What parameters impact CiscoWorks QPM 3.2 traffic-monitoring performance?

A. Several parameters impact CiscoWorks QPM 3.2 monitoring performance: polling interval time; network response time; polled data (number and type of policies); number of interfaces; server configuration; and disk space. For more information, refer to the CiscoWorks QPM QoS Analysis tutorial at:

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

Q. What is the maximum length of time a QoS monitoring task can run?

A. The maximum length of time a monitoring task can run is six months.

Q. How many router interfaces can be viewed in a single graph?

A. It is possible to display up to 12 interfaces in a graph for a single policy (for example, voice traffic gets low-latency queuing [LLQ] and 33 percent of link) or display several graphs, each with a different interface but for a common set of policies (for example, gold—voice, silver—SAP/Oracle, bronze—best effort). Both views provide a network administrator with QoS feedback for a multihop path, including bandwidth use and dropped packets per interface and per service class.

DEPLOYMENT AND ADMINISTRATION

Q. Does CiscoWorks QPM 3.2 support large-scale QoS deployments?

A. CiscoWorks QPM 3.2 includes features and functions to enable QoS management for large networks. Table 3 describes these features included in CiscoWorks QPM 3.2.

Table 3. CiscoWorks QPM 3.2 QoS Management Features

Features
Relational database (part of CiscoWorks Common Services) for storage of policies and QoS statistics
Structured management that includes deployment groups with integrated policy groups and device groups
Deployment control, allowing guidelines to dictate the number of devices in a concurrent deployment and schedule
Support for Secure Sockets Layer (SSL) policy distribution to devices
As part of defining a policy group, generation of a capabilities report indicating common QoS functions for various devices running different Cisco IOS versions
Policy libraries that include Cisco or user-defined templates that can be copied, modified, or attached to multiple policy groups for “one-to-many” configuration
Scheduled backups to an offsite server

Q. How many authorization roles are supported in CiscoWorks QPM 3.2?

A. CiscoWorks QPM 3.2 has various permissions (view, modify, deploy) for different roles. What a user can do in CiscoWorks QPM 3.2 depends on the assigned role. CiscoWorks Desktop offers five possible roles, each with a set of permissions assigned to a single default device group. For example, the system administrator role has global permission to view and modify policies but not deploy them. When using Cisco Secure Access Control Server (ACS), CiscoWorks QPM 3.2 inherits the defined administrative device groups and role-based permissions. Cisco Secure ACS allows for three different roles associated with different device groups. For example, a user may have system administrator permission for western U.S. routers only.

Q. Is it possible to deploy policies based on an external trigger?

A. CiscoWorks QPM allows external applications to trigger the distribution of policies to the network for a deployment group (you can have more than one deployment group), by issuing an HTTP request. This feature allows you to implement event- or time-based triggering of policy deployment, as required. Certain parameters must be included in the HTTP request. They include: username, user password, device group name, and deployment group name.

NETWORK CONVERGENCE

Q. How does CiscoWorks QPM 3.2 help in building and managing converged networks?

A. CiscoWorks QPM 3.2 takes advantage of the Cisco intelligent network to control delay and packet loss. You can provision end-to-end service classes for critical data (for example, SAP, Oracle, PeopleSoft, custom applications) and real-time traffic generated by voice gateways, IP phones, and IP videoconferencing systems. You can use CiscoWorks QPM 3.2 QoS analysis to determine if service-class policies deployed to the network are delivering the desired results.

Q. What does CiscoWorks QPM 3.2 offer for IP telephony?

A. IP telephony usually requires a rather complex QoS configuration for the devices that carry voice traffic flows. IP telephony QoS management is one of the primary features of CiscoWorks QPM 3.2. CiscoWorks QPM 3.2 includes a rules-based, step-by-step wizard with a built-in library of predefined QoS policy templates based on Cisco design recommendations. These predefined policies allow for accurate, fast configuration of voice QoS mechanisms on switches and routers, yet can be modified as needed to meet specific network requirements. Provisioning QoS for IP telephony in an enterprise network becomes a simple task, where the wizard intelligently maps policy templates to network devices (the user can reassign the default mappings as needed). CiscoWorks QPM 3.2 also includes a network voice-readiness report (devices that have all the required software and hardware to support QoS for voice) and deployment audit. QoS monitoring can be used for troubleshooting and adjusting policies as needed.

VIRTUAL PRIVATE NETWORK

Q. How does CiscoWorks QPM 3.2 help in building and managing converged networks?

A. CiscoWorks QPM 3.2 is used to specify policies for network elements (refer to the CiscoWorks QPM 3.2 device support list). If a given network element also serves as an IP Security (IPSec) VPN endpoint, the network administrator should consider enabling QoS “preclassify” on the router interface so that granular QoS classification using CiscoWorks QPM 3.2 can be facilitated. The QoS policy should be specified for the interfaces associated with IPSec cryptographic maps. CiscoWorks QPM 3.2 also supports Multiprotocol Label Switching (MPLS) and MPLS VPNs by providing EXP bit matching and setting. When using Cisco IOS Software Release 12.2 (11)T or later, the CBQoS MIB works with QoS preclassify enabled, so CiscoWorks QPM 3.2 can be used for monitoring on those router interfaces.

INSTALLATION AND COMPATIBILITY

Q. What operating systems does CiscoWorks QPM 3.2 support?

A. CiscoWorks QPM 3.2 server software is available on Windows 2000 Professional, Server, or Advanced Server with Service Pack 3 or 4.

Q. Can CiscoWorks QPM 3.2 use device inventory data stored in CiscoWorks Resource Manager Essentials (RME)?

A. Yes. CiscoWorks QPM 3.2 can import device inventory from CiscoWorks RME 3.3, 3.4, and 3.5 installed on the same (CiscoWorks RME 3.5 only) or separate server.

Q. Should CiscoWorks QPM 3.2 be installed on its own dedicated server?

A. Yes. If you plan to use CiscoWorks QPM 3.2 with many or complex historical monitoring tasks, it is best to use a dedicated server to allow for maximum performance and disk space to store QoS statistics collected from the CBQoS MIB.

Q. Can CiscoWorks QPM 3.2 be installed on the same server with other CiscoWorks applications?

A. Yes. CiscoWorks QPM 3.2 can be used with the following CiscoWorks solutions on the same server:

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

ORDERING AND FULFILLMENT INFORMATION

Q. How do I order CiscoWorks QPM 3.2?

A. The CiscoWorks QPM 3.2 software is available for purchase through regular Cisco sales and distribution channels worldwide.

To place an order, visit the Cisco Ordering Home Page.

Q. I have CiscoWorks QPM 2.x. Is CiscoWorks QPM 3.2 available for free?

A. No. CiscoWorks QPM 2.1 customers who want QPM 3.2 must purchase the QPM 3.2 upgrade using part number CWQPM-3.2-URUP-K9.

Q. I have CiscoWorks QPM 3.1. Is CiscoWorks QPM 3.2 available for free?

A. Yes, if you have a valid Software Application Support (SAS) service support agreement. Customers with CiscoWorks QPM 3.x SAS agreements may request entitlement update kits from the Cisco Product Upgrade Tool at www.cisco.com/upgrade.

Q. Where do I go to obtain part number and ordering information for CiscoWorks QPM 3.2?

A. Refer to the CiscoWorks QPM 3.2 product bulletin for more information:

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

FOR MORE INFORMATION

For more information about the CiscoWorks QoS Policy Manager, visit www.cisco.com/go/qpm or contact your local account representative at Cisco Systems® or send an e-mail to the Customer Support group at ciscoworks@cisco.com.

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

205314.H_ETMG_LF_5.05

Printed in the USA