Cisco Bandwidth Quality Manager User Guide

Software Release 3.0

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

Text Part Number: OL-11097-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, 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. (0609R)

PREFACE XI

ABOUT THIS GUIDE XI
OBJECTIVE XI
AUDIENCE XI
PREREQUISITE KNOWLEDGE XI
RELATED DOCUMENTATION XI
CONVENTIONS USED IN THIS GUIDE XII
OBTAINING DOCUMENTATION XII
CISCO.COM XII
PRODUCT DOCUMENTATION DVD XII
ORDERING DOCUMENTATION XIII
DOCUMENTATION FEEDBACK XIII
CISCO PRODUCT SECURITY OVERVIEW XIII
REPORTING SECURITY PROBLEMS IN CISCO PRODUCTS XIII
PRODUCT ALERTS AND FIELD NOTICES XIV
OBTAINING TECHNICAL ASSISTANCE XIV
CISCO TECHNICAL SUPPORT & DOCUMENTATION WEBSITE XV
SUBMITTING A SERVICE REQUEST XV
DEFINITIONS OF SERVICE REQUEST SEVERITY XVI
OBTAINING ADDITIONAL PUBLICATIONS AND INFORMATION XVI

1 BANDWIDTH QUALITY MANAGER OVERVIEW 1-1

MONITORING AND CONFIGURATION INTERFACE FEATURES 1-2
SWITCHING BETWEEN MODES 1-5
SELECTING A REPORTING PERIOD 1-5
GENERATING REPORTS 1-6

2 CONFIGURING BQM QOS MONITORING 2-1

OVERVIEW 2-1
ENABLING QOS MONITORING FEATURES WITH MONITOR QUEUING AND END TO END MAPS 2-2
Default Monitor-Queuing-Map 2-2
Enabling Microburst Event Detection 2-3

Enabling and Disabling Congestion Analysis and Bandwidth Sizing Features 2-3
End-to-End Measurements 2-5
CLASSIFYING TRAFFIC WITH CLASS MAPS 2-6
MODELING ROUTER QOS CONFIGURATION WITH POLICY MAPS 2-6
COMPLETING THE NETWORK MODEL WITH SITES, ROUTERS, AND INTERFACES 2-7
CUSTOM APPLICATIONS 2-9
CONFIGURING QOS MONITORING FEATURES 2-9
CONFIGURING A MONITOR-QUEUING-MAP 2-9
Configuring Expected Queuing Delay and Loss 2-11
Configuring Corvil Bandwidth (CB) Measurement 2-12
Configuring Microburst Detection 2-13
CONFIGURING A MONITOR END-TO-END MAP 2-14
CONFIGURING CLASS MAPS 2-16
CONFIGURING POLICY MAPS 2-21
CONFIGURING A SINGLE-CLASS POLICY MAP 2-22
CONFIGURING A MULTI-CLASS POLICY MAP 2-23
Configuring a Strict Priority Queuing Policy Map 2-23
Configuring a Weighted Fair Queuing (WFQ) Policy Map 2-26
Configuring a Low Latency Queuing (LLQ) Policy Map 2-29
CONFIGURING CUSTOM APPLICATIONS 2-32
CONFIGURING SITES, ROUTERS, AND INTERFACES 2-35
EDITING THE LOCAL SITE 2-36
Configuring a Local Site Router 2-37
Configuring a Local Site Router Interface 2-39
CONFIGURING A NEW REMOTE SITE 2-41
Configuring a Remote Site Router 2-43
Configuring a Remote Site Router Interface 2-45
Configuring Advanced Interface Settings 2-48
EDITING A REMOTE SITE 2-49
DELETING A REMOTE SITE 2-50

3 CONFIGURING NETWORK DEPLOYMENTS 3-1

OVERVIEW 3-1
BASIC ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 3-1
BASIC MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT 3-8
VPN DEPLOYMENT WITH REDUNDANT LOCAL SITE CONNECTIVITY 3-15
VPN DEPLOYMENT WITH REDUNDANT REMOTE SITE CONNECTIVITY 3-15
DUAL-HOMED ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 3-16
DUAL-HOMED MPLS DEPLOYMENT 3-22
HYBRID DEPLOYMENT 3-29

4 MONITORING NETWORK TRAFFIC 4-1

MONITORING DASHBOARD OVERVIEW 4-1
IDENTIFYING RECENT QUALITY ALARMS 4-2
IDENTIFYING THE TOP CONGESTED INTERFACES 4-3

IDENTIFYING WAN APPLICATION LEADERS 4-4
VIEWING SUMMARY INTERFACE AND CLASS RESULTS 4-5
Congestion Results 4-6
Top Applications Results 4-7
Microburst or Congestion Indicator, Corvil Bandwidth and Expected Delay and Loss Results 4-8
MONITORING CONGESTED INTERFACES 4-9
CONGESTION ANALYSIS OVERVIEW 4-9
SELECTING A REPORT PERIOD 4-13
Defining a Custom Report Period 4-14
SORTING THE CONGESTION ANALYSIS TABLE 4-14
FILTERING THE CONGESTION ANALYSIS TABLE 4-15
REPORTING CONGESTION ANALYSIS RESULTS 4-15
VIEWING INTERFACE AND CLASS CONGESTION 4-16
VIEWING ROUND TRIP DELAY AND LOSS 4-16
VIEWING INTERFACE MICROBURST AND CONGESTION INDICATOR MEASUREMENTS 4-18
VIEWING CLASS MEASUREMENTS 4-19
Expected Queuing Delay 4-20
Expected Queuing Loss 4-21
Microburst Detection 4-21
Congestion Indicator 4-23
Corvil Bandwidth – Delay 4-24
Corvil Bandwidth – Queue Length 4-25
VIEWING PRIORITY CLASS RESULTS 4-26
Corvil Bandwidth - Priority 4-26
Expected Priority Drops 4-27
MONITORING QUALITY ALARMS 4-28
SORTING THE QUALITY ALARMS TABLE 4-30
FILTERING THE QUALITY ALARMS TABLE 4-30
GENERATING A QUALITY ALARMS REPORT 4-30
MONITORING TRAFFIC INSIGHT RESULTS 4-32
TRAFFIC INSIGHT OVERVIEW 4-33
SELECTING A REPORT PERIOD 4-34
Defining a Custom Report Period 4-34
SORTING THE TRAFFIC INSIGHT TABLE 4-35
FILTERING THE TRAFFIC INSIGHT TABLE 4-35
REPORTING TRAFFIC STATISTIC RESULTS 4-36
VIEWING SUMMARY INTERFACE STATISTICS 4-36
VIEWING INTERFACE AND CLASS STATISTICS 4-37
CLASS STATISTICS OVERVIEW 4-37
IDENTIFYING MICROBURST MEASUREMENTS 4-39
IDENTIFYING INTERFACE AND CLASS TRAFFIC PATTERNS 4-41
Average Bit Rate Graph 4-41
Average Packet Rate Graph 4-42
Peak-to-Mean Ratio Graph 4-42
Packet Size Distribution Chart 4-43
IDENTIFYING TRAFFIC LEADERS 4-44
Viewing Top Applications 4-44
Viewing Top Talkers 4-45
Viewing Top Listeners 4-46
Viewing Top Conversations 4-47

5 ANALYZING NETWORK EVENTS 5-1

OVERVIEW 5-1
INVESTIGATING NETWORK EVENTS 5-2
ANALYZING AN EVENT 5-3
Defining and Applying Traffic Filters to Event Analysis Results 5-6
VIEWING EVENT CONGESTION ANALYSIS RESULTS 5-8
Corvil Bandwidth – Delay 5-8
Corvil Bandwidth – Queue Length 5-9
Expected Queuing Delay 5-9
Expected Queue Length 5-10
Expected Queuing Loss 5-11
VIEWING PRIORITY CLASS EVENT RESULTS 5-11
Corvil Bandwidth - Priority 5-11
Expected Priority Drops 5-12
IDENTIFYING EVENT TRAFFIC LEADERS 5-13
Viewing Top Applications 5-13
Viewing Packet Size Distributions 5-14
Viewing Top Talkers 5-15
Viewing Top Listeners 5-16
Viewing Top Conversations 5-17
IDENTIFYING THE SOURCE OF APPLICATION PERFORMANCE PROBLEMS 5-18
IDENTIFYING EVENT TRAFFIC PATTERNS 5-19
Average Bit Rate and Byte-counts Graphs 5-20
Average Packet Rate and Packet-counts Graphs 5-21
Active Flows Graph 5-22
IDENTIFYING EVENT MICROBURST MEASUREMENTS 5-22
IDENTIFYING NETWORK DELAY PROBLEMS 5-23
DISABLING EVENT DETECTION ON SELECTED INTERFACES 5-24
WORKING WITH MANUAL PACKET CAPTURES 5-24
SETTING DISK SPACE QUOTA FOR MANUAL AND EVENT ANALYSIS PACKET CAPTURES 5-30
SETTING A PACKET CAPTURE PASSWORD 5-30
USING MANUAL PACKET CAPTURE TO IDENTIFY EVENTS 5-31

6 BANDWIDTH SIZING 6-1

OVERVIEW 6-1
BANDWIDTH SIZING SUMMARY TABLE 6-2
SELECTING A REPORT PERIOD 6-5
Defining a Custom Report Period 6-5
SORTING THE BANDWIDTH SIZING TABLE 6-6
FILTERING THE BANDWIDTH SIZING TABLE 6-6
REPORTING BANDWIDTH SIZING RESULTS 6-6
VIEWING SIZING RESULTS 6-7
BANDWIDTH SIZING RECOMMENDATIONS 6-8
Single class Configuration Recommendations 6-8
Multi-class Configuration Recommendations 6-9
Priority Class in a Multi class Configuration Recommendations 6-9

Viewing the Sizing Graph 6-10
MONITORING SINGLE-CLASS SIZING REQUIREMENTS 6-11
MONITORING MULTI-CLASS SIZING REQUIREMENTS 6-12
IDENTIFYING NEW CLASS RESOURCE REQUIREMENTS 6-12

7 USING THE COMMAND LINE INTERFACE (CLI) 7-1

INTRODUCTION TO THE CLI 7-1
USING THE HELP FEATURE 7-2
COMPLETING A PARTIAL COMMAND NAME 7-3
USING THE SHOW COMMAND 7-3
USING THE STATUS COMMAND 7-4
CONTINUING OUTPUT AT THE --MORE-- PROMPT 7-4
DELETING CONFIGURATION OBJECTS AND ENTRIES 7-4
SAVING AND RESTORING CONFIGURATION CHANGES 7-4
LOGGING OUT OF THE BQM CLI 7-5
CONFIGURING THE BQM USING THE CLI 7-5
DEFINING A MONITOR-QUEUING-MAP 7-5
DEFINING A MONITOR END TO END MAP 7-6
DEFINING A CLASS MAP 7-7
USING NESTED CLASS-MAPS 7-9
Combining match-all and match-any Statements 7-9
Maintenance 7-10
Converting Network-Based Application Recognition (NBAR) Configurations 7-10
DEFINING A POLICY MAP 7-13
DEFINING A REMOTE SITE, ROUTER, AND INTERFACE 7-16
ATTACHING A POLICY MAP TO AN INTERFACE 7-18
SAVING CONFIGURATIONS 7-18
WORKING WITH CONFIGURATION FILES 7-18
WORKING WITH SUBNET FILTERING 7-19
USING FILTER CLASSES 7-22
CONFIGURING NETWORK MODEL DEPLOYMENTS WITH THE CLI 7-23
BASIC ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 7-23
BASIC MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT 7-27
MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT WITH REDUNDANT LOCAL SITE CONNECTIVITY 7-34
MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT WITH REDUNDANT REMOTE SITE CONNECTIVITY 7-35
DUAL-HOMED ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 7-36
DUAL-HOMED MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT 7-42
HYBRID DEPLOYMENT 7-49

8 SYSTEM ADMINISTRATION 8-1

USER ADMINISTRATION 8-1
CHANGING USER PASSWORDS 8-2
PASSWORD RECOVERY 8-2

VIEWING CURRENT USER SESSIONS 8-3
SYSTEM SETUP 8-3
INSTALLING A LICENSE 8-3
Installing a License Using SSH 8-4
CONFIGURING NETWORK SETTINGS 8-5
RESTRICTING SNMP ACCESS 8-6
RESTRICTING IP ADDRESS ACCESS 8-6
SYSTEM TIME SETTINGS 8-7
Setting the System Time 8-7
Setting the Time Zone 8-8
Configuring an NTP Time Server 8-8
SYSTEM STATUS AND RESOURCES 8-9
BACKUP AND RESTORE 8-12
RESTORING SYSTEM SOFTWARE 8-12
BACKING UP AND RESTORING CONFIGURATION AND PACKET CAPTURE FILES 8-13
UPGRADING THE APPLICATION RECOGNITION MODULE (ARM) 8-15
DIAGNOSTICS 8-17
VIEWING SYSTEM ALERTS 8-17
System Alert Types 8-18
Viewing Active and Cleared Alerts Information 8-18
Adding a Comment to a System Alert 8-19
Clearing, Reactivating and Acknowledging System Alerts 8-19
Sorting the System Alerts Table 8-20
Filtering the System Alerts Table 8-20
Generating a System Alerts Report 8-20
Using the CLI to View Alerts 8-21
VIEWING THE AUDIT TRAIL 8-21
GENERATING SYSTEM TECHNICAL SUPPORT DIAGNOSTICS INFORMATION 8-22
REVIEWING THE SYSTEM LOG 8-22
STORING SYSTEM LOG MESSAGES 8-23
WATCHDOG OPERATION 8-23
CONFIGURING FAULT NOTIFICATION 8-23
OVERVIEW 8-23
CONFIGURING ALARM SEVERITY AND FREQUENCY SETTINGS 8-28
Checking Fault Configuration Status 8-29

9 CLI COMMAND REFERENCE 9-1

CONFIGURATION MODE 9-1
CLASS-MAP CONFIGURATION MODE 9-6
POLICY-MAP CONFIGURATION MODE 9-6
POLICY-MAP CLASS CONFIGURATION MODE 9-6
MONITOR END2END MAP CONFIGURATION MODE 9-7
MONITOR-QUEUING-MAP CONFIGURATION MODE 9-7
LOCAL SITE CONFIGURATION MODE 9-7
SITE CONFIGURATION MODE 9-8
SITE ROUTER CONFIGURATION MODE 9-9
INTERFACE CONFIGURATION MODE 9-9
PEER-INTERFACE CONFIGURATION MODE 9-10

PACKET CAPTURE CONFIGURATION MODE 9-10
COMMAND REFERENCE 9-11
? 9-11
ALLOW 9-13
ATTACH 9-14
ATTACHED-PORTS 9-15
BACKUP 9-16
BANDWIDTH 9-18
CAPTURE 9-20
CAPTURE-SETTINGS 9-21
CLASS 9-22
CLASS-ADJUST 9-24
CLASS-MAP 9-26
CLEAR 9-27
CLOCK 9-28
CONNECTS-TO 9-31
COPY 9-32
CUSTOM-APPLICATION 9-35
DELETE 9-37
DESCRIPTION 9-38
DIR 9-40
DOMAIN 9-41
DURATION 9-42
END2END-TARGET 9-43
ESTIMATE-SERVICE-LEVEL 9-44
ETHERNET 9-45
EXIT 9-46
FILTER-CLASS 9-47
HELP 9-49
INTERFACE 9-51
LICENSE 9-52
LINK-ADJUST 9-53
LOCAL-SITE 9-55
LOG 9-56
LOGGING 9-57
MATCH 9-58
MATCH ANY 9-60
MATCH APPLICATION 9-61
MATCH CLASS-MAP 9-63
MATCH ETHERTYPE 9-64
MATCH IP 9-66
MATCH MPLS 9-69
MATCH TCP 9-71
MATCH UDP 9-74
MATCH VLAN 9-77
MAX-RESERVED-BANDWIDTH 9-80
MEASURE-BANDWIDTH 9-81
MEASURE-MICROBURST 9-83
MEASURE-PING 9-85
MONITOR-QUEUING 9-87

MONITOR-END2END-MAP 9-89
MONITOR-QUEUING-MAP 9-90
MORE 9-91
NO 9-93
NTP 9-95
PASSWORD 9-96
PEER-INTERFACE 9-97
PING 9-99
PING-ADDRESS 9-101
POLICY-MAP 9-102
PORT 9-104
PPP 9-105
PRIORITY 9-106
PRIORITY-LEVEL 9-107
QUEUING-TARGETS 9-109
QUEUE-LIMIT 9-110
RELOAD 9-111
RENAME 9-112
RESTORE 9-113
ROUTER 9-114
SERVICE 9-116
SERVICE-POLICY 9-117
SETUP 9-118
SHOW 9-119
SHUTDOWN 9-128
SITE 9-129
SIZE 9-131
SIZE-FOR 9-132
SNAPLENGTH 9-134
SNMP-SERVER 9-135
START 9-140
START CAPTURE 9-141
STATUS 9-142
SUBNET 9-145
SUBNET-FILTERING 9-148
TERMINAL 9-152
TRACE-EVENTS 9-153
TRACEROUTE 9-154

10 APPENDIX A: CLASS-MAPS AND CLASSIFICATION 10-1

MATCHING CUSTOMER TRAFFIC 10-1
MATCHING PRIORITIZED TRAFFIC 10-1
MATCHING APPLICATION TRAFFIC 10-2
CLASS-MAP LOGIC 10-3

11 APPENDIX B: COMMON APPLICATION STATIC PORT ASSIGNMENTS 11-1

12 APPENDIX C: SUPPORTED PROTOCOLS 12-1

13 APPENDIX D: ETHERTYPE IDENTIFIERS 13-1

14 INDEX 14-5

Preface

About this Guide

Objective

This User Guide describes how to do the following:

- Use the basic BQM CLI features
- Configure the BQM directly based on an adjacent router configuration
- Configure application filtering on the BQM
- Perform BQM administrative tasks

Audience

This document is targeted at the following types of users:

- Network Planners and Architects
- Traffic Engineers and Capacity Planners
- Network Operation and Maintenance Personnel
- IT Staff and Telco Product Managers

Prerequisite Knowledge

Basic familiarity with Linux administration, Cisco router configuration, particularly configuring access control lists (ACLs) on Cisco routers, is assumed.

Related Documentation

For more information on installing and using the other BQM products, see the following documents:

- Cisco Bandwidth Quality Manager Installation Guide
- Cisco Bandwidth Quality Manager Getting Started Guide

- Cisco Bandwidth Quality Manager Release Notes

Conventions Used in This Guide

Command descriptions use these conventions:

`Monospace` indicates variable names, directory paths, file names, and configuration command examples.

Boldface indicates names of user interface elements, such as menu options, toolbar button, dialog box and window field names, and commands and keywords that are entered literally as shown.

Italics indicate net terms and command arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets (< >).

Square brackets ([ ]) indicate optional elements.

Braces ({ }) group required choices, and vertical bars (|) separate alternative elements.

Braces and vertical bars within square brackets ([{ | }]) indicate a required choice within an optional element.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the

Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and

we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non emergencies.

- For non emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security

Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

http://www.cisco.com/offer/subscribe

The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

http://www.cisco.com/go/guide

Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

http://www.cisco.com/ipj

Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

http://www.cisco.com/en/US/products/index.html

Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

"What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html

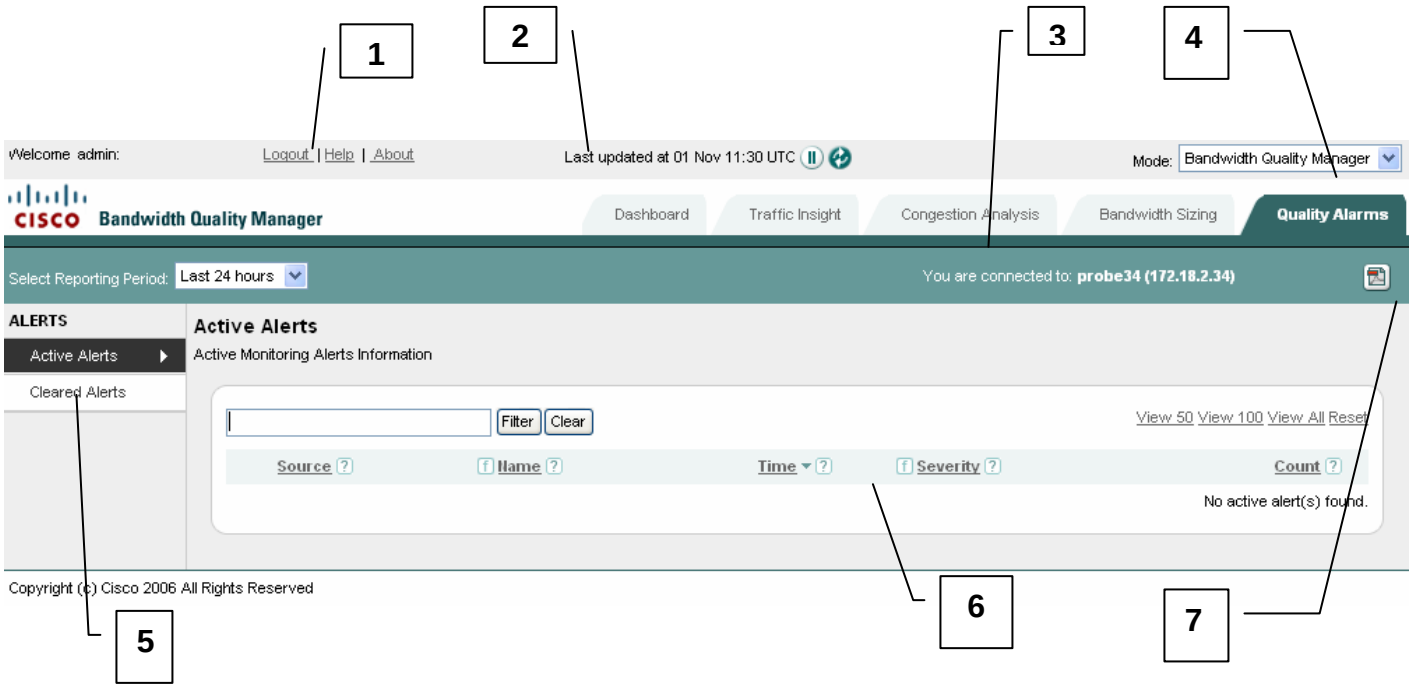
1 Bandwidth Quality Manager Overview

Cisco Bandwidth Quality Manager (BQM) is a network application congestion management appliance that provides unique visibility and analysis of traffic, bandwidth and QoS on IP access networks. You use the BQM to monitor, troubleshoot and assure network performance objectives for converged application traffic.

The BQM platform is an essential component of Cisco's solution for achieving predictable performance for data, voice and video services on IP networks. Cisco BQM builds on revolutionary technology that provides micro level visibility into the network and the congestion events compromising the user experience of network quality.

The BQM is a 1u rack-mount network device that attaches to a 10/100/1000 Ethernet network segment and performs the unique Corvil traffic measurement. The BQM supports a powerful filter classification engine that allows measurements to be carried out on specified traffic classes and/or application streams. The BQM software provides browser-based access to the monitoring and event analysis features of the product. The following illustration is an example of the Bandwidth Quality Manager user interface.

Figure 1-1: Bandwidth Quality Manager GUI



1 Links to access global features:
- Click **Logout** to log out of the Bandwidth Quality Manager.
- Click **Help** for context-sensitive information (information relevant to the current function). Help is displayed in a separate browser window.
- Click **About** to see information about the Bandwidth Quality Manager software.

2 Time of the last data update and buttons to pause the default screen refresh or to force a screen refresh.

3 Tabs for accessing the main features; the tabs are displayed in every window in the user interface (except in pop-up windows).

4 Option to change between **Bandwidth Quality Manager** and **System Administration** modes, if you are logged in as an admin user

5 Options associated with certain tabs; available features change in certain tabs depending on context.

6 Content area where information, graphs and charts are displayed.

7 Button to export the page as a pdf report.

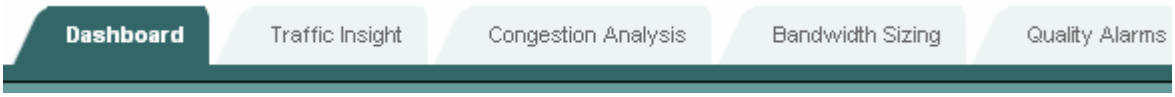
Note All times in the Bandwidth Quality Manager are typically displayed in 24-hour clock format. For example, 3:00 p.m. is displayed as 15:00.

Monitoring and Configuration Interface Features

The administrator user (admin) has full access to the system, and can use both modes of the BQM: **Bandwidth Quality Manager** and **System Administration**. The monitoring user (monitor) has access to all the monitoring features of the BQM, but does not have access to **System Administration** mode to perform configuration tasks.

In **Bandwidth Quality Manager** mode, you use the **Dashboard** tab to get an overview of monitoring activity by the BQM.

Figure 1-2: Dashboard Tab

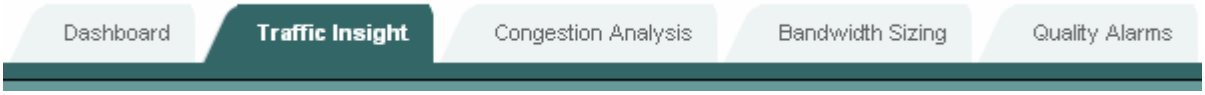


The information available from the dashboard includes:

- Top 10 Congested Interfaces – the top ten most congested interfaces as calculated by the BQM.
- WAN Traffic Leaders - the top ten applications with the highest traffic volume automatically discovered by the BQM.
- Recent Alarms - the most recent alarms triggered by quality events in the network.

You use the **Traffic Insight** tab view information for all of the interfaces you have configured in the BQM network model.

Figure 1-3: Traffic Insight Tab



The traffic statistic graphs available for each interface are as follows:

- Micro Burst Detection
- Average Rate
- Packet Rate
- Peak-to-Mean Ratio
- Packet Size Distribution

Along with the traffic statistics graphs, there are other tabs with further details that you can view for the interface:

- Applications
- Talkers
- Listeners
- Conversations

You can use these charts to identify the applications comprising the largest share of network traffic and the hosts transmitting and receiving the most traffic over a certain period.

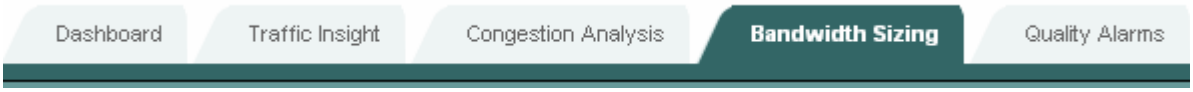
You use the **Congestion Analysis** tab to identify network congestion events for all of the interfaces you have configured in the BQM network model. For each congested interface you can analyze more information to troubleshoot a congestion event that is impacting on quality of service.

Figure 1-4: Congestion Analysis Tab

You can use the displayed Congestion Indicator values to identify the congestion level on each interface. A Congestion Indicator value greater than 1 means that loss or delay is above an acceptable level, as specified in the BQM configuration. A Congestion Indicator of less than 1 means the loss or delay is better than that specified.

You use the **Bandwidth Sizing** tab provides a guide to bandwidth utilization on network links and recommendations, where necessary, for link upgrades or adjustments to current QoS policy configuration.

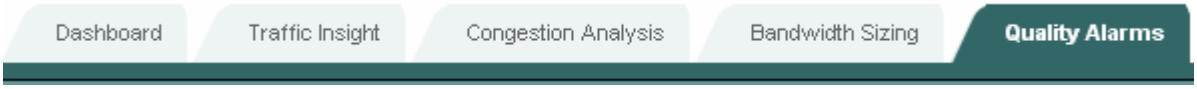
Figure 1-5: Bandwidth Sizing Tab



After you have completed configuration of the BQM network model to reflect your network, you typically should allow the system to measure traffic for at lest a week before considering the bandwidth sizing results. In many cases, you would wait until the system has accumulated a month's worth of measurements.

You use the **Quality Alarms** tab to monitor active and cleared quality alarms that are triggered by network events.

Figure 1-6: Quality Alarms Tab



The BQM includes configurable thresholds on many QoS measurements that trigger events when exceeded.

In **System Administration** mode, you use the **Configuration** tab to perform BQM configuration tasks.

Figure 1-7: Configuration Tab

You use this tab to configure the following:

- Sites, routers and interfaces – model the overall network deployment using the main components of the BQM network model
- Policy Maps – model the QoS policy configured on the routers of interest
- Class Maps – model the traffic classification scheme on the routers of interest
- Monitor-queuing-maps – enable and configure BQM QoS monitoring features for class traffic
- Monitor-end-to-end-maps – configure end-to-end network measurements
- Applications – configure custom applications to match those on your network and supplement the automatically discovered set supported by the BQM

You use the **System Alerts** tab to monitor active and cleared system alerts triggered by conditions on the BQM platform itself.

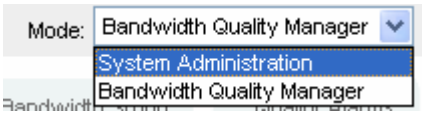
Figure 1-8: System Alerts Tab

Switching Between Modes

If you are logged in as an admin user, you can switch between the two GUI modes:

- Bandwidth Quality Manager
- System Administration

Figure 1-9: GUI Mode Options for Admin Users



You choose the required mode from the **Mode** list.

Selecting a Reporting Period

By default, each tab in **Bandwidth Quality Manager** mode displays summary information for the last 24 hours.

Figure 1-10: Selecting a Report Period

You can choose different reporting periods by clicking the **Reporting Period** list. The following reporting periods (and associated update rates) are available:

Last 1 hour – 5 minute updates
Last 12 hours – 5 minute updates
Last 24 hours – 5 minute updates
Last 48 hours – 30 minute updates
Last 7 days – 1 hour updates
Last 30 days - 3 hour updates
Last 60 days – 6 hour updates

The text at the top of the screen indicates the last time at which an update was made.

The screen itself refreshes every five minutes, but new measurements are displayed according to the update rate listed above for each reporting period.

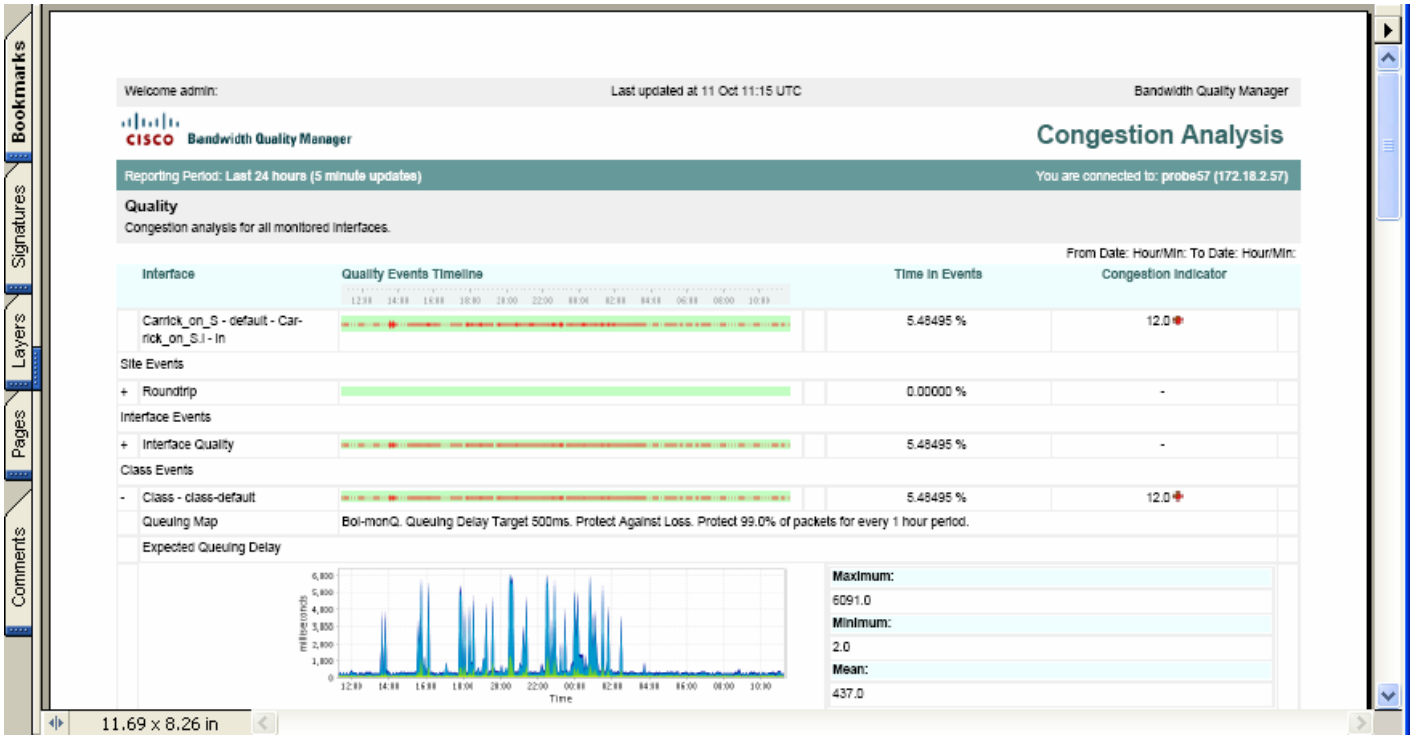
Generating Reports

You can generate a report in .pdf format at any point when viewing information on the **Traffic Insight**, **Congestion Analysis**, **Bandwidth Sizing**, or **Quality Alarm**s tabs.

To generate a report, click .

The generated report is available for download in .pdf format. Reports are not stored on the BQM.

Figure 1-11: Generating a Report



The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all interfaces with a Congestion Indicator value greater than one. If the original results are displayed across multiple pages onscreen, then you use the View All option so that the report contains the data from all such screens. Otherwise the report will present the results displayed on the current screen only.

The time displayed at the top of each report is the configured time zone of the BQM.

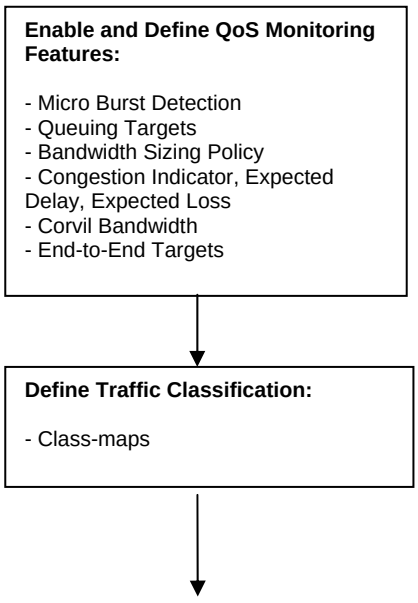
2 Configuring BQM QoS Monitoring

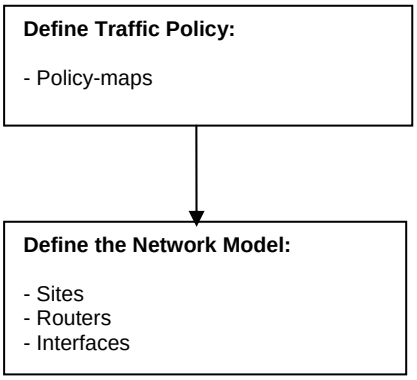
This chapter describes how you configure the BQM to model your network deployment and existing router QoS policies as closely as possible. This chapter contains the following sections:

- Overview
- Configuring QoS Monitoring Features
- Configuring Class Maps
- Configuring Policy Maps
- Configuring Custom Applications
- Configuring Sites, Routers, and Interfaces

Overview

Configuring the BQM comprises the following tasks:





These tasks can be performed using both the CLI and the GUI.

If you are performing a manual configuration using the CLI or GUI, you need to define monitor-queuing-maps, monitor-end-to-end-maps, and class-maps before configuring policy-maps or sites, routers, or interfaces. You then configure policy-maps before configuring the network model objects. This is because the monitor-queuing-maps and class-maps are referenced during policy-map configuration, and policy-maps are in turn referenced during interface configuration.

Enabling QoS Monitoring Features with Monitor Queuing and End to End Maps

To enable BQM QoS Monitoring features and view results for these features, there must be a monitor-queuing-map applied to an interface in the BQM configuration. To view end-to-end delay and loss measurements between the local site and remote sites, you must configure a monitor-end-to-end-map and apply it to each relevant remote site.

A monitor-queuing-map establishes the set of QoS-aware monitoring features enabled in the product for a particular interface (or group of interfaces). The monitor-queuing-map also establishes an associated quality event detection policy to be enabled for the classified traffic.

A monitor-queuing-map comprises the following: a name, microburst, queuing QoS target, sizing policy, expected service level and Corvil Bandwidth settings, and associated optional quality event detection thresholds.

Default Monitor-Queuing-Map

The system provides a default monitor-queuing-map, named monitor-queuing-map-default. This default monitor-queuing-map is automatically applied when you define a policy-map. The default monitor-queuing-map cannot be deleted. You can, however, edit the default map.

Microburst detection is enabled in the default monitor-queuing-map. However, no microburst-related events will be displayed in the **Congestion Analysis** screen for interfaces or classes using the default map.

The default queuing delay target is set to 500 ms. Event detection is enabled, so if the calculated expected delay value exceeds 500 ms (or if any loss is detected), an event is triggered.

Congestion Indicator and Corvil Bandwidth class sizing calculations are based on a sizing policy where 99.9% of packets must meet the 500 ms delay target in any 4-hour period. Event detection is enabled against Corvil Bandwidth values exceeding 1005 of the interface capacity.

So using the default monitor-queuing-map means that you can see the following **Congestion Analysis** tab results:

- Congestion Indicator values and graphs
- Microburst Detection values and graphs
- Expected Loss and Delay graphs
- Corvil Bandwidth Delay graphs

You can also view **Bandwidth Sizing** tab results.

The **Traffic Insight** tab will show Microburst Detection results and Congestion Indicator values along with all the standard traffic statistics graphs and charts.

Enabling Microburst Event Detection

Peak measurement data at millisecond resolution is enabled by default when you configure a monitor-queuing-map or use the default monitor-queuing-map. However, to be able to identify and investigate peak threshold violations you need to configure the required threshold in the monitor-queuing-map.

To enable microburst event detection on the BQM without enabling any other features of the product, you configure only a microburst measurement resolution and event detection threshold in the monitor-queuing-map.

Enabling and Disabling Congestion Analysis and Bandwidth Sizing Features

Expected Delay and Loss graphs are enabled by default when you configure a monitor-queuing-map or use the default monitor-queuing-map.

The following table identifies which monitor-queuing-map parameters must be configured to enable the following BQM quality monitoring features presented in Bandwidth Quality Manager mode:

- Congestion Indicator
- Corvil Bandwidth (Delay and Loss)
- Bandwidth Sizing

Table 2-1: Monitor-Queuing-Map Attributes Required to Enable Monitoring Features

To enable and configure this feature…	Enable and configure a queuing delay target?	Configure a sizing policy?	Enable and configure Corvil Bandwidth measurement?
Congestion Indicator	Yes	Yes	Not applicable
Corvil Bandwidth (Delay and Loss)	Yes	Not applicable	Yes
Bandwidth Sizing	Yes	Yes	Yes

The following describes which monitor-queuing-map parameters must be configured to enable the BQM quality monitoring features presented in the **Congestion Analysis** and **Bandwidth Sizing** tabs in Bandwidth Quality Manager mode.

Queuing Targets and Sizing Policy
The results presented on the **Congestion Analysis** tab include graphs of expected queuing delay and expected loss, and Congestion Indicator values, all calculated by the BQM. Both the **Congestion Analysis** and **Bandwidth Sizing** tabs present results based on Corvil Bandwidth calculations. To configure Congestion Indicator and expected queuing delay and loss calculation, and Corvil Bandwidth calculation for congestion analysis and for bandwidth sizing, you enable and configure the following in the monitor-queuing-map:

- queuing delay target
- sizing policy

The queuing delay target takes the form of a configured millisecond value, for example 150 ms.

You also have the option of enabling event detection when a specified threshold is exceeded:

- Expected delay exceeds the configures queuing delay value
- Any expected loss is detected
- Corvil Bandwidth exceeds a certain proportion of interface capacity or a certain kbps value

You do not explicitly enable or disable a separate loss target.

When event detection is enabled for any of these triggers, and a threshold is exceeded, you can identify and investigate the corresponding reported events in the **Congestion Analysis** tab.

Note The **Congestion Analysis** tab also includes a **Corvil Bandwidth – Queue Length** graph based on the queue length configured for a class. The Corvil Bandwidth values plotted represent the minimum bandwidth required to avoid packet loss due to queue buffer overflow. For example, if the queue length configured for the class is 64 packets, then the graph displays the bandwidth required to prevent the queue for the class traffic building up past 64 packets.

The queue length limit (in packets) is configured for the class when you are attaching a class to a policy-map. For more information on configuring a queue length limit for a class, see the section “Configuring Policy Maps.” If you do not configure an explicit queue length limit, then the default value of 64 packets is used by the system when calculating the values plotted in the **Corvil Bandwidth – Queue Length** graph.

The sizing policy parameters enable you to permit a fraction of the packets during the defined busy period to violate the configured queuing targets. Permitting a certain fraction of the packets to violate the queuing targets allows a statistical softening of the required bandwidth down from that needed to guarantee no loss or delay whatsoever for every single packet. For example, by setting the percentage of packets to protect to 99%, the resulting Corvil Bandwidth value will be sufficient to guarantee that 99% of arriving packets experience a total per-hop delay no greater than the configured queuing delay value.

The busy period for the network is the timescale that has historically seen the greatest volumes of traffic. So if the network busy period has been identified as 30 minutes, you will want to make sure that the sizing calculation takes every 30-minute period of traffic into account. The resulting sizing calculation is sufficient to ensure that the configured queuing delay and loss targets are met for the configured fraction of packets over any consecutive period of this length. For example, if the proportion of traffic to protect is set to 99% and the busy period is set to 30 minutes, and bandwidth sizing is carried out for a 24-hour period, then the resulting Corvil Bandwidth values guarantee that over each of the 282 groups of consecutive 30-minute periods that fit entirely within the full 24 hours, no more than 1% of the packets that arrive during any given 30-minute period are delayed by more than the defined delay target.

For Queue Length Corvil Bandwidth, the sizing calculation produces the bandwidth sufficient to ensure that the protected proportion of packets see a queue-length no greater than the configured queue-limit. This bandwidth is an upper-bound on the bandwidth required to protect the packets against tail drop.

If you do not configure all the relevant parameters that support a particular feature, then you will not be able to view data or graphs for that feature in **Bandwidth Quality Manager** mode. The relevant column values or graphs will indicate that the supporting parameters are not configured.

Note Conversely, to disable the Congestion Analysis or Bandwidth Sizing features, you need to disable the relevant parameter(s) in any monitor-queuing-map that is being applied to a given interface or class.

Because the default monitor-queuing-map is applied to interfaces by default, you also need to disable the parameter in the default monitor-queuing-map.

For more information on the default monitor-queuing-map, see the following section, “Default Monitor-Queuing-Map.”

End-to-End Measurements

The purpose of a monitor-end-to-end-map is to define the required end-to-end QoS monitoring features, and associated quality event detection thresholds, for traffic from the local site to remote sites. A monitor-end-to-end-map comprises the following: a name, ping interval and packet size settings, and associated delay and loss event detection thresholds. A monitor-end-to-end-map establishes an end-to-end delay and loss-based event detection policy for traffic between the local site and remote sites.

The system provides a default monitor-end-to-end-map, named end2end-target-default. This default monitor-end-to-end-map is automatically applied when you define a remote site. The default monitor-end-to-end-map cannot be deleted, but can be edited.

The system is also preconfigured with a selection of monitor-end-to-end-maps that you can use depending on the deployment you are modeling.

Classifying Traffic with Class Maps

You configure class-maps to classify traffic and establish the traffic classification scheme to be used in the defined traffic policy (policy-map) for an interface.

A class-map comprises the following: a name, a series of match rules, and, if more than one match rule is defined, an instruction on how to evaluate these match commands. The match rules are used to specify various criteria for classifying packets. If a packet matches the specified criteria, that packet is considered a member of the class and is processed according to the QoS specifications set in the traffic policy. Packets that do not meet any of the configured match rules are classified into the default traffic class.

The system provides a default class, named class-default. This default class is automatically applied when you define a single-class policy-map. The default class cannot be deleted or edited.

If you are modeling a multi-class configuration on the router of interest, you define multiple class-maps as appropriate. These class-maps are then each referenced in the multi-class policy-map that you define.

Modeling Router QoS Configuration with Policy Maps

The purpose of a policy-map is to apply the required QoS features, and associated quality event detection thresholds, to the classified traffic. A policy-map comprises the following: a name, one or more traffic classes (previously defined by class-maps) and the QoS policies and associated quality event detection thresholds (previously defined by monitor-queuing-maps). A policy-map establishes a traffic policy for the classified traffic that is then applied to a site router interface.

If you are modeling a single-class configuration on the router of interest, the policy-map will comprise only the default class, named class-default. If you are modeling a multi-class configuration, then the policy-map comprises references to each of the defined class-maps.

Completing the Network Model with Sites, Routers, and Interfaces

The components of the network model configuration include the following:

- Local site
- Remote site(s)
- Site subnet(s)
- Router(s)
- Interface(s)

The following table describes the main components of the network model:

Table 2-2 Network Model Components

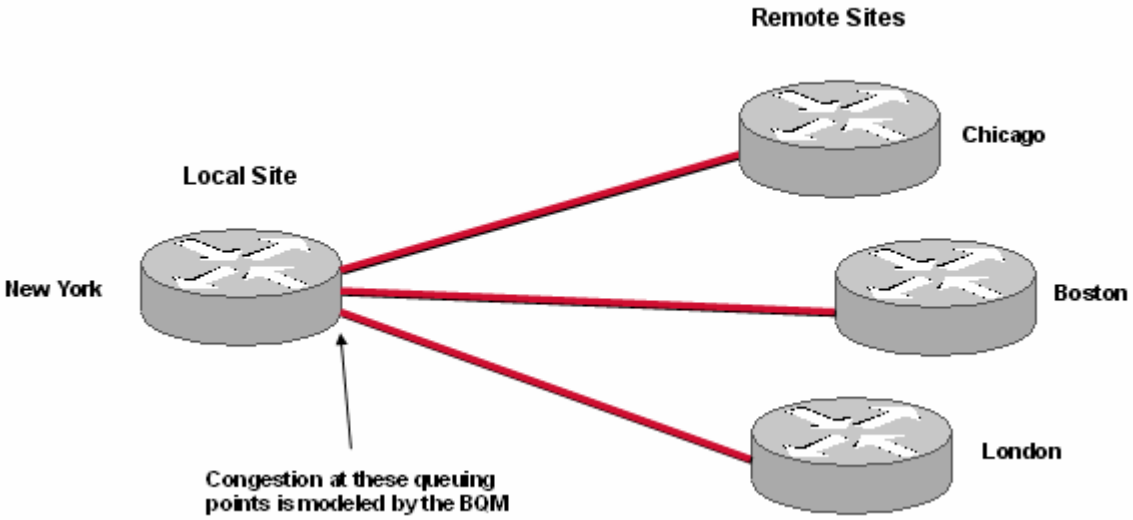
Component	Description
Local Site	A representation of a physical site where the BQM is installed in the network of interest. A local site is defined in the network model (at a minimum) by specifying network subnets.
Remote Site	A representation of a physical site that is connected to, but remote from, the local site in the network of interest. A remote site is defined (at a minimum) by specifying network subnets.
Site subnet	The subnet address that identifies a site. Traffic with the same destination address as the configured subnet address is considered to be inbound to the site. Traffic with the same source address as the configured subnet address is considered to be outbound from the site.
Router	A representation of a physical router installed in a location that is being represented in the network model by a local or remote site.
Interface	A representation of the interface(s) on a site router. The interface attributes configured should match those on the router being modeled as closely as possible. Interface results in Bandwidth Quality Manager mode represent the traffic outbound from sites.
Peer-interface	A representation of the Service Provider router interface(s) to which local and remote site interfaces connect in an MPLS VPN, Internet VPN, Private VPN network model. The peer-interface attributes configured should match those on the router being modeled as closely as possible. Peer-interface results in Bandwidth Quality Manager mode represent the traffic inbound to sites.

The network model is used to take knowledge of the network topology and apply the BQM technology within it. You choose the supported network model deployment that most accurately captures the network configuration. The purpose of a local site is to represent the physical site where the BQM is installed in the network of interest. A local site is defined in the network model (at a minimum) by specifying network subnets.

The purpose of a remote site is to represent a physical site in the network that is connected to, but remote from, the local site. A remote site is defined (at a minimum) by specifying network subnets.

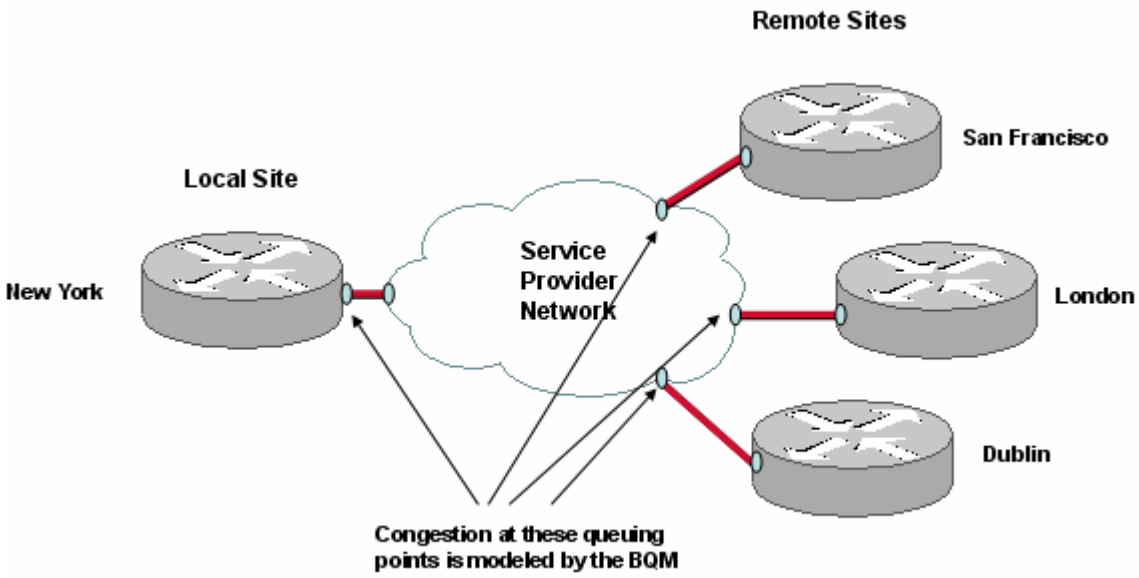
Each site comprises at least one router and its associated interfaces, configured to match the details of the network devices being modeled.

Figure 2-1: ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Network Model



In the example shown here, the local site is connected directly to three remote sites. The local site router has three interfaces being represented, with each interface connected to a single remote site router interface. All sites are identified by subnet addresses. The policy-maps configured on each router interface reflect the policy configurations on the physical routers being modeled.

Figure 2-2: MPLS VPN, Internet VPN, Private VPN Network Model



In the example shown here, the local site is connected via a Service Provider network to three remote sites. The local site router has one interface being represented, to the SP PE router. Similarly, the remote sites are each connected to an SP PE router on the other side of the network cloud. All sites are identified by subnet addresses.

The figure indicates that the interfaces on the SPN routers to which the local and remote sites connect are also modeled. They are called peer-interfaces in the BQM network model. When you are monitoring the network with the BQM, the peer-interfaces represent the traffic inbound to sites, whereas the interfaces represent the traffic outbound from sites. The policy-maps configured on each router interface should reflect as closely as possible the policy configurations on the physical routers being modeled.

Custom Applications

You can define custom applications to use within class-maps for traffic classification. A custom application definition comprises the following: a name, match rule(s).

The system provides a default set of auto-discovered applications and predefined protocols as listed on the **Applications** page. The predefined applications cannot be edited or deleted, but you can edit or delete the predefined protocols.

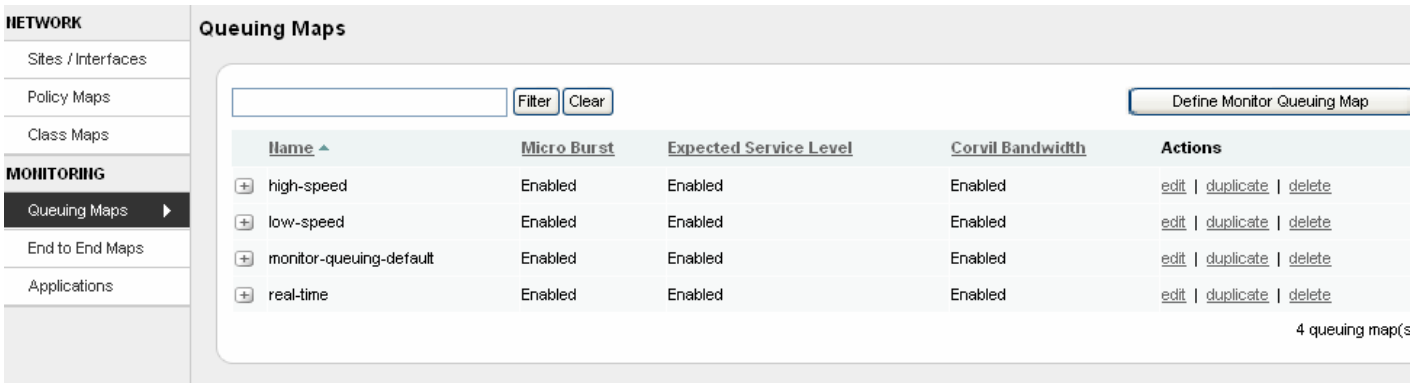
Configuring QoS Monitoring Features

The BQM product provides QoS monitoring results and alerting based on both per-hop and end-to-end network traffic measurements. To view these results you need to configure monitor-queuing-maps and monitor-end-to-end-maps. Monitor-queuing-maps and end-to-end maps are not found on Cisco routers, these are specific to the BQM configuration. Monitor-queuing-maps enable QoS monitoring features and define the quality thresholds used to report on traffic such as the maximum delay that a class can tolerate. Monitor-end-to-end-maps define quality thresholds for round-trip delay and loss between the local site and remote sites.

Configuring a Monitor-Queuing-Map

You can define monitor-queuing-maps in the GUI from the **Monitor Queuing Maps** page in the **Configuration** tab.

Figure 2-3: Monitor Queuing Maps



The **Monitor Queuing Maps** page displays the current list of configured monitor-queuing-maps in the system. Click to view the configuration details for a given listed monitor-queuing-map.

The following table describes the information displayed on the page:

Table 2-3 Monitor-Queuing-Map Page

Name	Displays the name of the monitor-queuing-map.
Micro Burst	Displays whether microburst measurement is enabled for the monitor-queuing-map. If no threshold is configured, you will not see any related events reported in the Congestion Analysis or Quality Alarms tabs in Bandwidth Quality Manager mode.
Expected Service Level	Displays whether expected service level calculations are enabled in this monitor-queuing-map. You must enable Expected Service Level calculations to see Congestion Indicator, Expected Queuing Delay and Expected Queuing Loss results in Bandwidth Quality Manager mode.
Corvil Bandwidth	Displays whether Corvil Bandwidth calculations are enabled in this monitor-queuing-map. You must enable Corvil Bandwidth calculation to see Corvil Bandwidth Delay and Loss graphs in Congestion Analysis or any Bandwidth Sizing results in Bandwidth Quality Manager mode.
Actions	edit – click to edit monitor-queuing-map details duplicate – click to duplicate the details of the selected monitor-queuing-map in a new map delete – click to delete the monitor-queuing-map.

To define a monitor-queuing-map, you do the following:

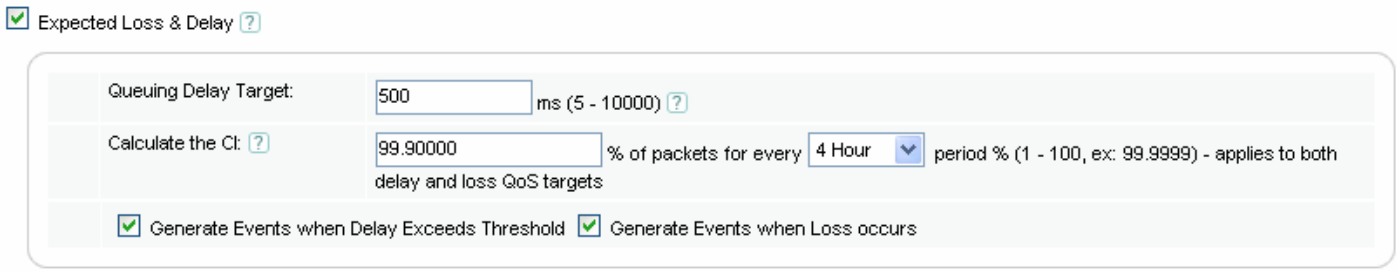
Step 1 Click **Define Monitor Queuing Map**.

Step 2 Enter a unique name for the monitor-queuing-map in the **Name** field.

Step 3 Enter a brief text description for the monitor-queuing-map in the **Description** field.

Step 4 Configure the combination of parameters that will enable the monitoring features you want to set.

Figure 2-4: Expected Delay and Loss Configuration



Configuring Expected Queuing Delay and Loss

To enable the calculation of expected delay and loss results, check the **Expected Loss and Delay** check box.

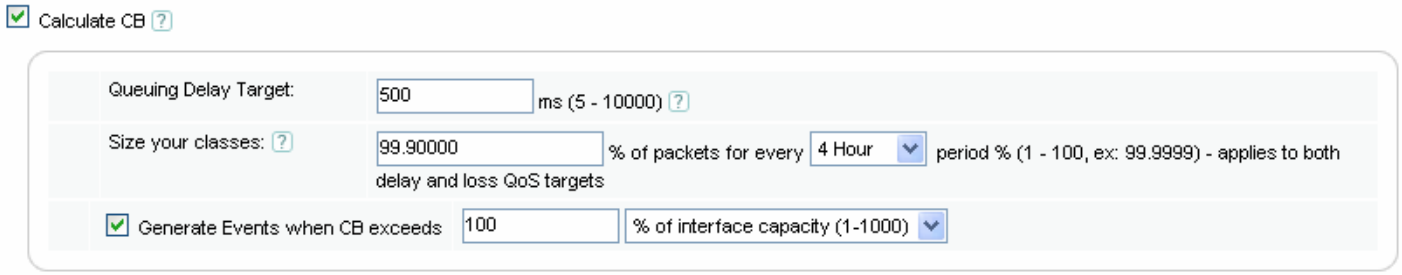
To configure queuing QoS targets for the expected loss and delay calculations, enter a queuing delay target in milliseconds in the **Queuing Delay Target** field [Range: 5 - 10000 ms, Default 500 ms].

To configure Congestion Indicator (CI) calculation, you configure a sizing policy in the **Calculate the CI** fields (also used for bandwidth sizing). Enter a percentage value in the first field [Range: 0.0-100.0000%, Default 99.90000% (Six significant figures)]. This value determines the percentage of traffic (for example 99.9999%) that must meet the configured queuing targets (both delay and loss). Next, select a busy period from the list on which to base the policy (Default: 4 hours). The busy period is the timescale that has historically seen the greatest volumes of traffic.

Note These parameters are always identical to the Size your classes parameters set below in the Calculate CB section. This ensures that the Congestion Indictor reflects violations with respect to the sizing policy.

To enable event detection when the calculated delay exceeds the configured delay target, check the **Generate Events when Delay Exceeds Threshold** check box. The queuing delay target you configure sets the threshold value that must not be exceeded. Similarly, check the **Generate Events when Loss occurs** check box to enable event detection if the expected loss calculation indicates any packet loss.

Figure 2-5: Corvil Bandwidth Configuration



Configuring Corvil Bandwidth (CB) Measurement

To enable calculation of Corvil Bandwidth values for bandwidth sizing, check the **Calculate CB** check box. If you have already enabled expected loss and delay calculation with defined queuing targets and sizing policy values, these values are automatically populated in the relevant fields for Corvil Bandwidth calculation. Only one set of queuing targets and sizing policy values can be specified in a single monitor-queuing-map.

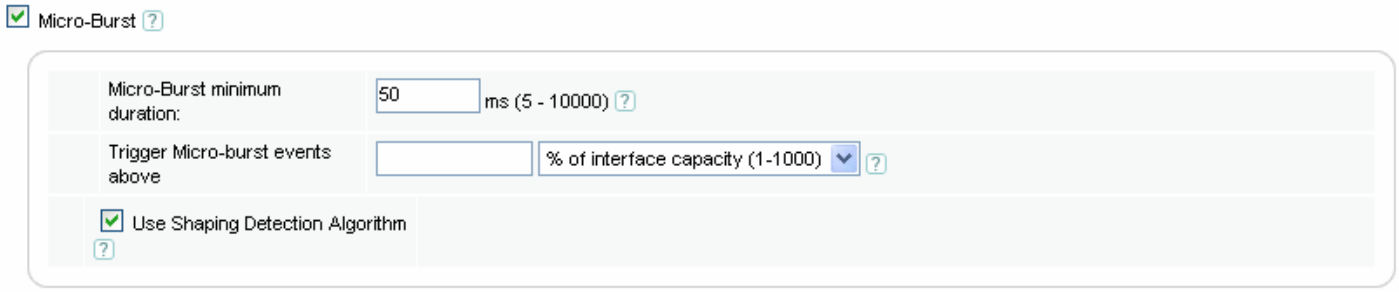
If you are enabling bandwidth sizing with Corvil Bandwidth but are not enabling expected loss and delay calculation, then to configure queuing QoS targets for the Corvil Bandwidth calculations, enter a queuing delay target in milliseconds in the **Queuing Delay Target** field [Range: 5 - 10000 ms].

To configure a sizing policy for bandwidth sizing in the **Size your classes** fields, enter a percentage value in the first field [Range: 0.0-100.0000%. (Six significant figures)]. This value determines the percentage of traffic (for example 99.9999%) that must meet the configured queuing targets (both delay and loss). Next, select a busy period from the list on which to base the policy. The busy period is the timescale that has historically seen the greatest volumes of traffic.

Note These parameters are always identical to the **Size your classes** parameters set above in the **Expected Loss and Delay** section. This ensures that the Congestion Indictor reflects violations with respect to the sizing policy.

To set a Corvil Bandwidth threshold, at which event detection is triggered, enter a value in the **Generate Events when CB Exceeds** field as a percentage of the link bandwidth [Range: 1 - 1000] or in kbps [Range: 1 - 10000000].

Figure 2-6: Microburst Configuration



Configuring Microburst Detection

To enable Micro Burst Detection, check the **Micro Burst Detection** check box.

To enter a minimum millisecond resolution for peak measurements in the **Micro Burst minimum duration** field [Range: 5 - 10000 ms].

To configure a threshold value at which to trigger event detection, enter a value in the **Trigger Micro burst events above** field as either a percentage of the link bandwidth [Range: 1 - 1000] or in kbps [Range: 1 - 10000000].

The **Use Shaping Detection Algorithm** check box is checked by default. We recommend that you leave this feature enabled, because it allows you to identify traffic from a remote site to the local site that is being shaped. For example, if you are monitoring a 2 Mbps link from a remote site, and the measured microburst values are flat-lining at a lower rate, say 1 Mbps, then the traffic from the remote site to the local site is being shaped to this rate.

Step 5 Click **Save**.

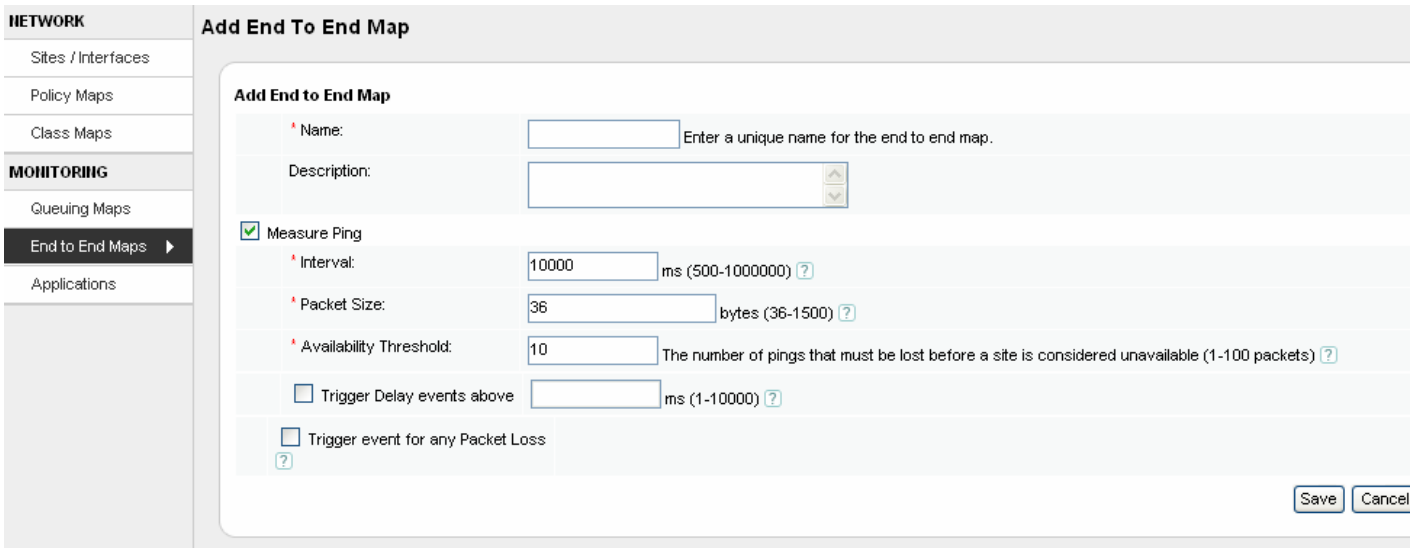
The new monitor-queuing-map is saved and displayed on the **Monitor Queuing Maps** page. It can now be used when defining policy-maps. If you click **Save** without configuring any details, the monitor-queuing-map will contain the default settings. The default settings are as follows:

- Micro Burst – enabled (50 ms with shape detection)
- Queuing Targets – delay 500 milliseconds and loss protection enabled
- Bandwidth Sizing Policy – protect 99.9% of packets in every 4-hour period
- Expected Service Level (Expected Delay and Loss graphs) – enabled
- Corvil Bandwidth Monitoring - enabled

Configuring a Monitor End-to-End Map

You can define monitor-end-to-end-maps in the GUI from the **End-to-End Maps** page in the **Configuration** tab.

Figure 2-7: Monitor End-to-End Maps

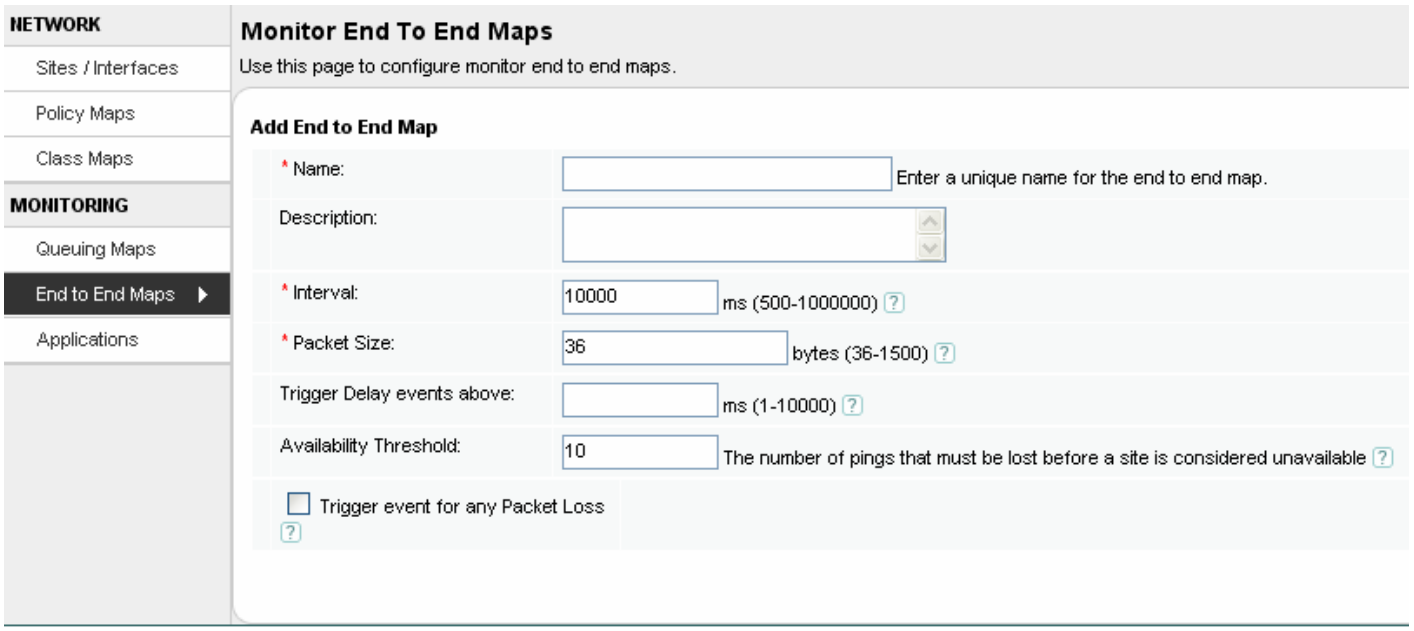


The **Monitor End to End Maps** page displays the current list of configured monitor-end-to-end-maps in the system. The following table describes the information displayed on the page:

Table 2-4 Monitor End to End Map Page

Column	Description
Name	Displays the name of the monitor-end-to-end-map.
Interval	Displays the configured ping packet interval for the monitor-end-to-end-map.
Packet Size	Displays the ping packet size configured for the monitor-end-to-end-map.
End to End Delay	Displays whether an event detection threshold for end-to-end delay is configured.
End to End Packet Loss	Displays whether an event detection threshold for end-to-end loss is configured.
Actions	**edit** – click to edit monitor-end-to-end-map details **duplicate** – click to duplicate the details of the selected monitor-end-to-end-map in a new map **delete** – click to delete the monitor-end-to-end-map.

Figure 2-8: End-to-End Map Configuration



To define a monitor-end-to-end-map, you do the following:

Step 1 Click **Add End to End Map**.

Step 2 Enter a unique name for the monitor-end-to-end-map in the **Name** field.

Step 3 Enter a brief text description for the monitor-end-to-end-map in the **Description** field.

Step 4 Check the **Measure Ping** check box.

Step 5 To configure the ping packet interval, enter a value in milliseconds in the **Interval** field.

Step 6 To configure the ping packet size, enter a value in bytes in the **Packet Size** field.

Step 7 To establish the number of pings that must be lost before a site is considered unavailable, enter a value in the **Availability Threshold** field.

Step 8 To enable event detection and set an event detection threshold based on measured end-to-end packet delay, enter a delay value in milliseconds in the **Trigger Delay events above** field.

Step 9 To enable event detection if any end-to-end packet loss is detected, check the **Trigger event for any Packet Loss** check box.

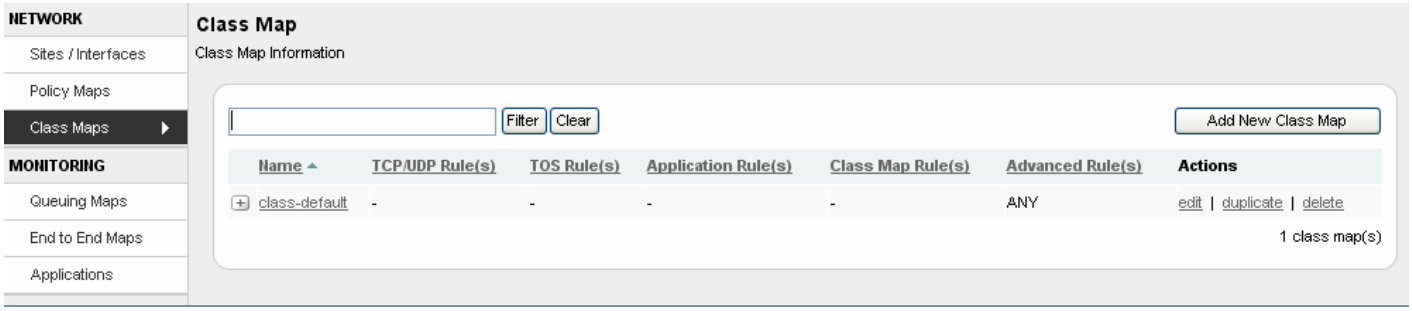
Step 10 Click **Save**.

The new monitor-end-to-end-map is saved and displayed on the **Monitor End to End Maps** page. The monitor-end-to-end-map is available to select when defining remote sites.

Configuring Class Maps

You can define class-maps in the GUI from the **Class Maps** page in the **Configuration** tab.

Figure 2-9: Class Map Configuration



The **Class Maps** page displays the current list of configured class-maps in the system. The following table describes the information displayed on the page:

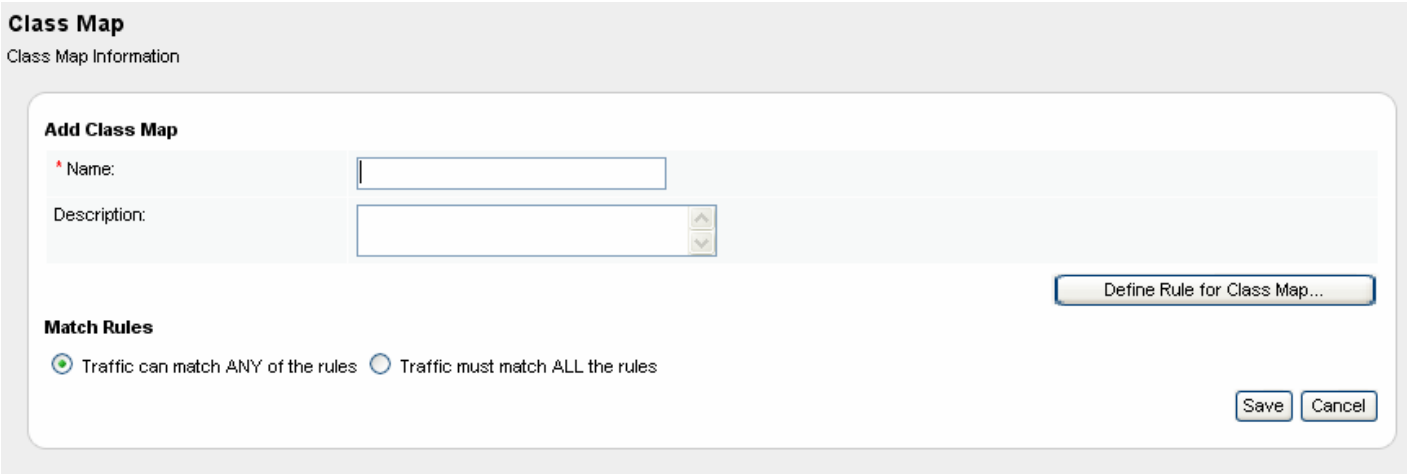
Table 2-5 Class Map Page

Column	Description
Name	Displays the name of the class-map.
TCP/UDP Rule(s)	Displays a summary if a single 5-tuple TCP or UDP match rule (source and destination ports and addresses) is defined, or, if there are multiple match rules of this type defined, the number defined in the class-map.
TOS Rules	Displays a summary if a single Type of Service (ToS) match rule (IP Precedence, ToS, DSCP) is defined, or, if there are multiple match rules of this type defined, the number defined in the class-map.
Application Rule(s)	Displays a summary if a single application match rule is defined, or, if there are multiple match rules of this type defined, the number defined in the class-map.
Class map Rule(s)	Displays a summary if a single match rule referencing other class-maps is defined, or, if there are multiple match rules of this type defined, the number defined in the class-map.
Advanced Rule(s)	Displays a summary if a single advanced match rule (IP Protocol, MPLS, vLAN, Ethertype) is defined, or, if there are multiple match rules of this type defined, the number defined in the class-map.
Actions	**edit** – click the link to edit the class-map configuration.

	duplicate – click the link to duplicate the class-map configuration. **delete** – click the link to delete the class-map.

Note If you are using Network-Based Application Recognition (NBAR) on the router being modeled in the BQM configuration, you need to convert the NBAR match rules from the router configuration to equivalent BQM match rules. For more information, see the section "Converting Network-Based Application Recognition (NBAR) Configurations" in the chapter "Using the Command Line Interface (CLI)."

Figure 2-10: Class Map Configuration



To define a class-map, you do the following:

Step 1 Click **Define Class Map**.

The **Add Class Map** page is displayed.

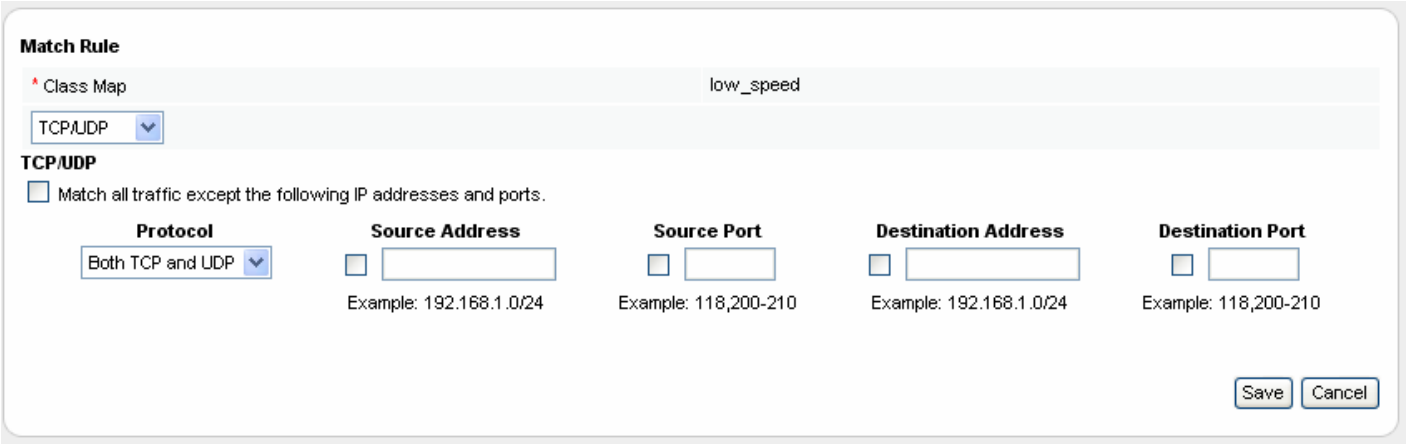
Step 2 Enter a unique name for the class-map in the **Name** field.

Step 3 Enter a brief text description for the class-map.

Step 4 Click **Define Rule for Class Map**.

The **Define Match Rule** page is displayed.

Figure 2-11: Defining a Match Rule



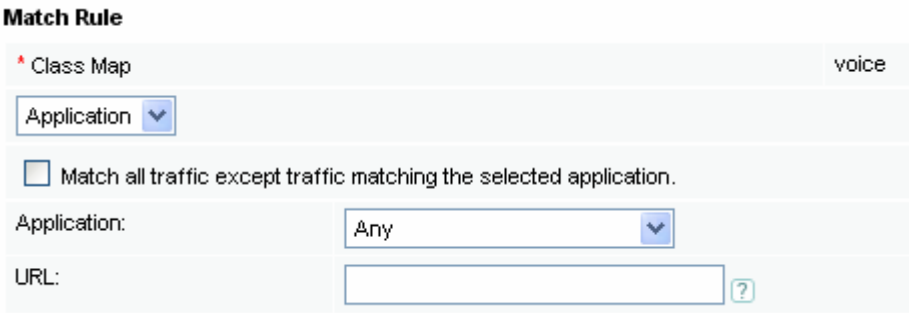
Step 5 Select the match rule type from the list.

Step 6 If you select **TCP/UDP**, then select and fill out the source and destination port and address fields as required.

To match all traffic except the IP addresses and ports you specify, check the box labeled **Match all traffic except the following**.

Step 7 If you select **Application**, then select the chosen application from the list.

Figure 2-12: Defining a Match Rule - Applications

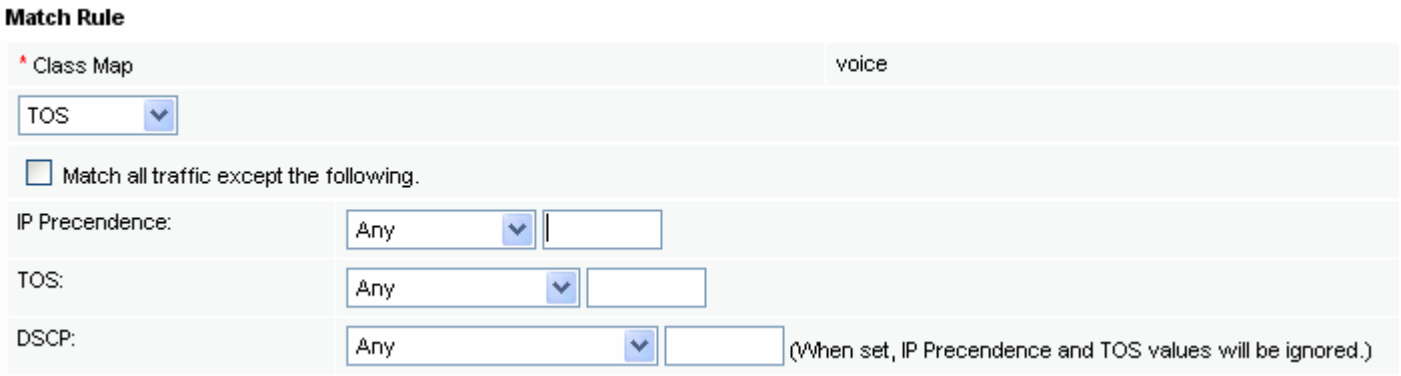


To match all traffic except the application you specify, check the box labeled **Match all traffic except the following**.

Note You can only specify a URL if HTTP is the selected application.

Step 8 If you select **Type of Service (TOS)**, then select the required IP Precedence and TOS, or DSCP values from the respective lists.

Figure 2-13: Defining a Match Rule - TOS

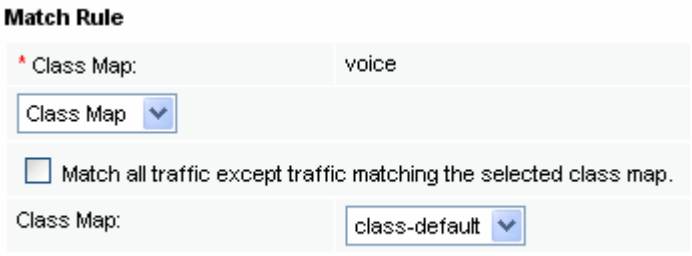


To match all traffic except the IP Precedence, TOS, or DCSP values you specify, check the box labeled **Match all traffic except the following**.

Note IP precedence and TOS values can be specified in the same rule. However, entering DSCP values means you cannot specify values of another type within the same TOS rule.

Step 9 If you select **Class-map**, then select the required, previously configured class-map from the list.

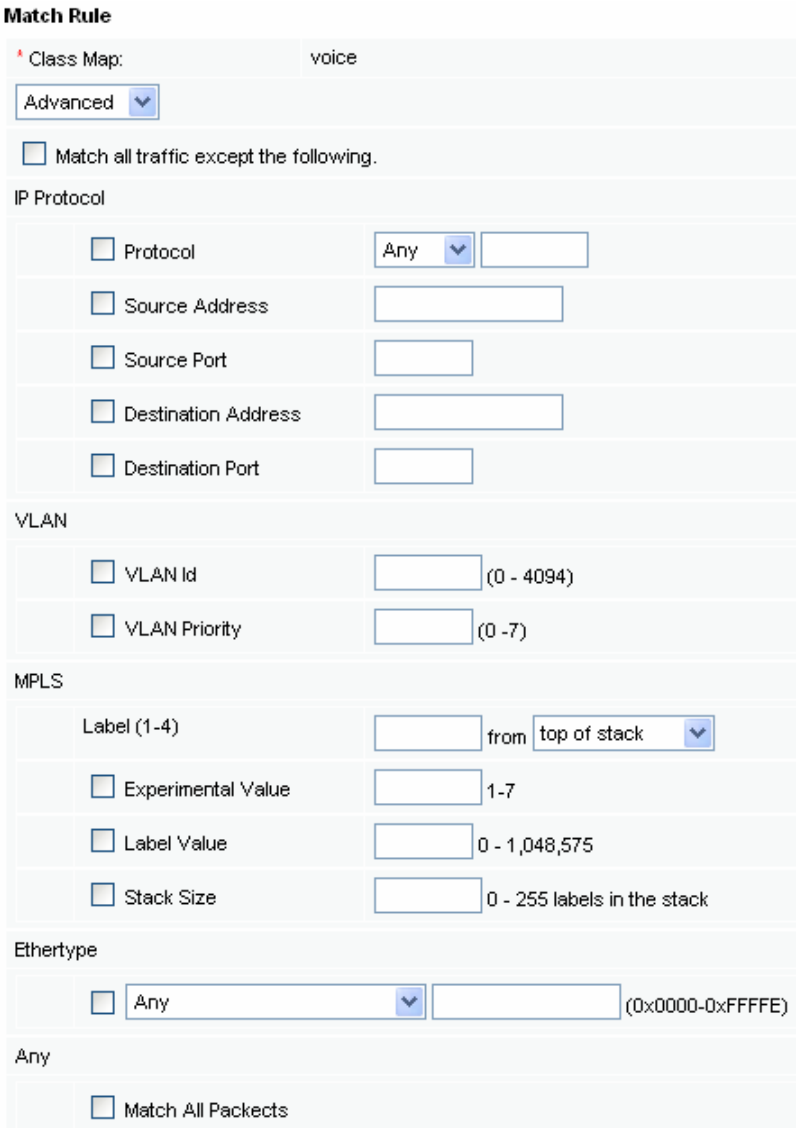
Figure 2-14: Defining a Match Rule – Class Map



To match all traffic except class-map you specify, check the box labeled **Match all traffic except the following**.

Step 10 If you select **Advanced**, then select IP Protocol, VLAN, MPLS, or Ethertype as required, and then select or enter the required values as appropriate.

Figure 2-15: Defining a Match Rule – Advanced



To match all traffic except the IP Protocol, VLAN, MPLS or Ethertype values you specify, check the box labeled **Match all traffic except the following**.

Step 11 Click S**ave**.

Step 12 Select the appropriate radio button to define whether you want traffic to match ANY of the defined match rules or to match ALL of the defined match rules.

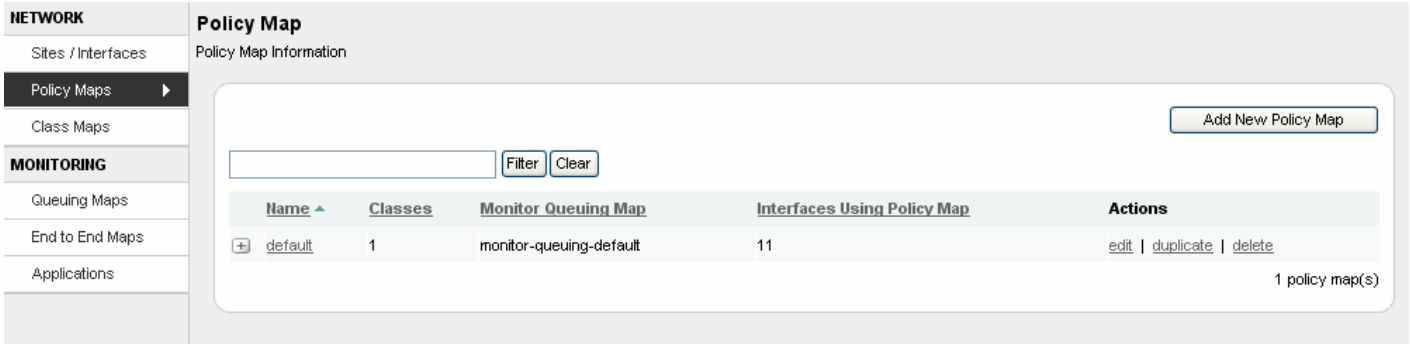
Step 13 Click **Save**.

The configured class-map is saved and the **Class Maps** page is displayed.

Configuring Policy Maps

You can define policy-maps in the GUI from the **Policy Maps** page in the **Configuration** tab.

Figure 2-16: Policy Maps



The **Policy Maps** page displays the current list of configured policy-maps in the system. The following table describes the information displayed on the page:

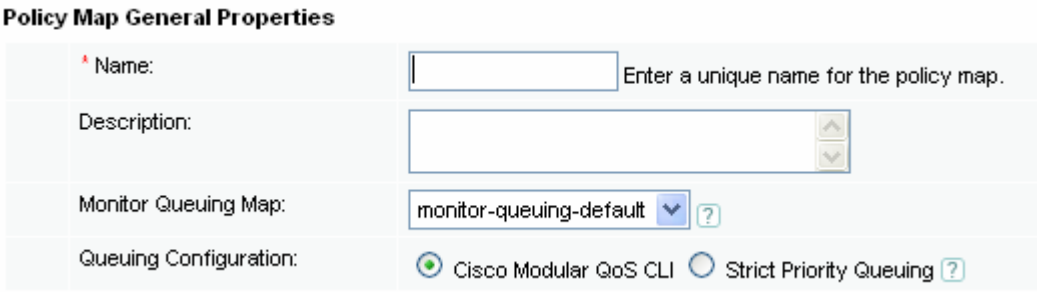
Table 2-6 Policy Map Page

Column	Description
Name	Displays the name of the policy-map.
Number of Classes	Displays the number of classes in the policy-map.
Monitor-queuing-map	Displays the name of the monitor-queuing-map being used by the policy-map.
Interfaces Using Policy Map	Displays the number of interfaces to which the policy-map is applied.
Actions	**edit** – click the link to edit the policy-map configuration. **duplicate** – click the link to duplicate the policy-map configuration in a new policy-map. **delete** – click the link to delete the policy-map.

Note Policy-maps that are already assigned to an interface cannot be deleted. You must delete the relevant interface(s) first before deleting the policy-map.

When editing a policy-map, all changes must be valid for all interfaces to which the policy-map is assigned. If not, a message is displayed indicating the problem and the relevant interface(s).

Figure 2-17: Policy Map Configuration



Configuring a Single-Class Policy Map

To define a single-class policy-map to model a first-in first-out (FIFO) queue, you do the following:

Step 1 Click **Add New Policy Map**.

Step 2 Enter a unique name for the policy-map in the **Name** field.

Step 3 Enter a brief text description for the policy-map in the **Description** field.

Step 4 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps.

Step 5 Click **Save**.

The new policy-map is saved and displayed on the **Policy Maps** page. The single class, class-default, is added to the policy-map automatically by the system.

Configuring a Multi-Class Policy Map

The system supports configuration of the following multi-class router queuing types:

- Strict priority queuing (PQ)
- Weighted fair queuing (WFQ)
- Low latency queuing (LLQ)

Choose one of the procedures in this section according to the type of queuing system on the router of interest that you are modeling in the policy-map.

Configuring a Strict Priority Queuing Policy Map

To define a multi-class policy-map to model strict priority queuing (PQ), you do the following:

Step 1 Click **Add New Policy Map**.

Step 2 Enter a unique name for the policy-map in the **Name** field.

Step 3 Enter a brief text description for the policy-map in the **Description** field.

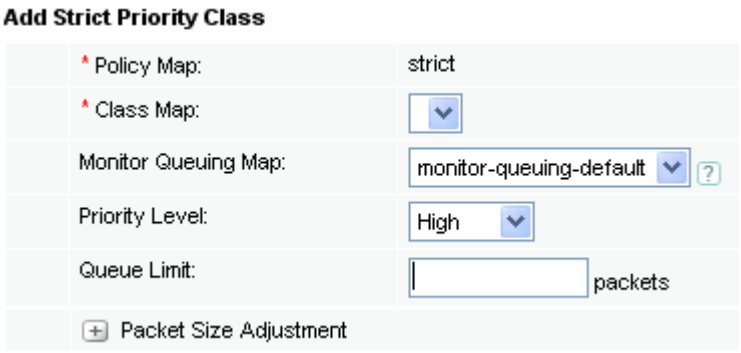
Step 4 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list contain only the default monitor-queuing-map. See the section "Configuring a Monitor-Queuing-Map" for more information on defining monitor-queuing-maps.

Step 5 Select **Strict Priority Queuing**.

Step 6 Click **Define Class**.

The **Add Class** page is displayed.

Figure 2-18: Configuring a Strict Priority Queuing Class



Step 7 Select a class-map from the list of previously configured class-maps. If you have not already configured any class-maps the list will contain only the default class-map. See the section "Configuring a Class Map" for more information on defining class-maps.

Step 8 If you are applying a monitor-queuing-map to the class, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section "Configuring a Monitor-Queuing-Map" for more information on defining monitor-queuing-maps.

Note If you do not define a class for a policy-map, the policy-map will comprise the default class, class-default, only. This default class cannot be deleted.

Step 9 Select a strict priority level for the class from the list: High, Medium, Low, Normal.

Note The following restrictions apply when using the **priority-level** command:

If multiple priority-level queues are defined then associated queue limit sizes with the Cisco defaults of 20, 40, 60 and 80 for high, medium, normal and low, respectively, are assumed, unless otherwise specified.

No more than a single instance of each priority-level queue is allowed in each policy-map; that is, a policy-map cannot have the same level appear twice in a policy-map.

Unless otherwise specified, the class-default in a policy-map is assumed to be associated with a normal priority queue.

Step 10 Enter a value in packets for the maximum allowable queue length for the class in the **Queue Limit** field.

Note The **Congestion Analysis** tab includes a **Corvil Bandwidth – Queue Length** graph based on the queue length limit you configure here. The Corvil Bandwidth values plotted represent the minimum bandwidth required to avoid packet loss due to queue buffer overflow. For example, if the queue length configured for the class is 64 packets, then the graph displays the bandwidth required to prevent the queue for the class traffic building up past 64 packets.

If you do not configure an explicit queue length limit, then the default value of 64 packets is used by the system when calculating the values plotted in the **Corvil Bandwidth – Queue Length** graph.

Step 11 To specify an optional packet size adjustment value in bytes for the class, select **Packet Size Adjustment** and enter a value in the following range: -2000 to +2000 bytes. By default, there is no packet size adjustment selected.

This value determines how much (in bytes) to adjust the size of a packet that matches the current class. Primarily used to correctly measure compressed RTP. This traffic is seen by the device as uncompressed but it subsequently gets compressed inside the router before being queued on an output interface. Specifying a value here allows for increased accuracy when calculating class measurements.

To specify an adjustment for compressed RTP, select **Packet Size Adjustment** and choose an option from the list.

Note udp-checksum - the default, corresponds to a byte adjustment value of -36.
no-udp-checksum - corresponds to a byte adjustment value of -38.

Step 12 Click **Save**.

Step 13 Repeat the steps for each class to be defined, noting the restrictions listed in Step 9. In particular, note that no two classes may be assigned the same priority level in the same policy-map.

Step 14 Click **Save**.

The **Policy Map** page is displayed. The new policy-map is listed on this page. The policy-map should now be available for selection when defining site router interfaces.

Configuring a Weighted Fair Queuing (WFQ) Policy Map

To define a multi-class policy-map to model weighted fair queuing (WFQ), you do the following:

Step 1 Click **Add New Policy Map**.

Step 2 Enter a unique name for the policy-map in the **Name** field.

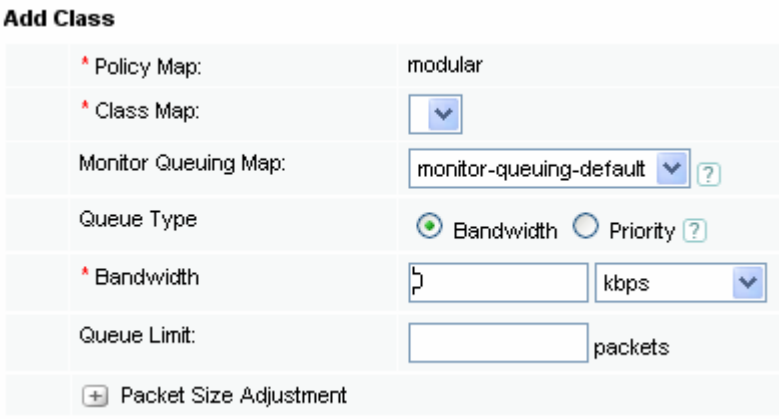
Step 3 Enter a brief text description for the policy-map in the **Description** field.

Step 4 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section "Configuring a Monitor-Queuing-Map" for more information on defining monitor-queuing-maps.

Step 5 Select **Cisco Modular QoS CLI**.

Step 6 Click **Define Class**.

Figure 2-19: Configuring a Cisco Modular QoS CLI Class



The **Add Class** page is displayed.

Step 7 Select a class-map from the list of previously configured class-maps. If you have not already configured any class-maps the list will contain only the default class-map. See the section "Configuring a Class Map" for more information on defining class-maps.

Step 8 If you are applying a monitor-queuing-map to the class, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section "Configuring a Monitor-Queuing-Map" for more information on defining monitor-queuing-maps.

Note If you do not define a class for a policy-map, the policy-map will comprise the default class, class-default, only. This default class cannot be deleted.

Step 9 Select queue type **Bandwidth**.

Step 10 Enter the bandwidth allocated for the class in the **Reserve Bandwidth** field.

You can specify reserved bandwidth in terms of kilobits per second, a remaining percentage, or a percentage.

Select **kbps** from the list to specify the amount of reserved bandwidth in kilobits per second to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use. If the link bandwidth is unknown or variable, class bandwidth settings in kbps should not be used. Range: 8 – 2000000 kbps

Select **remaining %** from the list to specify the amount of guaranteed bandwidth for the class, based on a relative percentage of available bandwidth. You use this option in cases where the link bandwidth is unknown or variable. In this case, the class bandwidths are always proportional to the specified percentages of the interface bandwidth. If the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. Range: 1 to 100%

Select **%** from the list to specify the amount of guaranteed bandwidth set aside for a priority class, based on an absolute percentage of available bandwidth. Range: 1 to 100%.

Note The weighted fair queuing (WFQ) scheduling system derives the weight for packets belonging to the class from the reserved bandwidth allocated to the class. The WFQ scheduler then uses the weight to ensure that the queue for the class is serviced fairly. You can specify bandwidth in kbps, or as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages.

The following restrictions apply when working with reserved bandwidth configuration:

- A given policy-map can have all the class bandwidths specified in kbps or all the class bandwidths specified in percentages but not a mix of both.
- The amount of reserved bandwidth configured should be large enough to also accommodate Layer 2 overhead.
- You cannot have 0% available on the link for use by a class. When the policy-map containing class configurations is attached to an interface to define the service policy for that interface, available bandwidth is assessed. If there is insufficient interface bandwidth, and the policy-map cannot be attached to a particular interface, then the policy is removed from all interfaces to which it was successfully attached.

Step 11 Enter a value in packets for the maximum allowable queue length for the class in the **Queue Limit** field.

Step 12 To specify an optional packet size adjustment value in bytes for the class, select **Packet Size Adjustment** and enter a value in the following range: -2000 to +2000 bytes. By default, there is no packet size adjustment selected.

This value determines how much (in bytes) to adjust the size of a packet that matches the current class. Primarily used to correctly measure compressed RTP. This traffic is seen by the device as uncompressed but it subsequently gets compressed inside the router before being queued on an output interface. Specifying a value here allows for increased accuracy when calculating class measurements.

To specify an adjustment for compressed RTP, select **Packet Size Adjustment** and choose an option from the list.

Note udp-checksum - the default, corresponds to a byte adjustment value of -36.
no-udp-checksum - corresponds to a byte adjustment value of -38.

Step 13 Click **Save**.

Step 14 Repeat the steps for each class to be defined, noting the restrictions listed in Step 10. In particular, note that all bandwidth classes must be defined in either kbps or as a percentage, but not as a mixture of both.

Step 15 Click **Save**.

The **Policy Map** page is displayed. The new policy-map is listed on this page. The policy-map should now be available for selection when defining site router interfaces.

Configuring a Low Latency Queuing (LLQ) Policy Map

To define a multi-class policy-map to model low latency queuing (LLQ), you do the following:

Step 1 Click **Add New Policy Map**.

Step 2 Enter a unique name for the policy-map in the **Name** field.

Step 3 Enter a brief text description for the policy-map in the **Description** field.

Step 4 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps.

Step 5 Select **Cisco Modular QoS CLI**.

Step 6 Click **Define Class**.

The **Add Class** page is displayed.

Step 7 Select a class-map from the list of previously configured class-maps. If you have not already configured any class-maps the list will contain only the default class-map. See the section “Configuring a Class Map” for more information on defining class-maps.

Step 8 If you are applying a monitor-queuing-map to the class, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps.

Note If you do not define a class for a policy-map, the policy-map will comprise the default class, class-default, only. This default class cannot be deleted.

Step 9 Select queue type **Priority**.

When you are defining classes in a policy-map for low latency queuing, you assign one of the classes (and one only) to be the priority class in the multi-class system using the **Priority** option. The remaining classes are defined as bandwidth classes using the **Bandwidth** option.

Step 10 Enter a reserved bandwidth value for the priority class in the **Reserve Bandwidth** field. If you are defining a priority class, you can specify reserved bandwidth in kilobits per second, or as a percentage.

Select **kbps** from the list to specify the guaranteed allowed bandwidth, in kbps, for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Range: 8 – 2000000 kbps

Select **%** from the list to specify the amount of guaranteed bandwidth available to the priority class. The percentage can be a number from 1 to 100. Range: 1 – 100%

Specify an optional burst size in bytes to accommodate temporary bursts of traffic. The default burst value, which is computed as 250 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. Range: 32 to 2000000 bytes.

Note The LLQ scheduling system allows packets in the low-latency queue that conform to the configured reserved bandwidth and burst-size to be prioritized over packets in other queues. This allows delay-sensitive data such as voice to be sent before packets in other queues. The units you specify for the priority class can be different from the bandwidth unit of the non-priority class(es) in the policy-map.

The LLQ reserve bandwidth and burst size is used to configure a policer on the LLQ class, preventing misbehaving priority traffic from starving low-priority traffic. Policing is a traffic regulation method used on Cisco IOS routers. Traffic policing allows you to control the maximum rate of traffic sent or received on an interface. The traffic policing feature on routers manages the maximum rate of traffic through a token bucket algorithm. The token bucket algorithm can use the user-configured values to determine the maximum rate of traffic allowed on an interface at a given moment in time. The token bucket algorithm is affected by all traffic entering or leaving (depending on where the traffic policy with traffic policing configured) and is useful in managing network bandwidth in cases where several large packets are sent in the same traffic stream.

Step 12 To specify an optional packet size adjustment value in bytes for the class, select **Packet Size Adjustment** and enter a value in the following range: -2000 to +2000 bytes. By default, there is no packet size adjustment selected.

This value determines how much (in bytes) to adjust the size of a packet that matches the current class. Primarily used to correctly measure compressed RTP. This traffic is seen by the device as uncompressed but it subsequently gets compressed inside the router before being

queued on an output interface. Specifying a value here allows for increased accuracy when calculating class measurements.

To specify an adjustment for compressed RTP, select **Packet Size Adjustment** and choose an option from the list.

Note udp-checksum - the default, corresponds to a byte adjustment value of -36.
no-udp-checksum - corresponds to a byte adjustment value of -38.

Step 14 Click **Save**.

Step 15 Having defined the priority class in the LLQ system, perform the steps for configuring a weighted fair queuing policy-maps for each remaining bandwidth class. See the section "Configuring a Weighted Fair Queuing Policy Map" for more information.

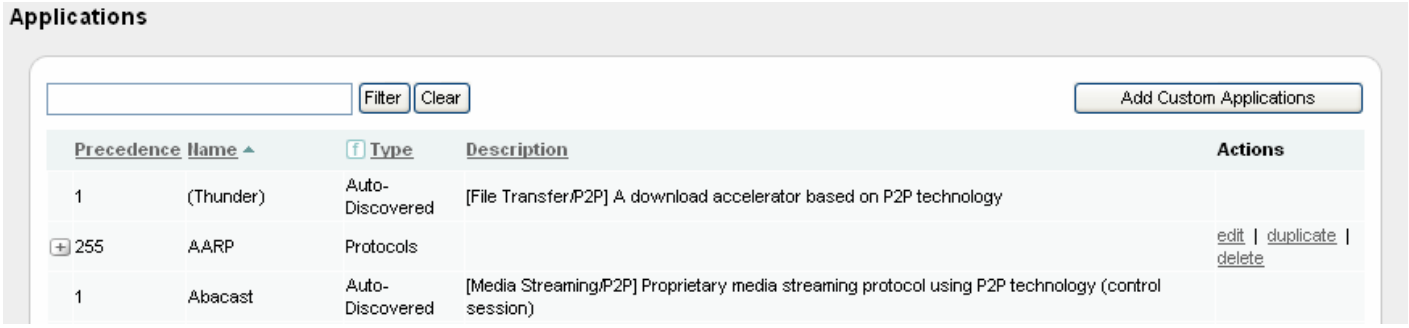
Step 16 Click **Save**.

The **Policy Map** page is displayed. The new policy-map is listed on this page. The policy-map should now be available for selection when defining site router interfaces.

Configuring Custom Applications

You can define custom applications in the GUI from the **Applications** page in the **Configuration** tab.

Figure 2-20: Custom Applications

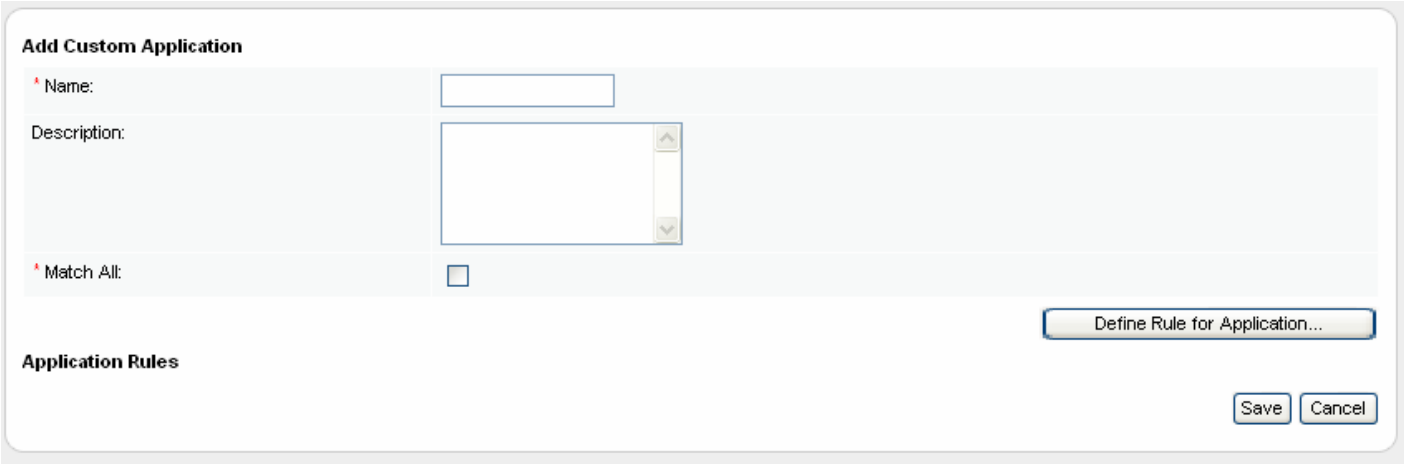


The **Applications** page displays the current list of auto-discovered and configured custom applications in the system. The following table describes the information displayed on the page:

Table 2-7 Applications Page

Column	Description
Precedence	Displays the precedence of the application. This value is editable for custom applications only. Setting a precedence value for a custom application enables you to specify which custom application takes precedence should a given network flow match the rules for more than one custom application.
Name	Displays the name of the application.
Type	Displays the type of application: Auto-discovered – one of the set of applications automatically discovered by the system. Protocol – predefined non-TCP or UDP protocol. Custom – user-defined application.
Description	Displays the description entered for the application (if any).
Actions	edit – click to edit custom application details duplicate – click to duplicate the details of the selected custom application delete – click to delete the custom application NOTE: Edit, duplicate and delete actions cannot be performed on auto-discovered applications.

Figure 2-21: Defining a Custom Application



To define a custom application, you do the following:

Step 1 Click **Add Custom Application**.

Step 2 Enter a unique name for the custom application in the **Name** field.

Note If you configure a custom application with the same name as a predefined application on the system, the custom application takes precedence.

Step 3 Enter a brief text description for the custom application in the **Description** field.

Step 4 To specify that all defined match rules must be satisfied before traffic is classed as being part of this custom application, check the **Match All** check box. If you leave the check box unchecked, then you are effectively specifying that traffic is identified as part of the custom application if ANY of the match rules are met.

Figure 2-22: Defining a Custom Application Match Rule

Step 5 To define match rules for the custom application, click **Define Rule for Application**.

Step 6 To add match rules for **TCP/UDP** source and destination addresses and ports, then select and fill out the source and destination port and address fields as required.

Step 7 To add advanced match rules, select TOS, Protocol or Applications from the **Advanced** panel, and then select or enter the required values as appropriate.

Step 8 Click **Save**.

Step 9 When you have defined and saved the match rules, click **Save**.

The new custom application is saved and displayed on the **Applications** page. The custom application is available to select when defining class-maps that match applications.

Configuring Sites, Routers, and Interfaces

You can define sites and associated routers and interfaces in the GUI from the **Sites/Interfaces** page in the **Configuration** tab. The **Sites/Interfaces** page displays information about the default local site and the current list of configured remote sites in the system. The following table describes the information displayed on the page for the local site and for configured remote sites:

Figure 2-23: Site Configuration

Table 2-8: Sites/Interfaces Page

Column	Description
Name	Displays the name of the site.
Router(s)	Displays the name of a single router or the number of routers configured for the site. To see a list of router names configured for the site, expand the site details
Interface(s)	Displays the name of a single interface or the number of interfaces configured for the site. To see a list of interface names configured for the site, expand the site details. The information icon is displayed if a filter class (defined using the CLI) is being applied to a remote site interface. Roll over the icon to see the name of the configured filter class. For more information on filter classes, see the section "Using Filter Classes" in the chapter "Using the Command Line Interface (CLI)."
Policy Map(s)	Displays the name of a single policy-map or the number of policy-maps configured for the site. To see a list of policy-map names configured for the site, expand the site details.
Subnet(s)	Displays the address of a single subnet or the number of subnets configured for the site. To see a list of subnet addresses configured for the site, expand the site

	details.
Ping Address	Displays the configured ICMP responder address for the site.
Actions	**edit** – click to display the site details for editing. **delete** – click to delete a site (Remote sites only.) **duplicate** – click to copy site details to a new site (Remote sites only.)

Editing the Local Site

The system automatically creates a default local site. When you open the **Sites/Interfaces** page on the **Configuration** tab the details of the default local site are displayed. You can change the default configuration of the local site by editing it.

Note The default local site cannot be deleted.

Figure 2-24: Editing the Local Site

To edit the default local site configuration, you do the following:

Step 1 Click the named local site link or the **edit** link.

Step 2 The **Edit Local Site** page is displayed.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix in the **Subnet** field.

Note LAN subnets of the local site are only required if the appliance will receive traffic from these subnets that is not destined for the WAN.

Step 5 To configure a router for the local site, click **Define Router**. Alternatively, to save the site without configuring a router, click **Update Site**.

.

Configuring a Local Site Router

As part of the configuring the network model, you configure at least one router for the local site. You define routers in the GUI from the **Edit Sites/Interfaces** page. The **Edit Sites/Interfaces** page displays information about the default local site configuration and the current list of configured routers for the local site.

The following table describes the information displayed on the page for the local site routers:

Table 2-9: Edit Local Site - Routers Page

Column	Description
Name	Displays the name of the router.
Monitored by Physical Port	Displays the physical BQM ports that are configured to measure traffic from the router being represented in the model.
Interface(s)	Displays the number of interfaces configured for the router. To see a list of interface names configured for the router, expand the router details.
Policy Map(s)	Displays the number of policy-maps configured for the router. To see a list of policy-map names configured for the router, expand the router details.
Actions	**edit** – click to display the router details for editing. **delete** – click to delete a router **duplicate** – click to copy router details to a new router.

Figure 2-25: Defining a Local Site Router

To add a router to the local site, you do the following:

Step 1 From the **Edit Sites/Interfaces** screen, click **Define Router**.

Step 2 Enter a name in the **Router Name** field.

Step 3 Enter a brief description in the **Router Description** field.

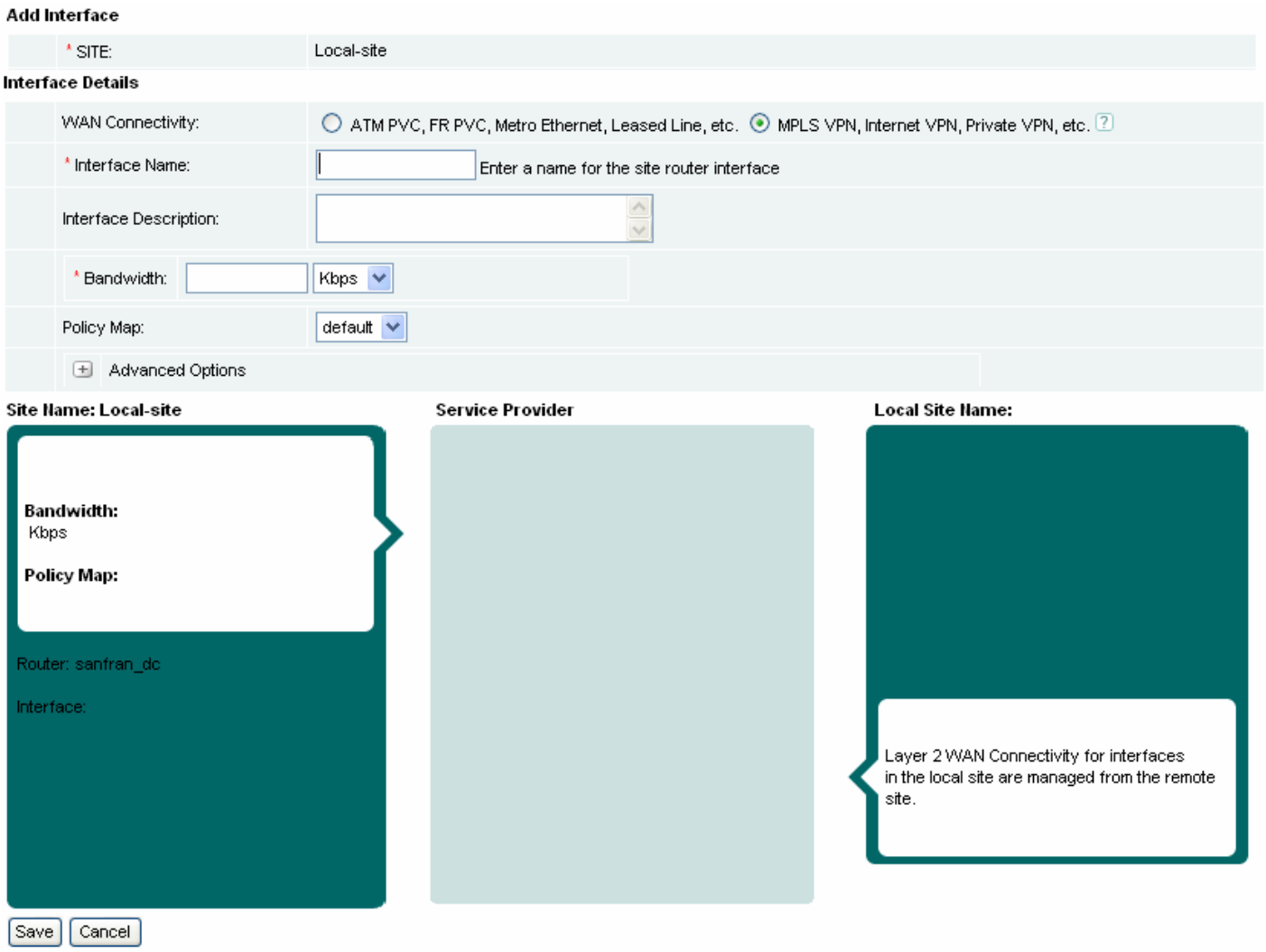
Step 4 Check each of the BQM physical ports from the **Physical Ports Monitoring this Router** field that are being used to measure traffic for this router.

Step 5 To configure an interface for the router, click **Define Interface**. Alternatively, to save the router without configuring an interface, click **Save**.

Configuring a Local Site Router Interface

The next task is to configure the router interface(s). As part of the configuring the network model, you configure at least one interface for the local site router. You define router interfaces in the GUI from the **Define Routers** page.

Figure 2-26: Defining a Local Router Interface



The **Define Routers** page displays information about the local site router configuration and the current list of configured interfaces for the router.

The following table describes the information displayed on the page for the router interfaces:

Table 2-10: Local Site – Define Routers Page

Column	Description
Name	Displays the name of the interface.
WAN Connectivity	Displays the WAN Connectivity type configured for the interface – ATM PVC, FR PVC, Metro Ethernet, Leased line, or MPLS VPN, Internet VPN, Private VPN, depending on the deployment being configured.
Bandwidth	Displays the configured bandwidth size of the link.
Outbound Policy Map	Displays the name of the policy-map configured for the outbound direction of the interface.
Actions	edit – click to display the interface details for editing. delete – click to delete an interface.

To add an interface to a site router, you do the following:

Step 1 Click **Define Interface**.

Step 2 Select the **Connectivity** type relevant to the deployment.

Note For more information on deployment types, see the chapter "Configuring Network Deployments."

Step 3 Enter a name in the **Interface Name** field.

Step 4 Enter a brief description in the **Description** field.

Step 5 Enter a link bandwidth for the interface in kbps or Mbps in the **Bandwidth** field.

Step 6 Select a policy-map for the interface from the **Policy Map** list.

If you have not configured any policy-maps, only the default policy-map will be displayed in the list.

Note For more information on configuring advanced options for an interface, see the section "Configuring Advanced Interface Settings."

Step 7 If you have selected a WAN Connectivity type of **MPLS VPN, Internet VPN, Private VPN** check that the displayed peer-interface details are correct and make any necessary adjustments. For example, if you want to apply a different policy-map to the peer-interface, you choose it from the list.

Step 8 Click **Save**.

The **Router** page is displayed.

Step 9 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

Step 10 Click **Save**.

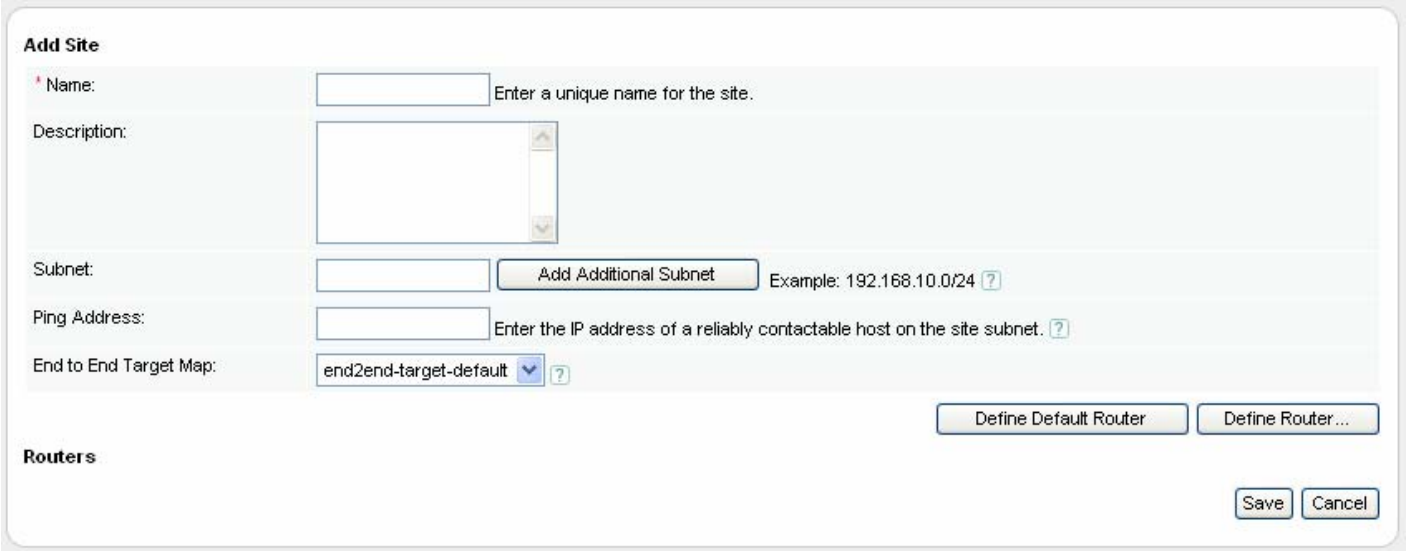
The new local site configuration is saved and the **Sites/Interfaces** page is displayed.

Configuring a New Remote Site

In summary, the following tasks are involved in configuring a new remote site:

1. Create the new site with a unique name, a subnet address, and an ICMP responder address for end-to-end measurements.
2. Define a router for the site.
3. Define the router interface(s) and attach a predefined traffic policy (policy-map).
4. For point-to-point deployments, specify the local site router interface to which the configured remote site interface is connected. For MPLS deployments, specify the Service Provider peer-interface to which the configured remote site interface is connected.

Figure 2-27: Remote Site Configuration



The following steps describe how to configure a new remote site:

Step 1 In **System Administration** mode, click the **Configuration** tab, click **Sites/Interfaces** and click **Define Remote Site**.

Step 2 Enter a unique name in the **Name** field.

Step 3 Enter a brief description of the site in the **Description** field.

Step 4 Enter the IP address of a reliably contactable host on the site subnet in the **Ping Address** field. This address provides the target address for end-to-end measurements to/from this site.

Step 5 Enter the site subnet address and prefix in the **Subnet** field.

Note The subnet address you configure here is used as a match rule to classify traffic. Packets with a source address matching the subnet address are identified as outbound traffic leaving the site; packets with a destination address matching the subnet are identified as inbound traffic to the site.

Any additional packet matching rules that you apply to site router interfaces in policy-maps are logically ANDed together with the subnet address to determine the packets that are matched.

If you are editing the default remote site named Unmatched Traffic or if you have used the CLI to define a subnet using the **subnet unmatched-remote** command, there is an **Unmatched remote** check box displayed here. This indicates that the remote site is currently configured as

a catch-all site that will measure traffic that does not get matched by other remote site subnets. Clicking the check box removes the definition.

Step 6 Select a previously defined end-to-end queuing map from the **End to End Map** list. If you have not already configured any end-to-end queuing maps, only the end-to-end queuing map will be displayed.

Step 7 To configure a router for the site, click **Define Router**. Alternatively, to save the site without configuring a router, click **Save**.

Note If no router has previously been defined for the remote site, you have the option of clicking **Define Default Router**. This creates a router named default and displays the **Add Interface** screen.

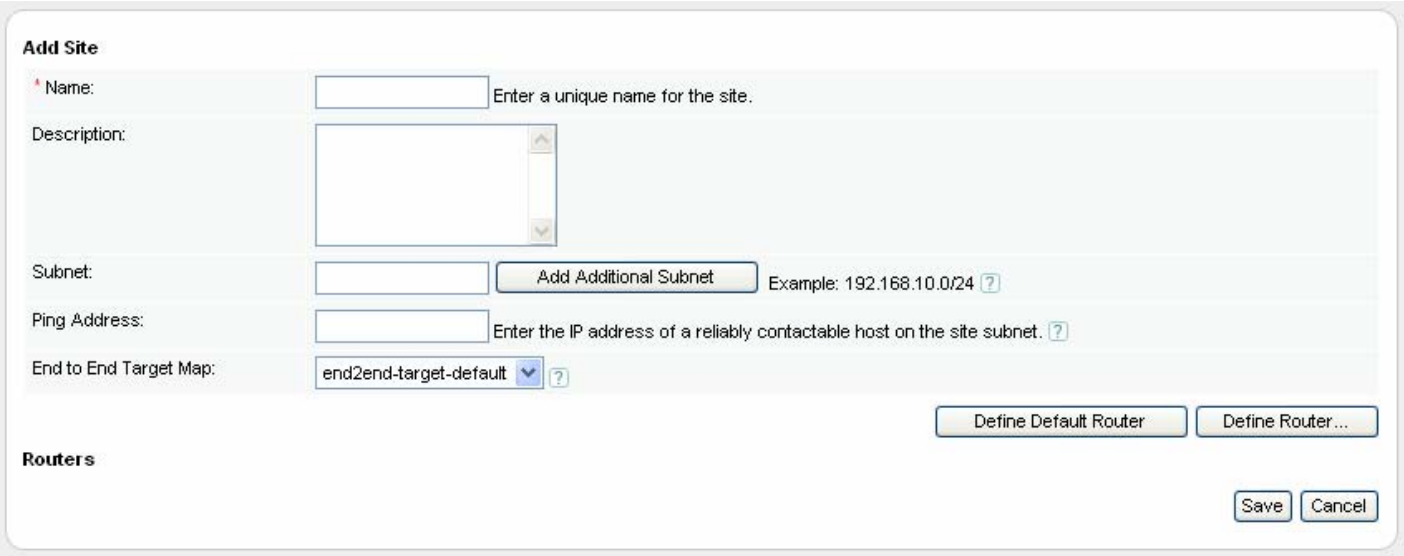
Configuring a Remote Site Router

As part of configuring the network model, you configure at least one router for a remote site. You define routers in the GUI from the **Add Sites/Interfaces** page. The **Add Sites/Interfaces** page displays fields to configure the remote site and also the current list of configured routers for the remote site. The following table describes the information displayed on the page for the remote site routers:

Table 2-11: Remote Site - Routers Page

Column	Description
Name	Displays the name of the router.
Description	Displays the description (if any) entered for the router.
Interface(s)	Displays the number of interfaces configured for the router. To see a list of interface names configured for the router, expand the router details.
Policy Map(s)	Displays the number of policy-maps configured for the router. To see a list of policy-map names configured for the router, expand the router details.
Actions	**edit** – click to display the router details for editing. **delete** – click to delete a router **duplicate** – click to copy router details to a new router.

Figure 2-28: Remote Site Router Configuration



To add a router to a site, you do the following:

Step 1 From the **Add Site** screen, click **Define Router**.

The **Add Router** page is displayed.

Step 2 Enter a name in the **Router Name** field.

Step 3 Enter a brief description in the **Router Description** field.

Step 4 To configure an interface for the router, click **Define Interface**. Alternatively, to save the router without configuring an interface, click **Save**.

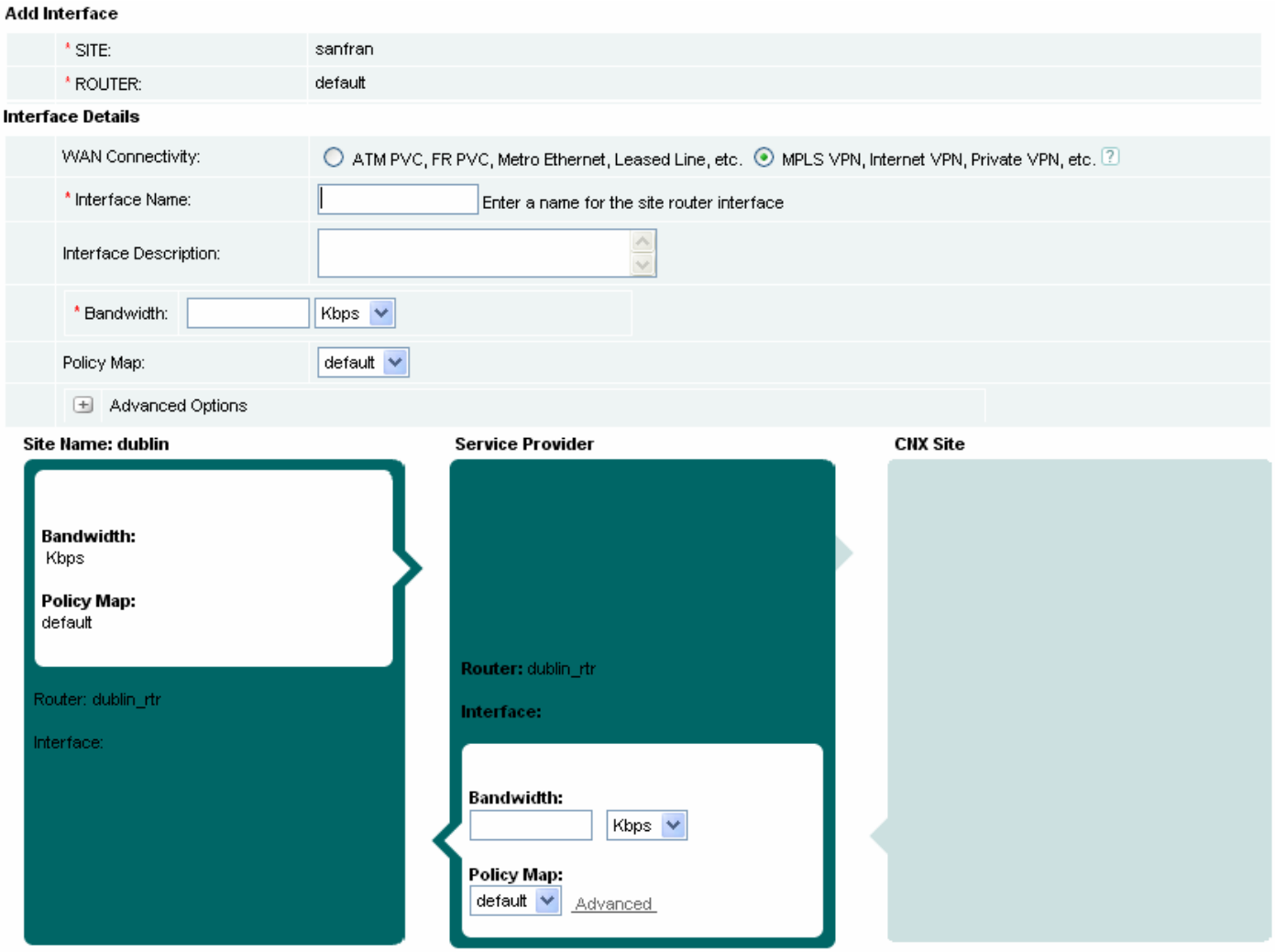
Configuring a Remote Site Router Interface

The next task is to configure the router interface(s). As part of the configuring the network model, you configure at least one interface for a remote site router. You define router interfaces in the GUI from the **Add Routers** page. The **Add Routers** page displays information about the local site router configuration and the current list of configured interfaces for the router. The following table describes the information displayed on the page for the router interfaces:

Table 2-12: Remote Site – Define Routers Page

Column	Description
Name	Displays the name of the interface.
WAN Connectivity	Displays the WAN Connectivity type configured for the interface – **ATM PVC, FR PVC, Metro Ethernet, Leased line**, or **MPLS VPN, Internet VPN, Private VPN**, depending on the deployment being configured.
Bandwidth	Displays the configured bandwidth size of the link.
Outbound Policy Map	Displays the name of the policy-map configured for the outbound direction of the interface.
Actions	**edit** – click to display the interface details for editing. **delete** – click to delete an interface. **duplicate** – click to copy interface details to a new interface.

Figure 2-29: Remote Site Interface Configuration



To add an interface to a site router, you do the following:

Step 1 Click **Add Interface**.

Step 2 Select the **Connectivity** type relevant to the deployment.

Step 3 Enter a name in the **Interface Name** field.

Step 4 Enter a brief description in the **Description** field.

Step 5 Enter a link bandwidth for the interface in kbps or Mbps in the **Bandwidth** field.

Step 6 Select a policy-map for the interface from the **Policy Map** list.

If you have not configured any policy-maps, there will be no policy-maps displayed in the list.

Note For more information on configuring advanced options for an interface, see the section "Configuring Advanced Interface Settings."

Step 7 If you have selected **ATM PVC…** as the **Connectivity** type, first, select the local router on the diagram. If a new router is to be configured on the local site, then click **Add Router**, fill in the router name and description then click **Save**. The list of local routers is updated. Select local interface that the remote interface connects to. If a new interface is to be configured on local router selected, then click **Add interface**. Enter the interface name, description, bandwidth details and select the policy map, then click **Save**. The newly created local interface will appear in the list of local interfaces to connect to. A given local interface can only be connected to one remote interface.

If you have selected **MPLS VPN…** as the **WAN Connectivity** type, check the bandwidth value and select a policy-map for the peer-interface to which this local site interface connects. Peer-interfaces on the local site cannot be connected to remote interfaces.

Note For more information on deployment types, see the chapter "Configuring Network Deployments."

Step 8 Click **Save**.

The **Router** page is displayed.

Step 9 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

Step 10 Click **Save**.

The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.

Configuring Advanced Interface Settings

There are a number of advanced settings available when configuring interfaces. The following section describes the router features that can be modeled by the system, how to configure them, and how to make adjustments for layer 2 packet overhead.

Max Reserved Bandwidth

Maximum Reserved Bandwidth is a Cisco concept. The sum of all bandwidth allocation on an interface using a policy-map cannot exceed 75 percent of the total available interface bandwidth (default setting for Maximum Reserved Bandwidth). The remaining 25 percent is used for other overhead, including Layer 2 overhead, routing traffic, and best-effort traffic. Bandwidth for the default class, for instance, is taken from the remaining 25 percent.

However, under aggressive circumstances in which you want to configure more than 75 percent of the interface bandwidth to classes, you can override the 75 percent maximum sum allocated to all classes or traffic using the Cisco max-reserved-bandwidth command on a router. If you want to override the default 75 percent, exercise caution and ensure that you allow enough remaining bandwidth to support best-effort and control traffic, and Layer 2 overhead.

Link Fragmentation and Interleaving (LFI)

Priority network traffic, such as VoIP packets, can suffer long delays due to the time taken to serialize large packets onto slow links. For example, on a 56 kbps serial line, it takes over 200 ms to serialize a 1500-byte packet. A recommended end-to-end delay for VoIP packets is just 150 ms. To solve this problem it is necessary to use packet fragmentation mechanisms such as Cisco's Link Fragmentation and Interleaving (LFI). The system models LFI scheduling. Fragmenting large data packets into smaller ones and interleaving voice packets among the fragments reduces jitter and delay.

The configured LFI value represents the maximum tolerable delay to be incurred by fragmented packets. The packet fragment size for fragmenting classes is based on the required delay.

Cisco recommends fragmenting data packets to sizes that incur no more than a 10-millisecond delay.

LFI configuration is typically only applied to links less than dedicated half-T1 (768 kbps).

Although you can enable LFI for a WFQ or FIFO (single-class WFQ) scheduler, no fragmentation or interleaving actually occurs. Therefore the Corvil Bandwidth value calculated will not change with LFI enabled on an interface with either WFQ or FIFO schedulers enabled.

For voice applications, the recommended serialization delay on a per-hop basis is 10 ms and should not exceed 20 ms.

Layer 2 Overhead

The BQM by default processes and bases calculations on layer 3 packet sizes only. That is, only the IP packet size is counted. However, this behavior can be adjusted, allowing for increased accuracy when calculating results. For example, on a HDLC Serial line, the adjustment can be made when calculating the correct number of bytes to allow for the layer 2 HDLC link layer headers when totaling the number of bytes in the packet versus the number of bytes due to an IP payload.

For example, if the BQM is monitoring an Ethernet link on the far side of a router that has both Ethernet and Serial interfaces. To compensate for the difference between the actual layer 2 frame size and the layer 3 packet size counted by the BQM, you make a layer 2 overhead adjustment.

The adjustment value can be positive or negative. For example, wanting to include an MPLS label in bandwidth calculations which has already been allowed for by the code, requires an adjustment value of minus four (- 4).

To configure advanced settings for an interface, you do the following:

Step 1 Expand the **Advanced Options**.

Step 2 To modify the maximum reserved bandwidth value, enter a new value in the **Max Reserved Bandwidth** field.

Step 3 To enable link fragmentation and interleaving, check the **Link Fragmentation Interleaving** check box and enter a millisecond value in the field.

Step 4 To account for layer 2 or tunneling overhead, check the **Layer 2 or Tunneling Overhead** check box and enter a byte value in the field.

Step 5 When you have completed the interface configuration, click **Save**.

The interface configuration is saved and the **Router** page is displayed.

Editing a Remote Site

To edit a remote site, you do the following:

Step 1 Click the **Edit** link beside the chosen site.

Step 2 Make the required changes to the remote site details.

Step 3 Click **Save**.

Note Note the following recommendations when making changes to remote site subnet definitions:

- adding to the range of subnets: no action required.
- reducing the range of subnets: delete the site and recreate it.
- reconfiguring due to misconfiguration: delete the site and recreate it.

The new details are saved and the Sites/Interfaces page is displayed.

Deleting a Remote Site

To delete a remote site, you do the following:

Step 1 Click the **Delete** link beside the chosen site.

Step 2 Click **OK** to confirm the site deletion.

The remote site is deleted from the system and the **Sites/Interfaces** page is displayed. All related interface Traffic Insight, Congestion Analysis, Bandwidth Sizing and Alarms information that was previously displayed for the site is no longer available in the system. If you restore a previous configuration with the same remote site now reincluded, the related historical information is still not available.

Note If you attempt to delete a site for which a manual packet capture is configured, you will get an error message indicating the affected site interface. You use the BQM CLI to remove the packet capture instance from the interface before attempting to delete the site.

3 Configuring Network Deployments

Overview

This chapter describes how to take knowledge of the existing network design, which the BQM is used to monitor and troubleshoot, and configure the appropriate deployment of the product network model. You need to decide which of the deployment models presented in this chapter most accurately captures the network configuration you are monitoring. There are different types of network model deployment which also then vary in complexity (usually given dual homing or failover configurations).

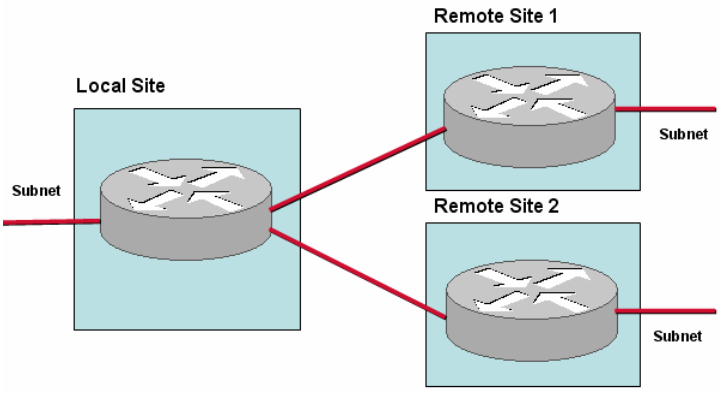
The basic network model deployments are

- ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line
- MPLS VPN, Internet VPN, Private VPN

Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM.

Figure 3-1 Network Model - Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment



To configure the network model for this example deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is not editable
  - Subnet
  - Router
  - Two interfaces specifying bandwidth configuration and policy-maps
- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Interface with link to local site-router-interface, bandwidth, policy-map

To configure the network model for this deployment from the GUI, the first task is to configure the monitor-queuing-map:

Step 1 In **System Administration** mode, click the **Configuration** tab, and then click **Queuing Maps**.

Step 2 Click **Define Monitor Queuing Map**.

Step 3 Enable and configure the required features and thresholds. In this example configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified.

Step 4 Click **Save**.

The next task is to configure a monitor-end-to-end-map. To define a monitor-end-to-end-map, you do the following:

Step 1 Click the **End to End Maps** menu and click **Add End to End Map**.

Step 2 Enter a unique name for the monitor-end-to-end-map in the **Name** field.

Step 3 Enter a brief text description for the monitor-end-to-end-map in the **Description** field.

Step 4 To configure the ping packet interval, enter a value in milliseconds in the **Interval** field.

Step 5 To configure the ping packet size, enter a value in bytes in the **Packet Size** field.

Step 6 To establish the number of pings that must be lost before a site is considered unavailable, enter a value in the **Availability Threshold** field.

Step 7 To enable event detection and set an event detection threshold based on measured end-to-end packet delay, enter a delay value in milliseconds in the **Trigger Delay events above** field.

Step 8 To enable event detection if any end-to-end packet loss is detected, check the **Trigger event for any Packet Loss** check box.

Step 9 Click **Save**.

The monitor-end-to-end-map is available to choose when defining remote sites.

The next task is to define the policy-map for the configuration. In this example, the single-class FIFO policy-map is configured, comprising only the default class, named class-default, and the monitor-queuing-map configured above is used:

Step 1 Click **Policy Maps**.

Step 2 Click **Add New Policy Map**.

Step 3 Enter a unique name for the policy-map in the **Name** field.

Step 4 Enter a brief text description for the policy-map in the **Description** field.

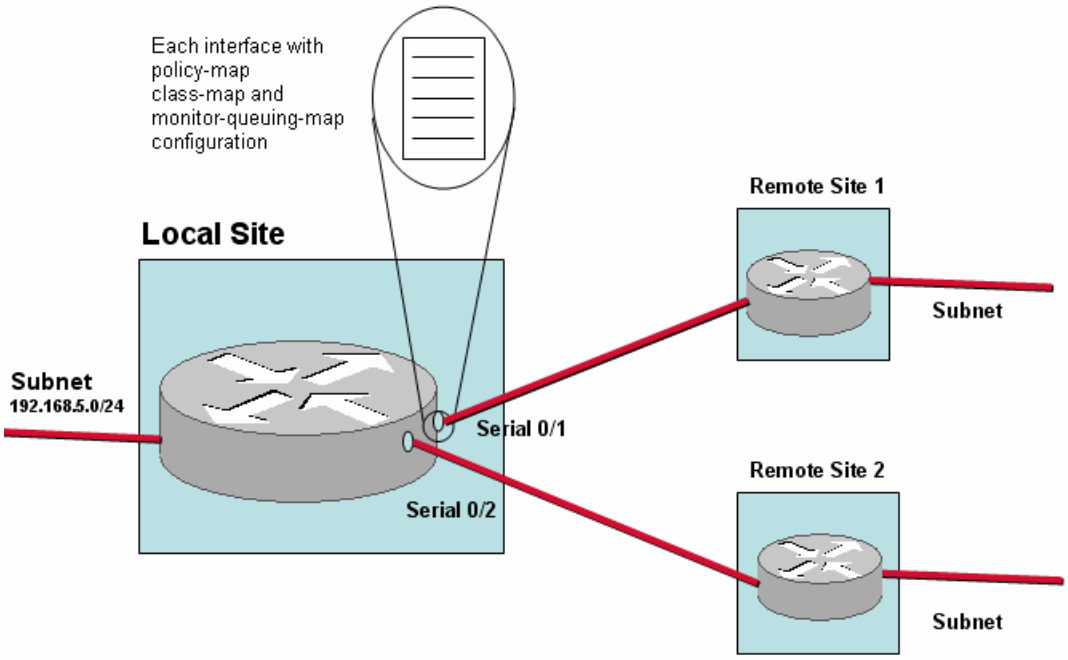
Step 5 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps.

Step 6 Click **Save**.

The new policy-map is saved and displayed on the **Policy Maps** page. The single class, class-default, is added to the policy-map automatically by the system.

The next task is to define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has two interfaces, Serial0/1 and Serial0/2, with both connected to links of 512 kbps and both using the FIFO policy-map:

Figure 3-2 Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Local Site Configuration



Step 1 Click the named local site link or the **edit** link.

Step 2 The **Edit Local Site** page is displayed.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix in the **Subnet** field.

Step 6 To configure a router for the local site, click **Define Router**.

Step 7 Enter a name in the **Router Name** field.

Step 8 Enter a brief description in the **Router Description** field.

Step 9 Check each of the BQM physical ports from the **Physical Ports Monitoring this Router** field that are being used to measure traffic for this router.

Step 10 To configure an interface for the router, click **Define Interface**.

Step 11 Selected **ATM PVC…** as the **WAN Connectivity** type.

Step 12 Enter a name in the **Interface Name** field, in this example Serial0/1.

Step 13 Enter a brief description in the **Description** field.

Step 14 Enter the link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.

Step 15 Select the FIFO policy-map for the interface from the **Policy Map** list.

Step 16 Click **Save**.

The **Router** page is displayed.

Step 17 Repeat Steps 10 to 16 to add the second interface, in this example Serial0/2.

Step 18 Click **Save**.

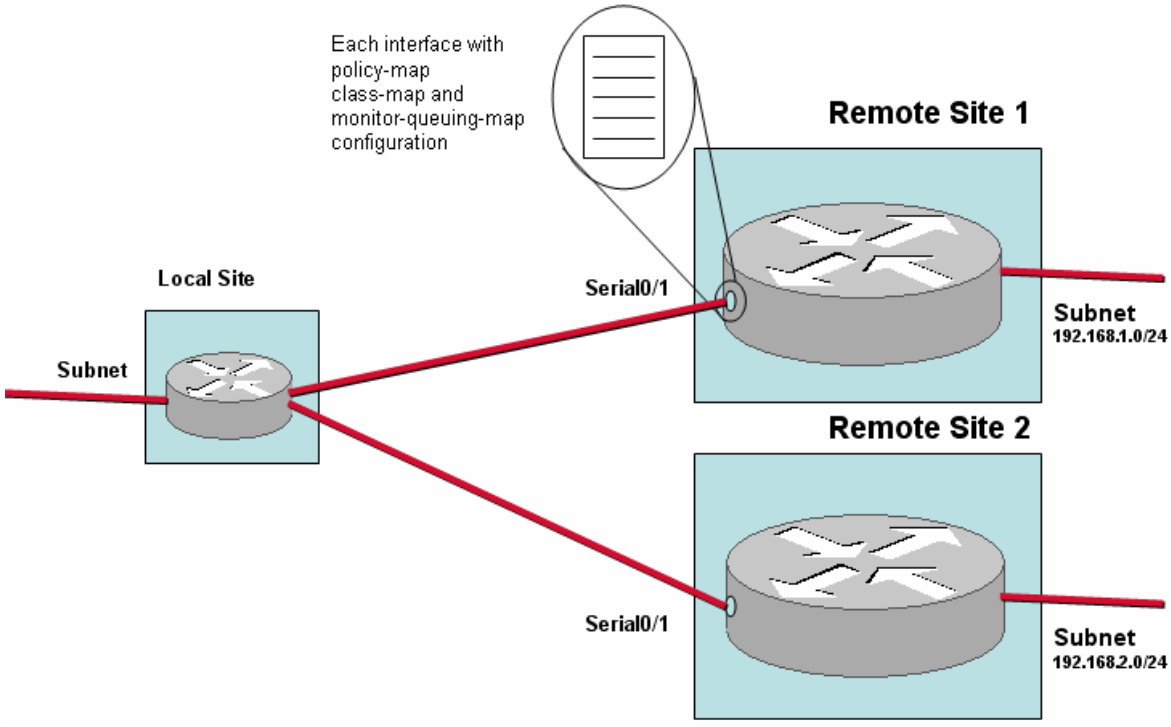
The **Edit Sites/Interfaces** page is displayed.

Step 19 Click **Save**.

The new local site configuration is saved and the **Sites/Interfaces** page is displayed.

The next task is to define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, whose interface connections back to each local site interface is made explicit when defining the interfaces:

Figure 3-3 Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Remote Site Configuration



Step 1 Click **Define Remote Site**.

Step 2 Enter a unique name in the **Site Name** field.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix, in this example 192.168.1.0/24, in the **Subnet** field.

Step 5 Enter the IP address of a reliably contactable host on the site subnet in the **Ping Address** field.

Step 6 Select a previously defined end-to-end queuing map from the **End to End Map** list. If you have not already configured any end-to-end queuing maps, the list will contain only the default end-to-end map.

Step 7 Click **Define Router**.

The **Add Router** page is displayed.

Step 8 Enter a name in the **Router Name** field, in this example remote1.

Step 9 Enter a brief description in the **Router Description** field.

Step 10 To configure an interface for the router, click **Define Interface**.

Step 11 Select **ATM PVC…** as the **WAN Connectivity** type, enter a bandwidth value (512 kbps) and select a policy-map (FIFO) for the local site interface (Serial0/1) to which this remote site interface connects.

Step 12 Enter a name in the **Interface Name** field, in this example Serial0/1.

Step 13 Enter a brief description in the **Description** field.

Step 14 Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.

Step 15 Select the FIFO policy-map for the interface from the **Policy Map** list.

Note For more information on configuring advanced options for an interface, see the section "Configuring Advanced Interface Settings."

Step 16 Click **Save**.

The **Router** page is displayed.

Step 17 Click **Save**

The **Edit Sites/Interfaces** page is displayed.

Step 18 Click **Save**.

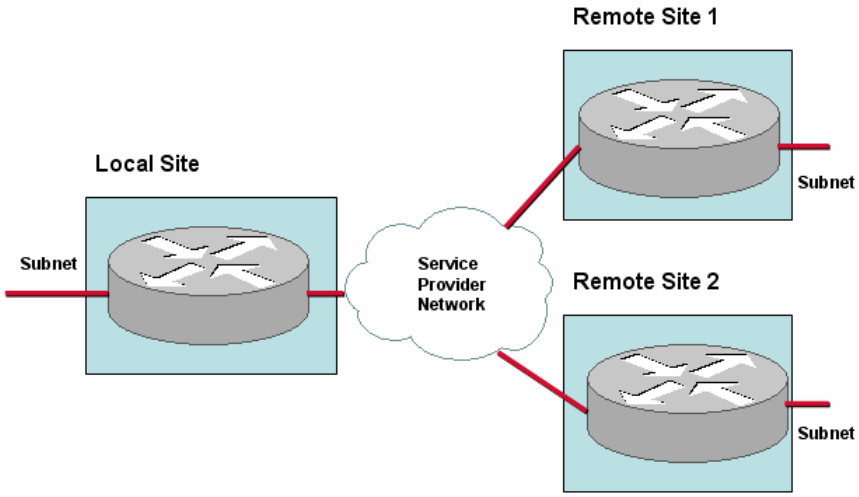
The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.

Step 19 Repeat this task from Step 1 to Step 19 to add the second remote site. Note that when defining interface connectivity for the second remote site router that in this example the second remote site router interface connects to local site interface Serial0/2.

Basic MPLS VPN, Internet VPN, Private VPN Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM and so all measurements are made from the perspective of the local site. At least one local site WAN link must be configured with the correct aggregate link bandwidth speed. Ideally you use the Service Provider Network policy-map for the remote site QoS policies. These polices can be modeled on the Service Provider Network, or less ideally the inbound direction of the remote site interfaces.

Figure 3-4 Network Model – Basic MPLS VPN, Internet VPN, Private VPN Deployment



To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is not editable
  - Subnet
  - Router
  - Local site interface/SPN peer-interface pair with bandwidth configuration and policy-maps
- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

To configure the network model for this deployment from the GUI, the first task is to configure the monitor-queuing-map:

Step 1 In **System Administration** mode, click the **Configuration** tab, and then click **Queuing Maps**.

Step 2 Click **Define Monitor Queuing Map**.

Step 3 Enable and configure the required features and thresholds. In this example configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified.

The next task is to configure a monitor-end-to-end-map. To define a monitor-end-to-end-map, you do the following:

Step 1 Click the **End to End Maps** menu and click **Add End to End Map**.

Step 2 Enter a unique name for the monitor-end-to-end-map in the **Name** field.

Step 3 Enter a brief text description for the monitor-end-to-end-map in the **Description** field.

Step 4 To configure the ping packet interval, enter a value in milliseconds in the **Interval** field.

Step 5 To configure the ping packet size, enter a value in bytes in the **Packet Size** field.

Step 6 To establish the number of pings that must be lost before a site is considered unavailable, enter a value in the **Availability Threshold** field.

Step 7 To enable event detection and set an event detection threshold based on measured end-to-end packet delay, enter a delay value in milliseconds in the **Trigger Delay events above** field.

Step 8 To enable event detection if any end-to-end packet loss is detected, check the **Trigger event for any Packet Loss** check box.

Step 9 Click **Save**.

The monitor-end-to-end-map is available to choose when defining remote sites.

The next task is to define the class-maps for the configuration. In this example, there are the following class-maps:

```
class-map besteffort (match-any)
  match ip dscp=0
class-map bulk (match-any)
  match ip dscp=10
class-map critical (match-any)
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map realtime (match-any)
  match ip dscp=46
  match ip dscp=40
class-map video (match-any)
  match ip dscp=18
  match ip dscp=16
```

Step 1 Click **Class Maps**.

Step 2 Click **Add New Class Map**.

Step 3 Enter a unique name for the class-map in the **Name** field, in this example besteffort.

Step 4 Enter a brief text description for the class-map.

Step 5 Click **Define Rule for Class Map**.

Step 6 Select **Type of Service (TOS)**, then select the DSCP value besteffort from the list.

Step 7 Click **Save**.

Step 8 Click **Save**.

Step 9 Repeat Step 2 to Step 8 for each class-map to be defined, naming each one appropriately and selecting the appropriate DSCP values when defining the match rules. Repeat Step 5 to Step 7 in each case where there are multiple match rules to be defined. In all cases in this example, you retain the default selection **Traffic can match ANY of the rules**.

The next task is to define the policy-map for the configuration. In this example, a multi-class WFQ policy-map is configured, comprising the class-maps and the monitor-queuing-map defined in the previous tasks:

Step 1 Click **Add New Policy Map**.

Step 2 Enter a unique name for the policy-map in the **Name** field.

Step 3 Enter a brief text description for the policy-map in the **Description** field.

Step 4 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps.

Step 5 Select **Cisco Modular QoS CLI**.

Step 6 Click **Define Class**.

The **Add Class** page is displayed.

Step 7 Select a class-map from the list of previously configured class-maps.

Step 8 If you are applying a monitor-queuing-map to the class, select a monitor-queuing-map from the list.

Step 9 Select queue type **Bandwidth**.

Step 10 Enter the bandwidth allocated for the class in the **Reserve Bandwidth** field. In this example, the bandwidth allocated for the critical class is 20%.

Step 11 Enter a value in packets for the maximum allowable queue length for the class in the **Queue Limit** field.

Step 12 Click **Save**.

Step 13 Repeat the steps for each class to be defined. In particular, note that all bandwidth classes must be defined in either kbps or as a percentage, but not as a mixture of both. So in this example, the remaining classes are configured with the following percentage values:

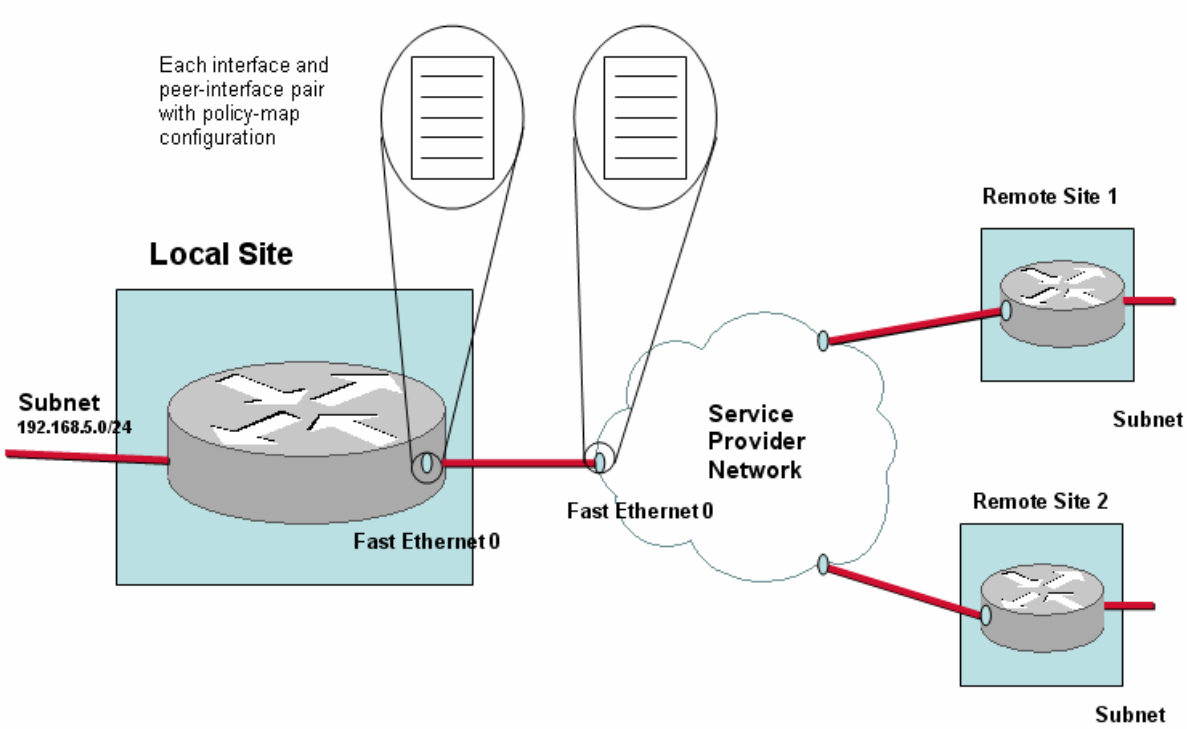
Realtime – 15%
Video – 10%
Bulk – 5%
Besteffort – 0%

Step 14 Click **Save**.

The **Policy Map** page is displayed. The new policy-map is listed on this page. The policy-map should now be available for selection when defining site router interfaces.

The next task is to define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has one interface, Fast Ethernet0, with an associated peer-interface, both connected to the 10000 kbps link and each using a separate policy-map:

Figure 3-5 Basic MPLS VPN, Internet VPN, Private VPN Deployment – Local Site Configuration



Step 1 Click the named local site link or the **edit** link.

Step 2 The **Edit Local Site** page is displayed.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix in the **Subnet** field, in this example 192.168.5.0/24.

Step 5 To configure a router for the local site, click **Define Router**.

Step 6 Enter a name in the **Router Name** field.

Step 7 Enter a brief description in the **Router Description** field.

Step 8 Check each of the BQM physical ports from the **Physical Ports Monitoring this Router** field that are being used to measure traffic for this router.

Step 9 To configure an interface for the router, click **Define Interface**.

Step 10 Select **MPLS VPN…** as the **WAN Connectivity** type.

Step 11 Enter a name in the **Interface Name** field, in this example FastEthernet0.

Step 12 Enter a brief description in the **Description** field.

Step 13 Enter the link bandwidth for the interface, in this example 100 Mbps, in the **Bandwidth** field.

Step 14 Select the policy-map for the interface from the **Policy Map** list.

Step 15 Check that the peer-interface details in the Service Provider panel are correct.

Step 16 Click **Save**.

The **Router** page is displayed.

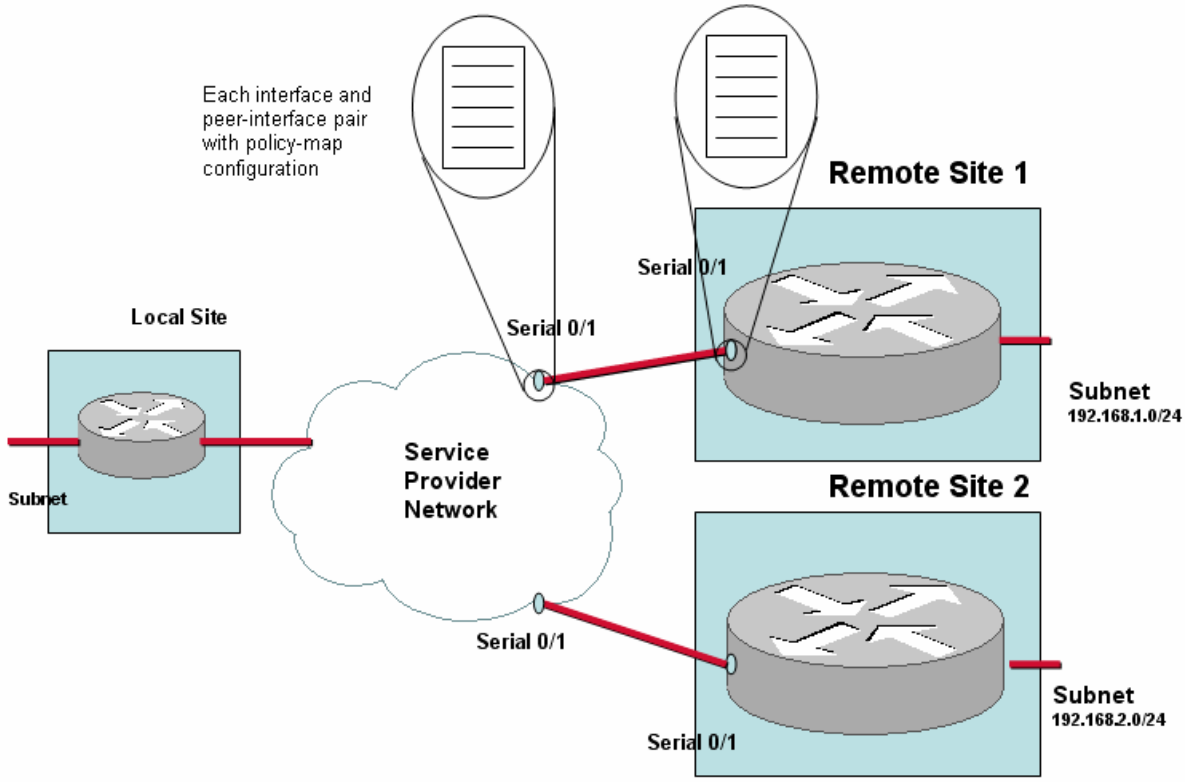
Step 17 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

Step 18 Click **Save**.

The new local site configuration is saved and the **Sites/Interfaces** page is displayed.

Figure 3-6 Basic MPLS VPN, Internet VPN, Private VPN Deployment – Remote Site Configuration



The next task is to define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, whose connection with its associated Service Provider PE router is made explicit by defining each interface and peer-interface pair:

Step 1 Click **Define Remote Site**.

Step 2 Enter a unique name in the **Site Name** field.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix, in this example 192.168.1.0/24, in the **Subnet** field.

Step 5 Enter the IP address of a reliably contactable host on the site subnet in the **Ping Address** field.

Step 6 Select a previously defined end-to-end queuing map from the **End to End Map** list.

Step 7 Click **Define Router**.

The **Add Router** page is displayed.

Step 8 Enter a name in the **Router Name** field, in this example remote1.

Step 9 Enter a brief description in the **Router Description** field.

Step 10 To configure an interface for the router, click **Add Interface**.

Step 11 Select **MPLS VPN…** as the **WAN Connectivity** type.

Step 12 Enter a name in the **Interface Name** field, in this example Serial0/1.

Step 13 Enter a brief description in the **Description** field.

Step 14 Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.

Step 15 Select the policy-map for the interface from the **Policy Map** list.

Note For more information on configuring advanced options for an interface, see the section "Configuring Advanced Interface Settings."

Step 16 Check that the peer-interface details in the Service Provider panel are correct.

Step 17 Click **Save**.

The **Router** page is displayed.

Step 18 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

Step 19 Click **Save**.

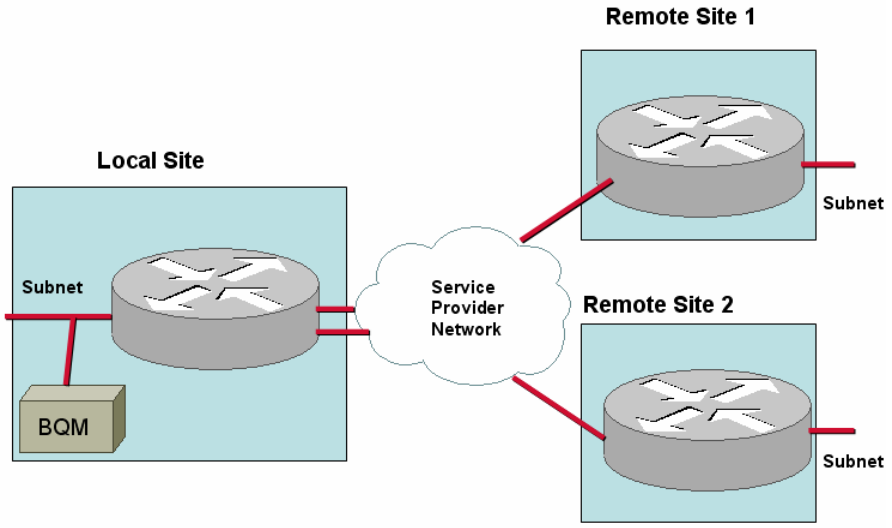
The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.

Step 20 Repeat this task from Step 1 to Step 19 to add the second remote site.

VPN Deployment with Redundant Local Site Connectivity

The BQM network model can be configured to model this deployment. However, because of the potential in a load balancing situation for the same traffic to be split over both links, the BQM does not present accurate traffic statistic results for the local site interfaces in this case.

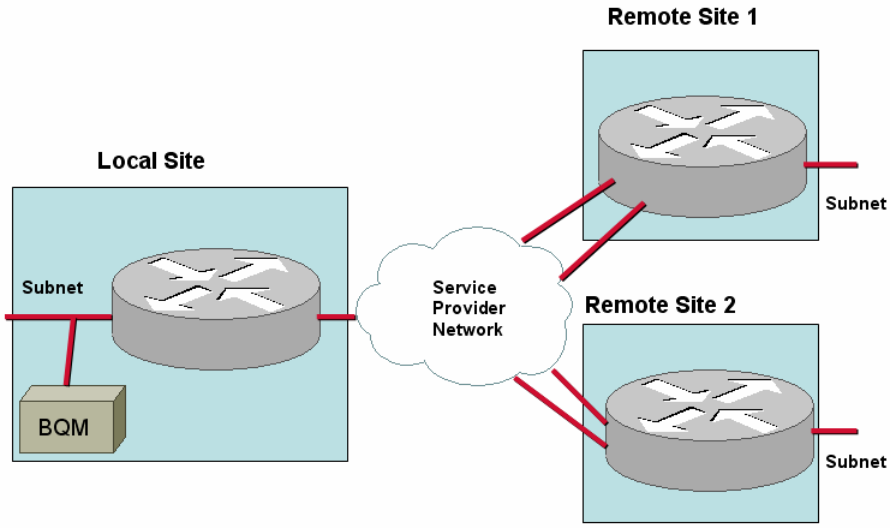
Figure 3-7 Network Model –VPN Deployment with Redundant Remote Site Connectivity



VPN Deployment with Redundant Remote Site Connectivity

The BQM network model can be configured to model this deployment. However, because of the potential in a load balancing situation for the same traffic to be split over both links, the BQM does not present accurate traffic statistic results for the remote site interfaces in this case.

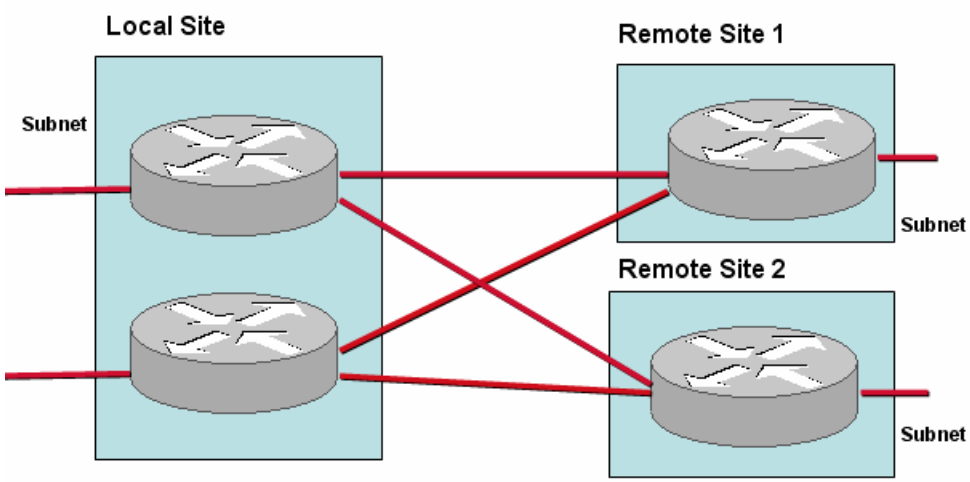
Figure 3-8 Network Model –VPN Deployment with Redundant Remote Site Connectivity



Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM and so all measurements are made from the perspective of the local site. Each local site router must be bound to specific BQM physical measurement ports.

Figure 3-9 Network Model – Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment



To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is not editable
  - Subnet
  - Router
  - Two interfaces specifying bandwidth configuration and policy-maps
  - Mapping of BQM physical measurement ports to routers

- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Interface with link to local site-router-interface, bandwidth, policy-map

To configure the network model for this deployment from the GUI, the first task is to configure the monitor-queuing-map:

Step 1 In **System Administration** mode, click the **Configuration** tab, and then click **Queuing Maps**.

Step 2 Click **Define Monitor Queuing Map**.

Step 3 Enable and configure the required features and thresholds. In this example configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified.

The next task is to configure a monitor-end-to-end-map. To define a monitor-end-to-end-map, you do the following:

Step 1 Click the **End to End Maps** menu and click **Add End to End Map**.

Step 2 Enter a unique name for the monitor-end-to-end-map in the **Name** field.

Step 3 Enter a brief text description for the monitor-end-to-end-map in the **Description** field.

Step 4 To configure the ping packet interval, enter a value in milliseconds in the **Interval** field.

Step 5 To configure the ping packet size, enter a value in bytes in the **Packet Size** field.

Step 6 To establish the number of pings that must be lost before a site is considered unavailable, enter a value in the **Availability Threshold** field.

Step 7 To enable event detection and set an event detection threshold based on measured end-to-end packet delay, enter a delay value in milliseconds in the **Trigger Delay events above** field.

Step 8 To enable event detection if any end-to-end packet loss is detected, check the **Trigger event for any Packet Loss** check box.

Step 9 Click **Save**.

The monitor-end-to-end-map is available to choose when defining remote sites.

The next task is to define the policy-map for the configuration. In this example, the single-class FIFO policy-map is configured, comprising only the default class, named class-default, and the monitor-queuing-map configured above is used:

Step 1 Click **Policy Maps**.

Step 2 Click **Add New Policy Map**.

Step 3 Enter a unique name for the policy-map in the **Name** field.

Step 4 Enter a brief text description for the policy-map in the **Description** field.

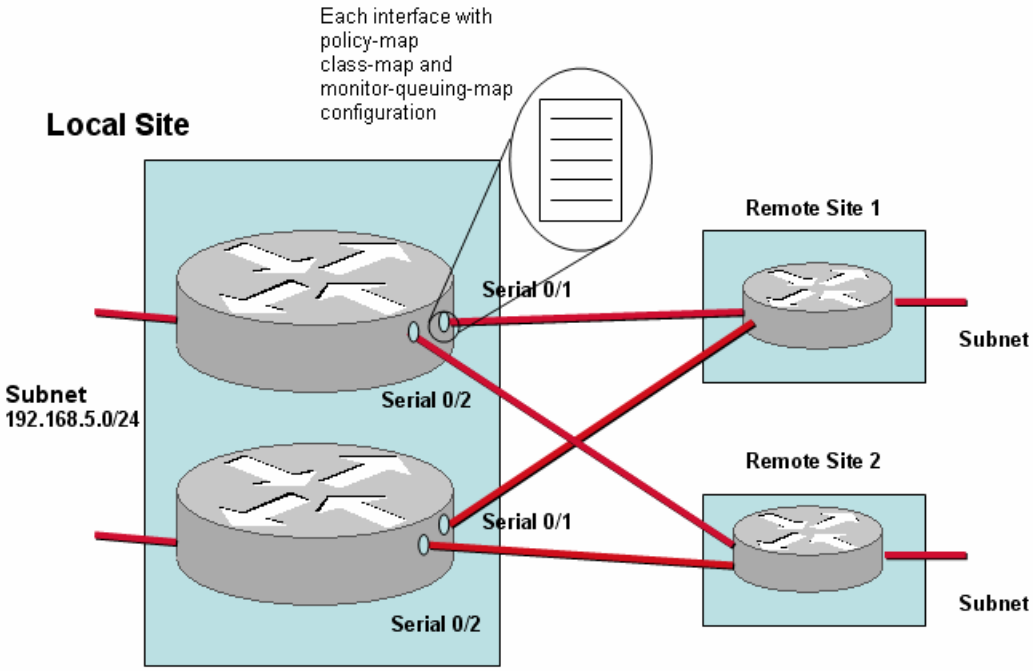
Step 5 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps.

Step 6 Click **Save**.

The new policy-map is saved and displayed on the **Policy Maps** page. The single class, class-default, is added to the policy-map automatically by the system.

The next task is to define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has two interfaces, Serial0/1 and Serial0/2, with both connected to links of 512 kbps and both using the FIFO policy-map:

Figure 3-10 Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Local Site Configuration



Step 1 Click the named local site link or the **edit** link.

Step 2 The **Edit Local Site** page is displayed.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix in the **Subnet** field, in this example 192.168.5.0/24.

Step 5 To configure a router for the local site, click **Add Router**.

Step 6 Enter a name in the **Router Name** field.

Step 7 Enter a brief description in the **Router Description** field.

Step 8 Check each of the BQM physical ports from the **Physical Ports Monitoring this Router** field that are being used to measure traffic for this router. In this example, PortA and PortB are being used to monitor this router.

Step 9 To configure an interface for the router, click **Define Interface**.

Step 10 Select **ATM PVC…** as the **WAN Connectivity** type.

Step 11 Enter a name in the **Interface Name** field, in this example Serial0/1.

Step 12 Enter a brief description in the **Description** field.

Step 13 Enter the link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.

Step 14 Select the FIFO policy-map for the interface from the **Policy Map** list.

Step 15 Click **Save**.

The **Router** page is displayed.

Step 16 Repeat Steps 10 to 15 to add the second interface, in this example Serial0/2.

Step 17 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

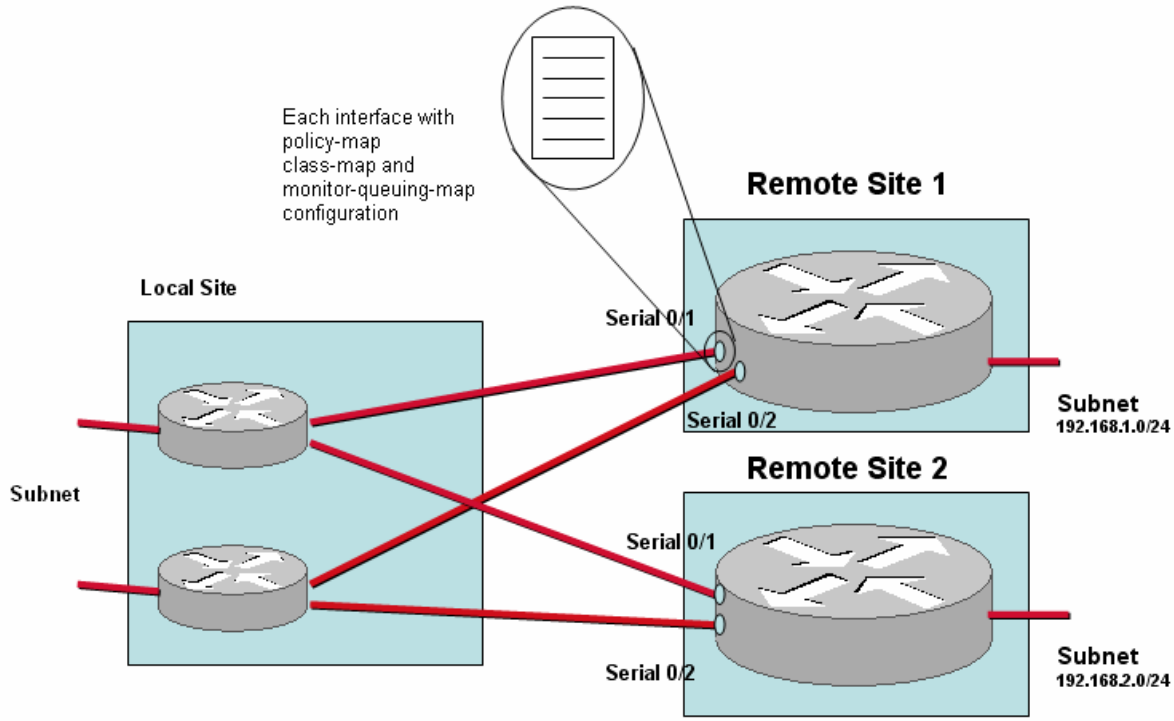
Step 18 Repeat Step 6 to Step 17 to define the second local site router and its interfaces. Note that in Step 8 for the second router, PortC and PortD are used to monitor the second router.

Step 19 Click **Save**.

The new local site configuration is saved and the **Sites/Interfaces** page is displayed.

The next task is to define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, whose interface connections back to each local site interface is made explicit when defining the interfaces:

Figure 3-11 Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Remote Site Configuration



Step 1 Click **Define Remote Site**.

Step 2 Enter a unique name in the **Site Name** field.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix, in this example 192.168.1.0/24, in the **Subnet** field.

Step 5 Enter the IP address of a reliably contactable host on the site subnet in the **Ping Address** field.

Step 6 Select a previously defined end-to-end queuing map from the **End to End Map** list. If you have not already configured any end-to-end queuing maps, the list will contain only the default end-to-end map.

Step 7 Click **Define Router**.

The **Add Router** page is displayed.

Step 8 Enter a name in the **Router Name** field, in this example remote1.

Step 9 Enter a brief description in the **Router Description** field.

Step 10 To configure an interface for the router, click **Define Interface**.

Step 11 Select **ATM PVC…** as the **WAN Connectivity** type, enter a bandwidth value (512 kbps) and select a policy-map (FIFO) for the local site interface (Serial0/1) to which this remote site interface connects.

Step 12 Enter a name in the **Interface Name** field, in this example Serial0/1.

Step 13 Enter a brief description in the **Description** field.

Step 14 Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.

Step 15 Select the FIFO policy-map for the interface from the **Policy Map** list.

Note For more information on configuring advanced options for an interface, see the section "Configuring Advanced Interface Settings."

Step 16 Click **Save**.

The **Router** page is displayed.

Step 17 Repeat Step 10 to Step 16 to add the second interface for the first remote site. Note that when performing Step 11 for the second interface, that in this example, this interface connects to interface Serial0/1 of the second local site router.

Step 18 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

Step 19 Click **Save**.

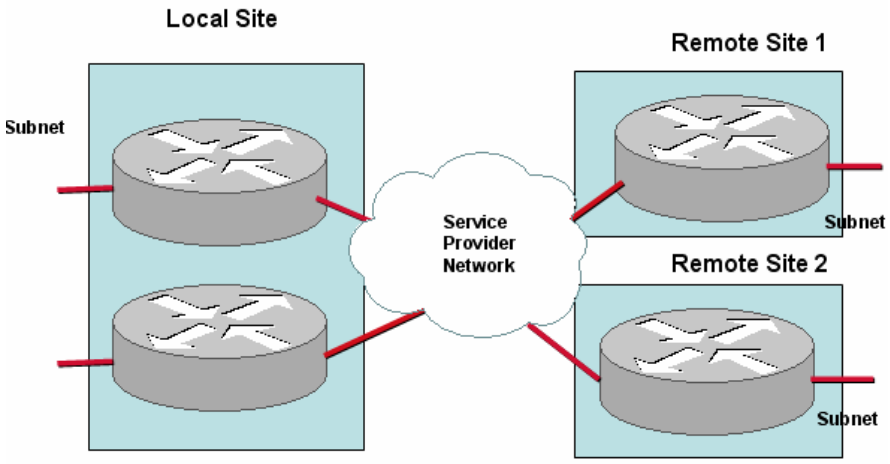
The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.

Step 20 Repeat this task from Step 1 to Step 19 to add the second remote site. Note that when defining interface connectivity for the second remote site router, that in this example interface Serial0/1 of the second remote site router connects to interface Serial0/2 of the first local site router, and interface Serial 0/2 of the second remote site router connects to interface Serial0/2 of the second local site interface.

Dual-homed MPLS Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM and so all measurements are made from the perspective of the local site. The local site link to the SPN cannot be sized, but you can calculate a 'total' WAN bandwidth value. The remote site links can be sized.

Figure 3-12 Network Model – Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment



To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is not editable
  - Subnet
  - Router
  - Local site interface/SPN peer-interface pair with bandwidth configuration and policy-maps
  - Mapping of BQM physical measurement ports to routers

- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

To configure the network model for this deployment from the GUI, the first task is to configure the monitor-queuing-map:

Step 1 In **System Administration** mode, click the **Configuration** tab, and then click **Queuing Maps**.

Step 2 Click **Define Monitor Queuing Map**.

Step 3 Enable and configure the required features and thresholds. In this example configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified.

The next task is to configure a monitor-end-to-end-map. To define a monitor-end-to-end-map, you do the following:

Step 1 Click the **End to End Maps** menu and click **Add End to End Map**.

Step 2 Enter a unique name for the monitor-end-to-end-map in the **Name** field.

Step 3 Enter a brief text description for the monitor-end-to-end-map in the **Description** field.

Step 4 To configure the ping packet interval, enter a value in milliseconds in the **Interval** field.

Step 5 To configure the ping packet size, enter a value in bytes in the **Packet Size** field.

Step 6 To establish the number of pings that must be lost before a site is considered unavailable, enter a value in the **Availability Threshold** field.

Step 7 To enable event detection and set an event detection threshold based on measured end-to-end packet delay, enter a delay value in milliseconds in the **Trigger Delay events above** field.

Step 8 To enable event detection if any end-to-end packet loss is detected, check the **Trigger event for any Packet Loss** check box.

Step 9 Click **Save**.

The monitor-end-to-end-map is available to choose when defining remote sites.

The next task is to define the class-maps for the configuration. In this example, there are the following class-maps:

```
class-map besteffort (match-any)
  match ip dscp=0
class-map bulk (match-any)
  match ip dscp=10
class-map critical (match-any)
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map realtime (match-any)
  match ip dscp=46
  match ip dscp=40
class-map video (match-any)
  match ip dscp=18
  match ip dscp=16
```

Step 1 Click **Class Maps**.

Step 2 Click **Add Class Map**.

Step 3 Enter a unique name for the class-map in the **Name** field, in this example besteffort.

Step 4 Enter a brief text description for the class-map.

Step 5 Click **Define Rule for Class Map**.

Step 6 Select **Type of Service (TOS)**, then select the DSCP value besteffort from the list.

Step 7 Click **Save**.

Step 8 Click **Save**.

Step 9 Repeat Step 2 to Step 8 for each class-map to be defined, naming each one appropriately and selecting the appropriate DSCP values when defining the match rules. Repeat Step 5 to Step 7 in each case where there are multiple match rules to be defined. In all cases in this example, you retain the default selection **Traffic can match ANY of the rules**.

The next task is to define the policy-map for the configuration. In this example, a multi-class WFQ policy-map is configured, comprising the class-maps and the monitor-queuing-map defined in the previous tasks:

Step 1 Click **Add New Policy Map**.

Step 2 Enter a unique name for the policy-map in the **Name** field.

Step 3 Enter a brief text description for the policy-map in the **Description** field.

Step 4 If you are applying a monitor-queuing-map to the policy-map, select a monitor-queuing-map from the list. If you have not configured any monitor-queuing-maps, the list will contain only the default monitor-queuing-map. See the section “Configuring a Monitor-Queuing-Map” for more information on defining monitor-queuing-maps

Step 5 Select **Cisco Modular QoS CLI**.

Step 6 Click **Define Class**.

The **Add Class** page is displayed.

Step 7 Select a class-map from the list of previously configured class-maps.

Step 8 If you are applying a monitor-queuing-map to the class, select a monitor-queuing-map from the list.

Step 9 Select queue type **Bandwidth**.

Step 10 Enter the bandwidth allocated for the class in the **Reserve Bandwidth** field. In this example, the bandwidth allocated for the critical class is 20%.

Step 11 Enter a value in packets for the maximum allowable queue length for the class in the **Queue Limit** field.

Step 12 Click **Save**.

Step 13 Repeat from Step 6 to Step 12 for each class to be defined. Note that all bandwidth classes must be defined in either kbps or as a percentage, but not as a mixture of both. So in this example, the remaining classes are configured with the following percentage values:

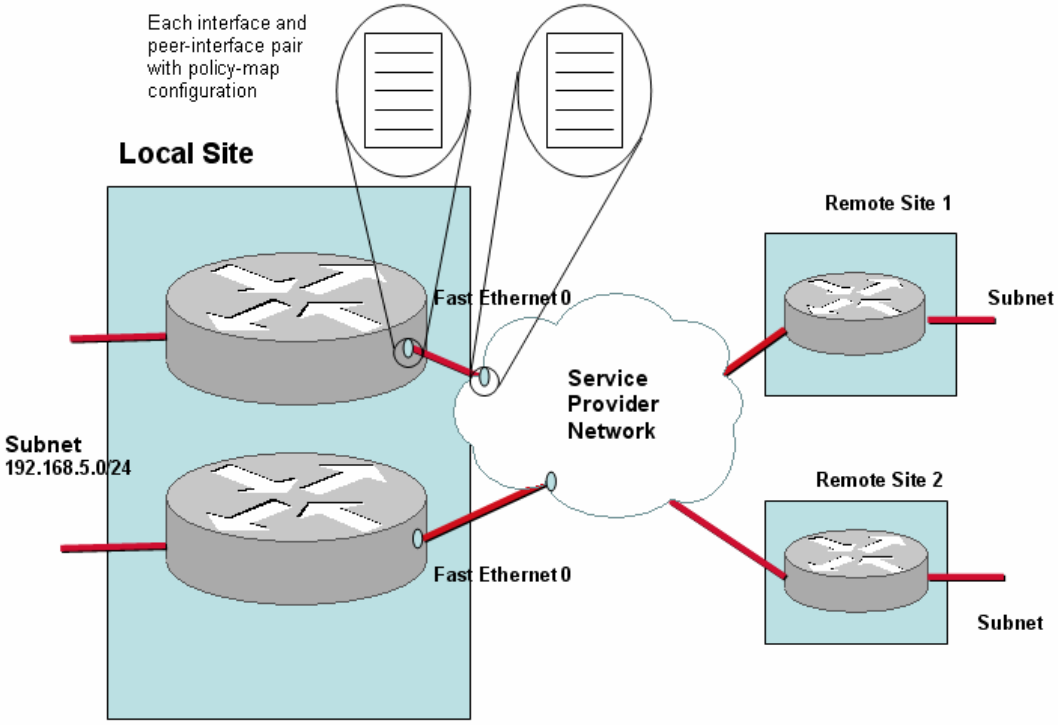
Realtime – 15%
Video – 10%
Bulk – 5%
Besteffort – 0%

Step 14 Click **Save**.

The **Policy Map** page is displayed. The new policy-map is listed on this page. The policy-map should now be available for selection when defining site router interfaces. In this example configuration, we assume that the same policy-map is applied to all interfaces and associated peer-interfaces.

The next task is to define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site routers, named core1 and core2 each have one interface, both named Fast Ethernet0, each with an associated peer-interface. Both interfaces are connected via a 100 Mbps link and each using a separate policy-map:

Figure 3-13 Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment – Local Site Configuration



Step 1 Click the named local site link or the **edit** link.

Step 2 The **Edit Local Site** page is displayed.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix in the **Subnet** field, in this example 192.168.5.0/24.

Step 5 To configure a router for the local site, click **Add Router**.

Step 6 Enter a name in the **Router Name** field.

Step 7 Enter a brief description in the **Router Description** field.

Step 8 Check each of the BQM physical ports from the **Physical Ports Monitoring this Router** field that are being used to measure traffic for this router. In this example, PortA and PortB are used to monitor the first local site router.

Step 9 To configure an interface for the first router, click **Define Interface**.

Step 10 Select **MPLS VPN…** as the **WAN Connectivity** type.

Step 11 Enter a name in the **Interface Name** field, in this example FastEthernet0.

Step 12 Enter a brief description in the **Description** field.

Step 13 Enter the link bandwidth for the interface, in this example 100 Mbps, in the **Bandwidth** field.

Step 14 Select the policy-map for the interface from the **Policy Map** list.

Step 15 Check that the peer-interface details in the Service Provider panel are correct.

Step 16 Click **Save**.

The **Router** page is displayed.

Step 17 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

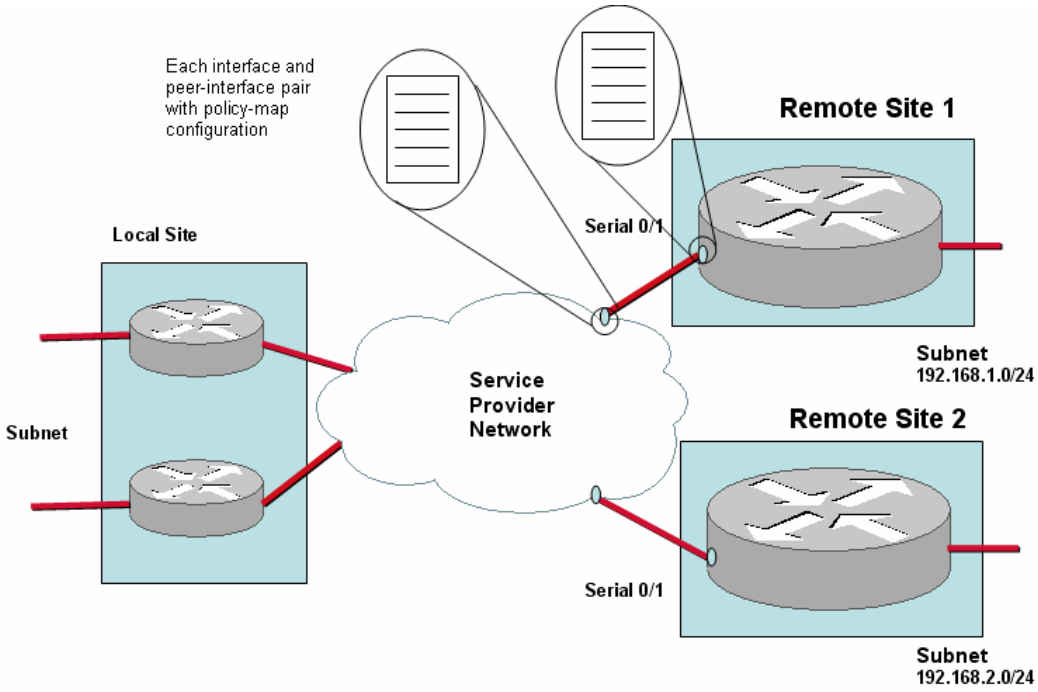
Step 18 Repeat from Step 6 to Step 17 for the second local site router. Note that in this example, when completing Step 8 for the second local site router, PortC and PortD are used.

Step 19 Click **Save**.

The new local site configuration is saved and the **Sites/Interfaces** page is displayed.

The next task is to define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, whose connection with its associated Service Provider PE router is made explicit by defining each interface and peer-interface pair:

Figure 3-14 Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment – Remote Site Configuration



Step 1 Click **Define Remote Site**.

Step 2 Enter a unique name in the **Site Name** field.

Step 3 Enter a brief description of the site in the **Site Description** field.

Step 4 Enter the site subnet address and prefix, in this example 192.168.1.0/24, in the **Subnet** field.

Step 5 Enter the IP address of a reliably contactable host on the site subnet in the **Ping Address** field.

Step 6 Select a previously defined end-to-end queuing map from the **End to End Map** list.

Step 7 Click **Define Router**.

The **Add Router** page is displayed.

Step 8 Enter a name in the **Router Name** field, in this example remote1.

Step 9 Enter a brief description in the **Router Description** field.

Step 10 To configure an interface for the router, click **Define Interface**.

Step 11 Select **MPLS VPN…** as the **WAN Connectivity** type.

Step 12 Enter a name in the **Interface Name** field, in this example Serial0/1.

Step 13 Enter a brief description in the **Description** field.

Step 14 Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.

Step 15 Select the policy-map for the interface from the **Policy Map** list.

Note For more information on configuring advanced options for an interface, see the section "Configuring Advanced Interface Settings."

Step 16 Check that the peer-interface details in the Service Provider panel are correct.

Step 17 Click **Save**.

The **Router** page is displayed.

Step 18 Click **Save**.

The **Edit Sites/Interfaces** page is displayed.

Step 19 Click **Save**.

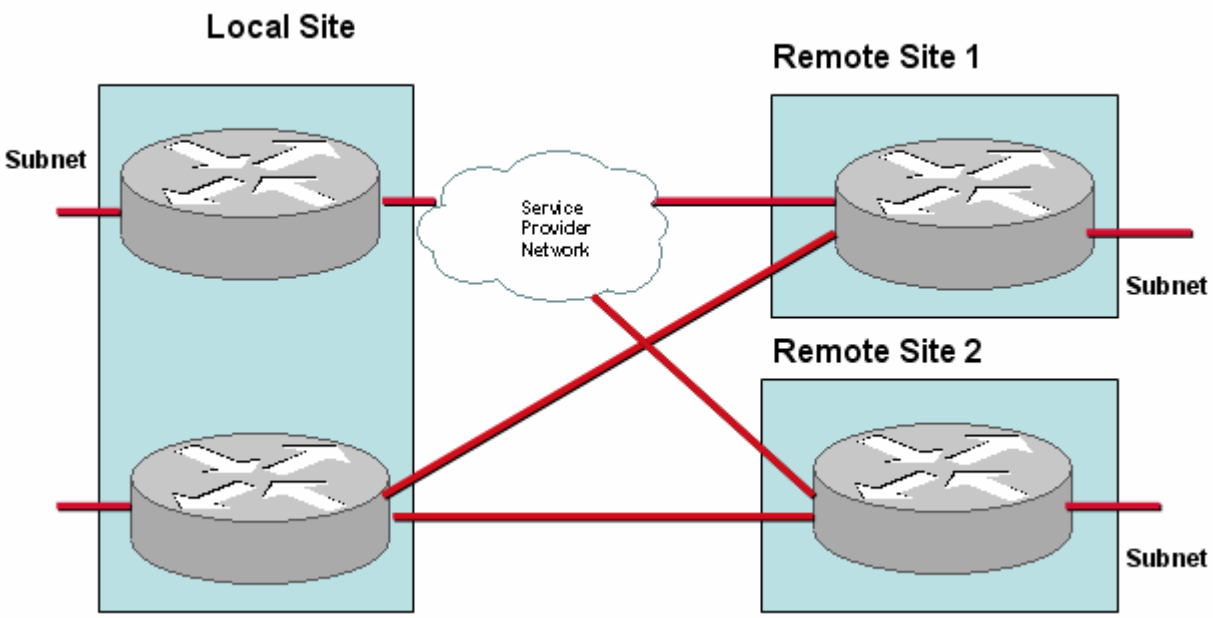
The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.

Step 20 Repeat this task from Step 1 to Step 19 to add the second remote site.

Hybrid Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM and so all measurements are made from the perspective of the local site. Each local site router must be bound to specific BQM physical measurement ports.

Figure 3-15 Network Model – Hybrid Deployment



You need to use the CLI to configure this deployment type successfully. For more information see "Configuring Network Model Deployments with the CLI."

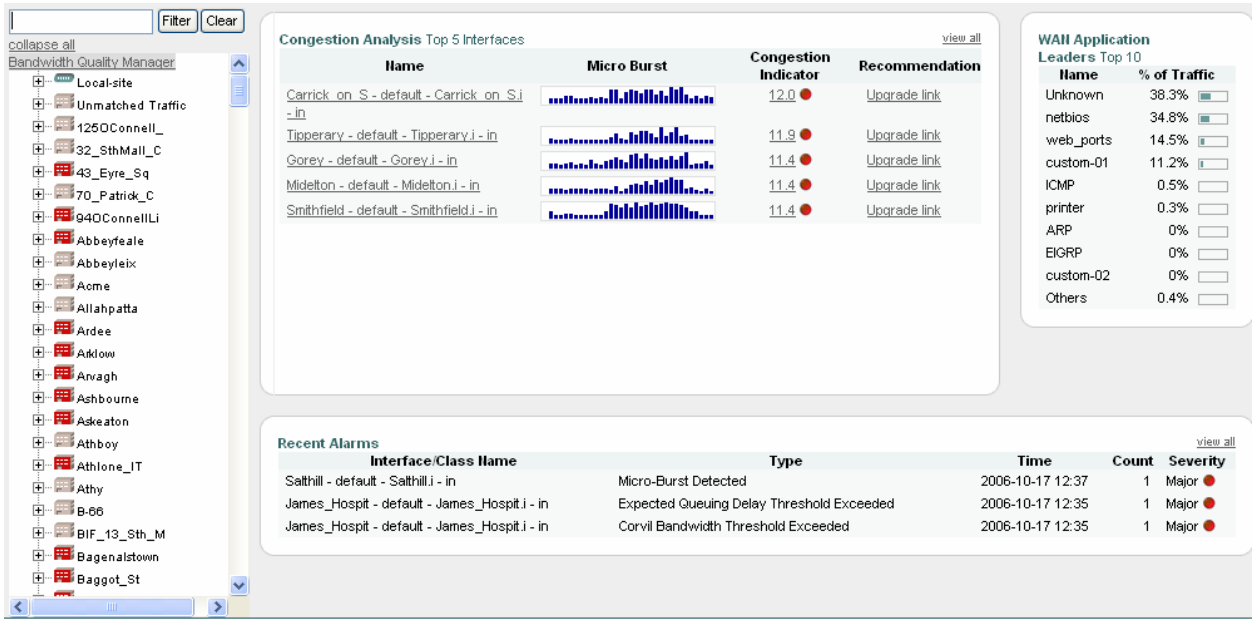
4 Monitoring Network Traffic

This chapter describes the network monitoring information available in the BQM Monitoring screens when the system has been successfully configured and is measuring data. The displayed information enables you to identify network issues by monitoring congestion, network traffic statistics and bandwidth sizing measurements.

Monitoring Dashboard Overview

This section introduces the use of the BQM to monitor the network. In many cases this means you will be looking to spot problems on the network before users report them. There are of course cases when users may report a problem and you would use the BQM to investigate the problem. The detailed analysis of traffic is done using the **Congestion Analysis** and **Traffic Insight** tabs, but the **Dashboard** tab provides a summary of network quality.

Figure 4-1: Monitoring Dashboard



Even if a user reports a problem you may still want to view many of the statistics displayed on the dashboard to determine if the problem is in fact network-related. In many cases the monitoring information displayed on the dashboard will confirm that the network is not the problem and will therefore allow you to concentrate your efforts elsewhere, such as on application analysis. In other cases, the dashboard information will confirm a network quality issue, and it will guide you as to where to begin further analysis.

The BQM dashboard displays summary information about the following:

- **Recent Alarms** - a list of most recent network quality alarms.
- **Congestion Analysis** Top 10 Interfaces - a list of the top ten most congested interfaces on the network and a chart of the total number of congested interfaces.
- **WAN Application Leaders** Top 10 - the list of the top ten applications using most resources on the network.

All of the displayed information relates to the selected reporting period. The default reporting period is the previous 24 hours. For information on changing the selected reporting period, see the section “Selecting a Reporting Period.”

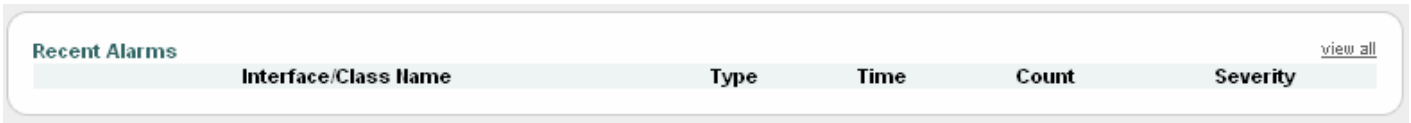
You can use the tree view on the dashboard to navigate to an interface or class of interest and view summary congestion, top application and microburst results.

Note The results presented by the BQM are based on the assumption that the device has not dropped packets. You can check this status on the **Quality Alarms** tab. If packets have been dropped then the presented results may not be an accurate reflection of the network traffic.

Identifying Recent Quality Alarms

The following describes the information displayed in the Recent Alarms table:

Figure 4-2: Recent Quality Alarms



Interface/Class Name - displays the full, qualified name identifying the interface or class for which the alarm was triggered: site name - router name – interface name – direction – class name.

Type - displays the quality alarm type.

Time - displays the time at which the active alarm triggered, or at which a cleared alarm was cleared.

Count - displays the number of alarms of this type that have been triggered during the selected reporting period.

Severity - displays the severity of the alarm. The severity levels for SNMP traps are the following:

Informational – events that require notification but do not cause failures.
Warning – typically used for thresholds that warn of an impending failure.
Minor – not used for defaults.
Major – an event that has the potential to make BQM no longer operational.
Severe – BQM no longer operational.

Quality alarms are generated whenever an event is generated. An alarm of a particular type persists until the system detects an interval with no events of that type. For example, if you have configured a delay threshold of 500ms, then if a single packet is delayed beyond 500ms, a quality alarm is generated.

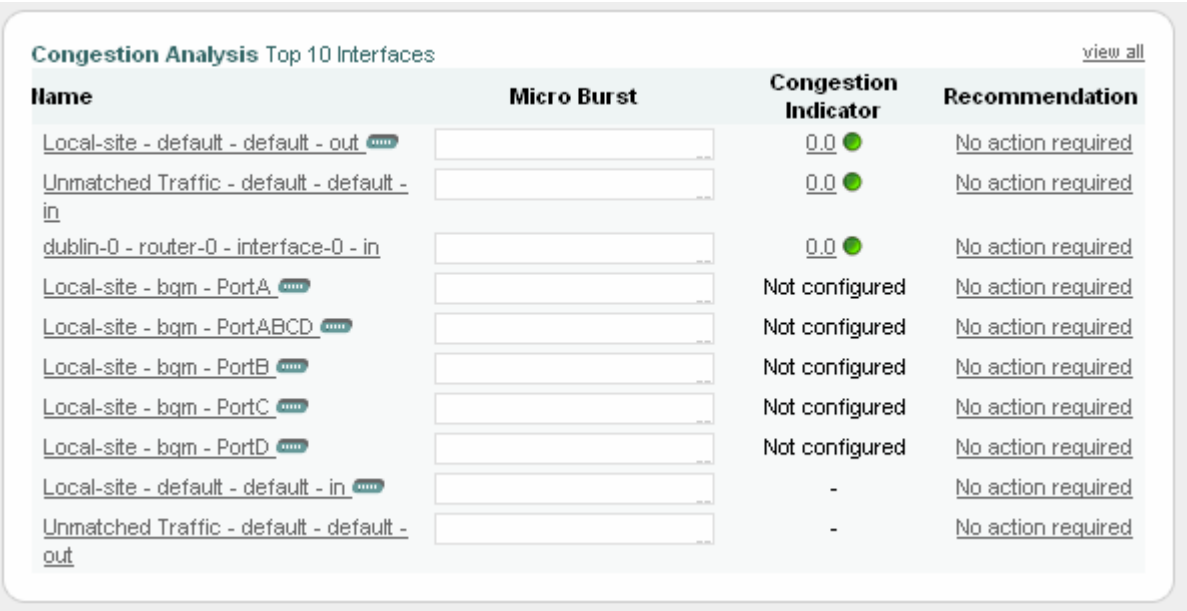
Thresholds for all links and classes can be created during configuration. Only the five most recent alarms remain in the table if more recent alarms occur.

To see all active alarms on the **Quality Alarms** tab, you click **view all**.

Identifying the Top Congested Interfaces

The **Congestion Analysis** section of the dashboard displays the top ten congested interfaces on the network.

Figure 4-3: Top Congested Interfaces



The following describes the congestion information displayed on the dashboard:

Name - displays the name (and direction) of the interface: 'interface name - direction'.

Microburst - displays a graph showing the largest byte volumes observed over the selected time period.

Congestion Indicator - displays a number reflecting the congestion level for an interface. The number represents the largest Congestion Indicator value seen on any class on that interface. A Congestion Indicator value greater than 1 means the loss and/or delay are greater than that specified. A Congestion Indicator of less than 1 means the loss and/or delay are better than that specified. The class value is the largest Congestion Indicator value calculated for the class over the chosen reporting period.

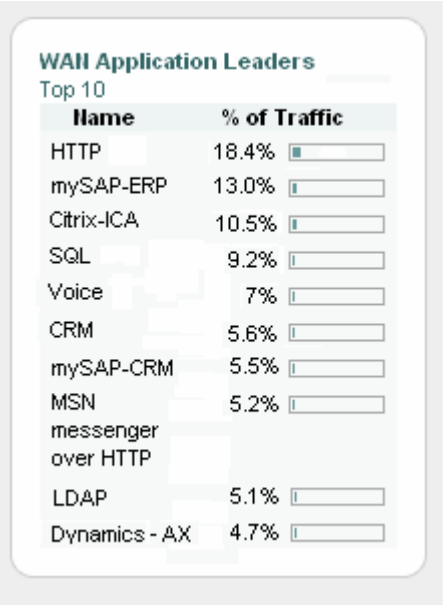
Recommendation - indicates whether or not an upgrade of the interface capacity is required.

If you click on an interface name in the list of top ten congested interfaces, the **Congestion Analysis** tab is displayed, showing the details of the congestion events associated with that interface. Alternatively, to see the state of congestion for all configured interfaces on the **Congestion Analysis** tab, you click **view all**.

Identifying WAN Application Leaders

The **WAN Application Leaders** Top 10 list displays the applications that have the top ten highest average volumes over a five-minute period for all traffic.

Figure 4-4: WAN Application Leaders



The following describes the application leader information displayed:

Name - displays the name of the application; the BQM maintains a database of application signatures and port numbers that all traffic is tested against. Matching signatures are displayed under the application name for that signature. You can also add custom applications to the database, so configured custom application names may

be displayed on the list. Application traffic that does not match any signatures currently in the BQM database, or any defined custom application match rules, is displayed as 'Unknown.'

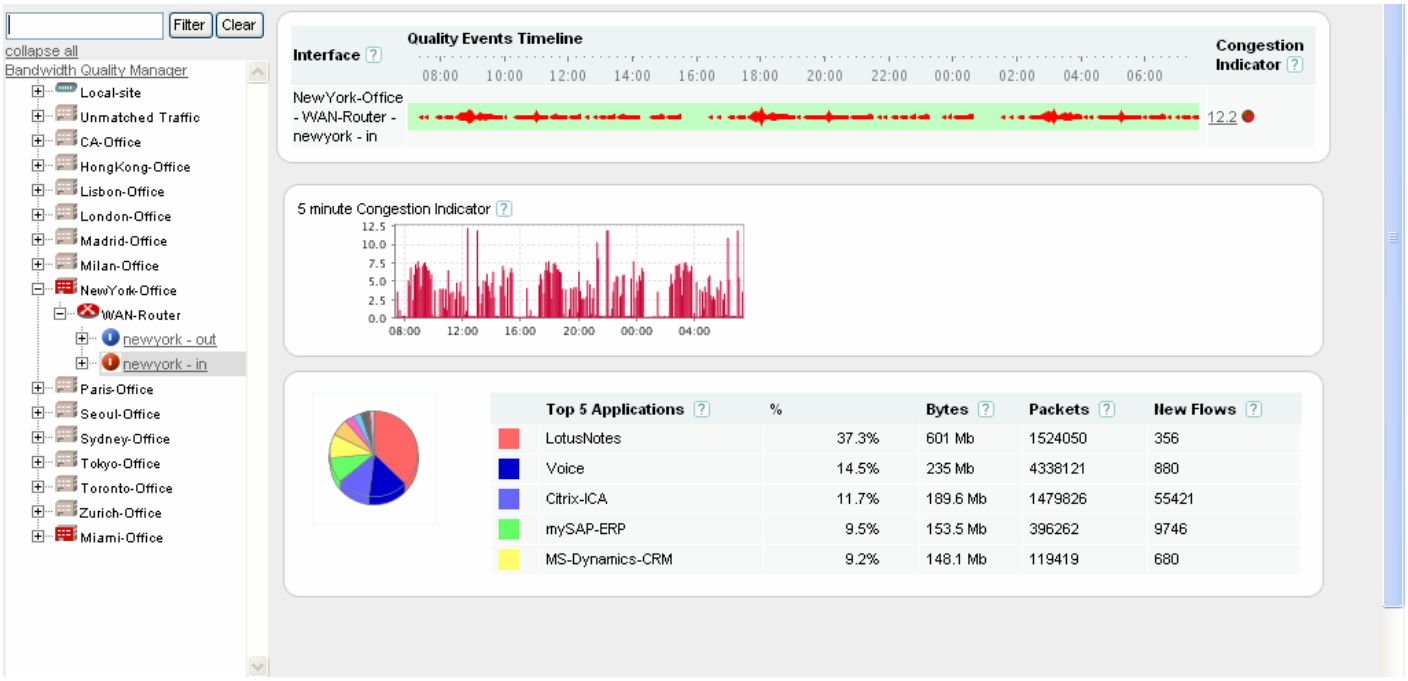
% of Traffic - displays the percentage of overall traffic volume that the application comprises.

To view detailed traffic statistics per interface you navigate to the **Traffic Insight** tab.

Viewing Summary Interface and Class Results

The BQM dashboard includes a navigation system that enables you to pick out a particular interface or group of interfaces, and their associated classes, and view summary results for each.

Figure 4-5: Dashboard Navigation



The navigation tree comprises the local site, all configured remote sites, and site to contain any unmatched traffic.

Note The default BQM configuration includes a pre-configured remote site named Unmatched Traffic. Before you change the default configuration, all non-local site traffic is measured by this site. As you add remote sites to your network model configuration, the amount of traffic appearing in the unmatched category decreases.

The unmatched traffic category only includes packets that don't go to any remote site (or connected local site interface). It also filters out packets that are internal to the local site subnet(s). Finally, it uses the local site subnet(s) to split out unmatched traffic into the interface (Unmatched Traffic - default - default - out) and peer-interface (Unmatched Traffic - default - default -in) directions, where possible; that is, if the packet is either coming from or going to a local site subnet, but not both.

You click the local or remote site name to display the configured routers for the selected site. You then click the router of interest to display the configured interface(s) for that router. When you click on an interface you see the summary results for that interface. You expand the interface node on the navigation tree and click the class of interest to see class results.

To collapse all parts of the navigation tree, click **collapse all**. To display the dashboard information for the whole network, click **Bandwidth Quality Manager**.

You can also type the name of a configuration object in the Filter field and click **Filter** to display only a set of matching interfaces and classes.

The interface and class results include the following:

- Congestion results
- Top Applications results

For local site outbound and remote site inbound interfaces, the summary results include Congestion Indicator, Corvil Bandwidth and Expected Delay and Loss graphs. For local site inbound and remote site outbound interfaces, the summary results include Microburst graphs.

Congestion Results

When you navigate to the interface or class level, you can view summary congestion results.

Figure 4-6: Congestion Results

Interface or **Class** - displays the configured name of the interface and the direction of the traffic (inbound or outbound), or the name of the selected class.

Quality Events Timeline - displays a graphical representation of the chosen reporting period where a mark on the timeline proportional to the congestion being detected indicates one or more quality threshold violation

events. If you do not have quality thresholds configured in the monitor-queuing-map for the interface of interest, then no events will be displayed on the timeline. The longer the chosen reporting period, the more likely that multiple events will be displayed as a single bar on the timeline. The shorter the chosen reporting period, the more likely that a single bar will represent a single event. An interface that is in constant violation of a particular configured threshold may show a single solid bar over the entire duration of shorter chosen timescales (for example, 1 hour). An alarm corresponding to each quality violation event is displayed in the **Quality Alarms** tab. The threshold at which quality events are triggered is determined by the configuration of the monitor-queuing-map applied to the interface.

Congestion Indicator - indicates quality issues in the network. The Congestion Indicator uses millisecond measurements to detect congestion events in the router queues based on the specified quality of service targets. Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets that are used to calculate the Congestion Indicator. If you have not enabled Congestion Indicator calculation in the monitor-queuing-map being applied to an interface or class, the status is displayed as "Not Configured."

Top Applications Results

The top applications summary for interfaces and classes include the following:

Figure 4-7: Top Applications Results

Top 5 Applications	%	Bytes	Packets	New Flows
LotusNotes	37.3%	601 Mb	1524050	356
Voice	14.5%	235 Mb	4338121	880
Citrix-ICA	11.7%	189.6 Mb	1479826	55421
mySAP-ERP	9.5%	153.5 Mb	396262	9746
MS-Dynamics-CRM	9.2%	148.1 Mb	119419	680

The **Top Applications** column identifies the name of each of the top five discovered applications during the selected reporting period. If the system has not had enough time to match a given set of traffic with a known application, it is listed as ‘Undetermined.’ If traffic does not belong to an application known to the system, it is added to the listed category ‘Unknown.’

The **Bytes** column displays the total number of bytes for the application during the selected reporting period.

The **Packets** column displays the total number of packets for the application during the selected reporting period.

The **New Flows** column displays the total number of new flows initiated for the application during the selected reporting period. This figure represents the lower bound on new flows which have been detected within the selected reporting period. Actual flow counts may be higher.

Note A flow is defined as follows - A network traffic flow is a unidirectional sequence of packets all sharing the same source and destination IP address, source and destination port, and IP protocol.

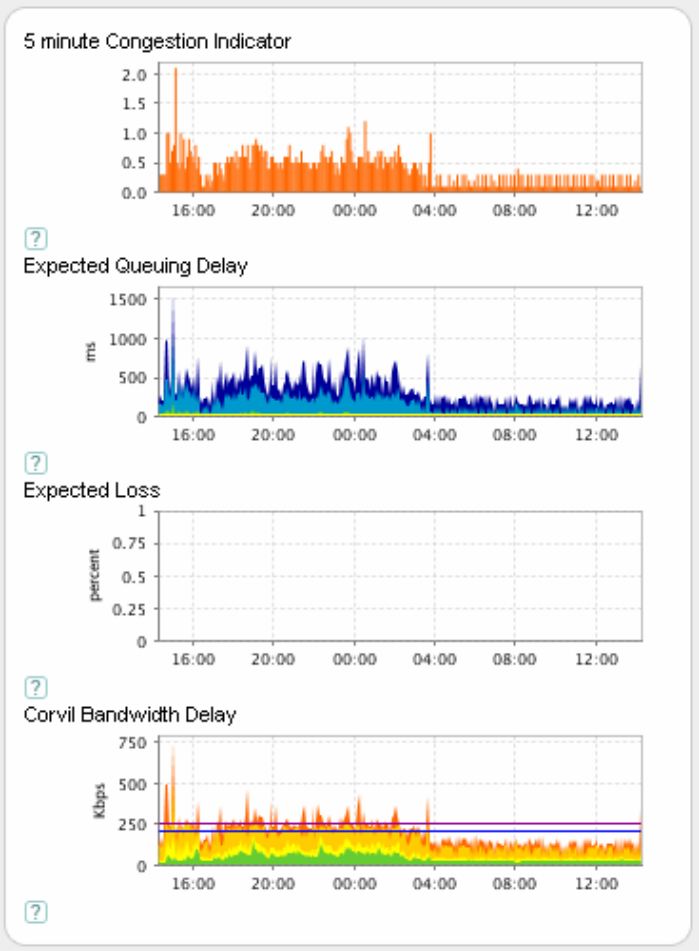
The color legend matches each colored segment of the chart to a listed application.

Microburst or Congestion Indicator, Corvil Bandwidth and Expected Delay and Loss Results

For local site inbound interfaces and remote site outbound interfaces, the microburst graph displays the measured peak bit rates during the selected reporting period at the configured millisecond-level resolution. The default resolution for microburst measurements is five milliseconds.

For local site outbound interfaces and remote site inbound interfaces, the Congestion Indicator graph displays the calculated Congestion Indicator values, Corvil Bandwidth (Delay) values, and Estimated Delay and Queue Length results as calculated by the BQM simulation based on the traffic measured during the selected reporting period.

Figure 4-8: Congestion Indicator, Corvil Bandwidth and Expected Delay and Loss Results



For more information on these graphs, see “Viewing Class Measurements.”

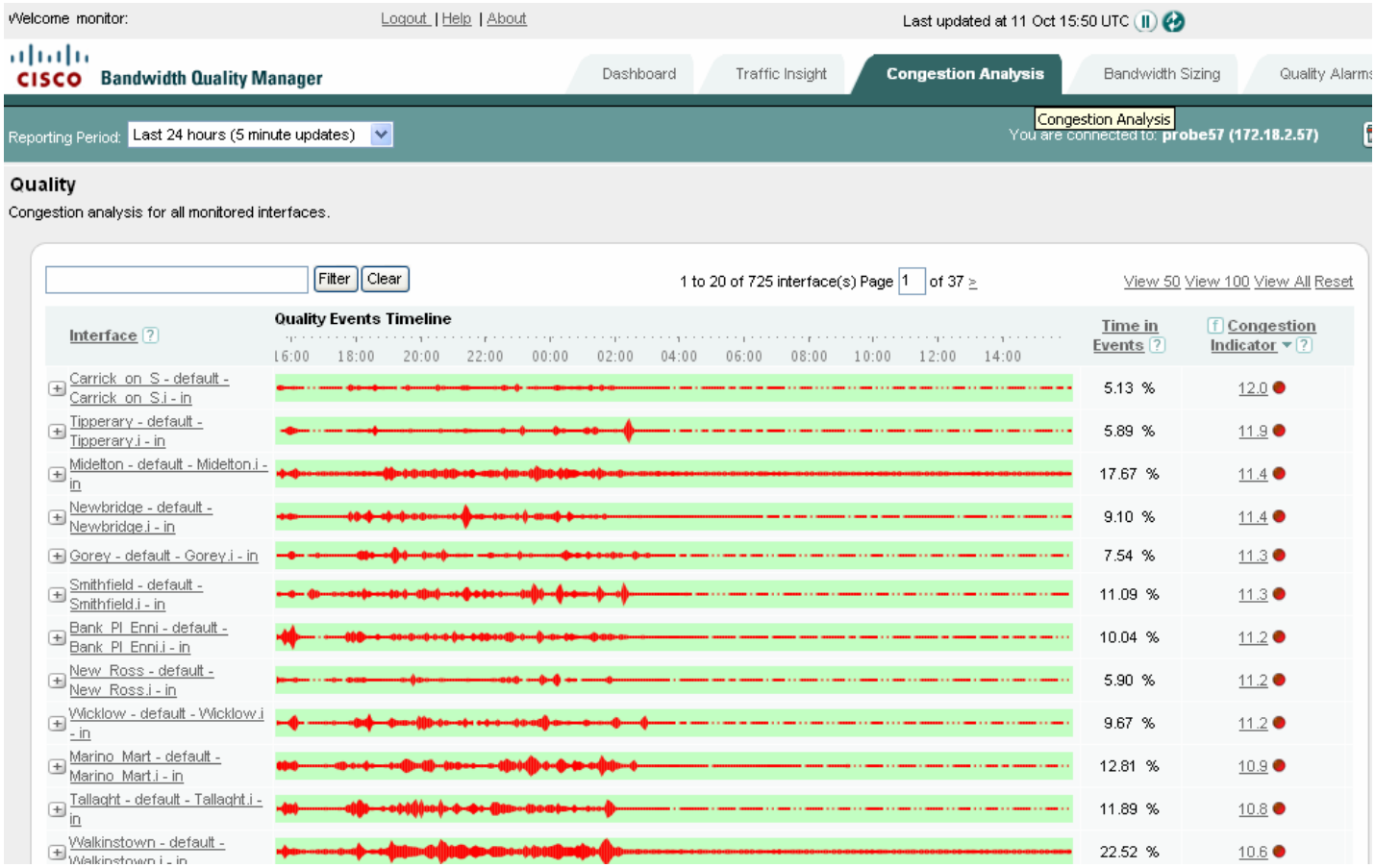
Monitoring Congested Interfaces

By default the **Congestion Analysis** tab lists all of the interfaces you have configured in the BQM network model. The summary table information is sorted by Congestion Indicator value and provides a visual guide to congestion events for each of these interfaces. You can choose from a predefined list of reporting periods up to 60 days or define a custom reporting period over which to view data. You can also sort the summary information by column and you can drill into each interface to view more details (such as class congestion events). This enables you to identify the information you need. For each congested interface you can analyze more information to troubleshoot a congestion event that is impacting on quality of service. For more information on investigating individual quality events, see the chapter "Troubleshooting a Quality Event."

Congestion Analysis Overview

By default, results for twenty interfaces are displayed per page and if there are more than twenty interfaces configured, you use the links to navigate between pages of results.

Figure 4-9: Congestion Analysis Results



If you have many interfaces configured, you can also click the **View 50**, **View 100**, or **View All** links to display the corresponding number of interfaces on a single page. In these cases you scroll down the page to view all the presented results.

The following table describes the information displayed in the congestion analysis summary table:

Table 4-1: Congestion Analysis Summary Table

Column	Description
Interface	Displays the full, qualified name identifying the interface and the direction of the traffic (inbound or outbound) being measured by the interface: *site name – router name – interface name – direction*. The site name, router name and interface name are those that have been configured in the BQM network model. The direction of traffic is always represented from the perspective of a site in the BQM network model. In the case of MPLS deployments this means that for each interface and peer interface pair configured in the network model, the configured interface represents the outbound traffic from the site (local or remote) and the peer-interface represents the inbound traffic to the site (local or remote).
Quality Events Timeline	Displays a graphical representation of the chosen reporting period where a mark on the timeline indicates one or more threshold violation events. If you do not have thresholds configured in the monitor-queuing-map for the interface of interest, then no events will be displayed on the timeline. The longer the chosen reporting period, the more likely that multiple events will be displayed on the timeline. The shorter the chosen reporting period, the more likely that a single mark will represent a single event. An interface that is in constant violation of a particular configured threshold may show a single solid bar over the entire duration of shorter chosen timescales (for example, 1 hour). An alarm corresponding to each quality violation event is displayed in the **Quality Alarms** tab. The threshold at which quality events are triggered is determined by the configuration of the monitor-queuing-map applied to the interface.
Time in Events	Displays the percentage of three-second intervals which contained at least one quality violation event. A quality violation event may be much shorter than ten seconds, but this will still be counted as a three-second quality violation.
Congestion Indicator	Indicates quality degradation issues in the network. The Congestion Indicator uses millisecond measurements to detect congestion events in the router queues based on the specified quality of service targets and sizing policy. Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and sizing policy that are used to calculate the

	Congestion Indicator. The Congestion Indicator value is a unitless number which reflects the congestion level on a link or class. For a class, it reflects the extent by which the loss and/or delay experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Congestion Indicator value seen on any class on that interface. A Congestion Indicator value greater than 1 means that loss or delay is above an acceptable level, as specified in the BQM configuration. This interface or class is not meeting its quality targets. A Congestion Indicator of less than or equal to 1 means the loss and/or delay are within the specified targets, so this interface or class is meeting its quality targets. Moreover, this means that the sizing policy has been achieved over the selected reporting period. If you have not enabled Congestion Indicator calculation in the monitor-queuing-map being applied to an interface, the status is displayed as 'Not Configured.' Congestion Indicator results are only available for local site outbound and remote site inbound interfaces.

Note Summary results are based on the selected reporting period and do not take recent configuration changes into account. If you have made configuration changes, you need to wait an appropriate period of time before checking for new summary results (for example, wait 24 hours if you want to use the 24-hour reporting period). Alternatively, you can define a custom reporting period to view data only since the configuration change.

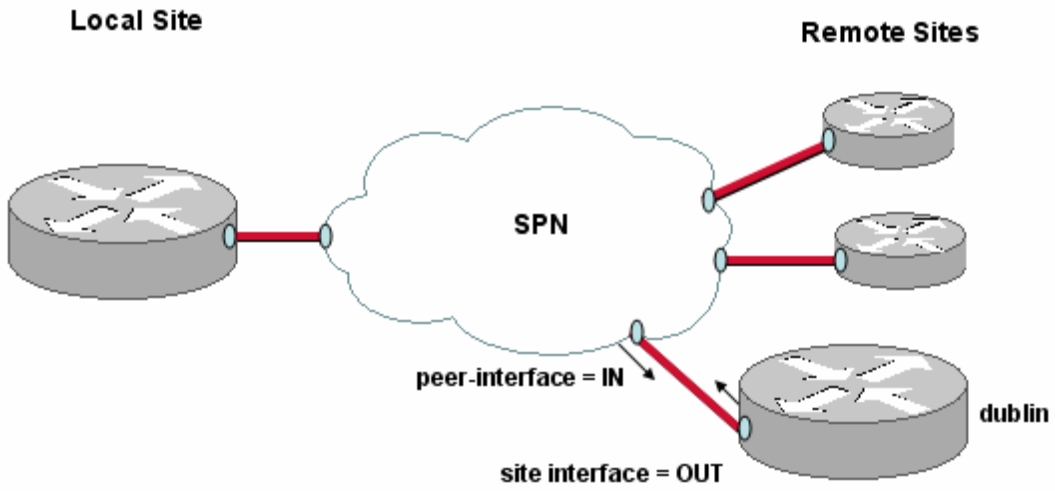
You should wait about ten minutes (that is, after a couple of data updates) following a configuration change before viewing congestion analysis graphs for interfaces.

Each interface entry in the **Congestion Analysis** table can be expanded to display quality events timelines and information for site round trip, interface and class congestion events. Click + beside the interface name to expand an interface.

Notice that although one interface has been configured, there are two interfaces listed: one is labeled with direction 'out' and the other is labeled direction 'in'. If the configuration is based on an MPLS VPN, Internet VPN, Private VPN network model, then each site interface has been configured with a matching peer-interface.

Note The results presented by the BQM are based on the assumption that the device has not dropped packets. You can check this status on the **Quality Alarms** tab. If packets have been dropped then the presented results may not be an accurate reflection of the network traffic.

Figure 4-10: MPLS VPN, Internet VPN, Private VPN Network Model



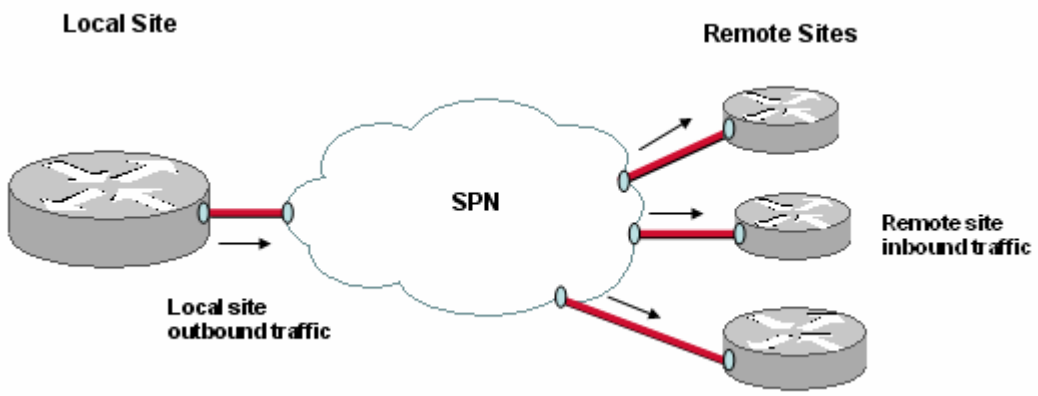
The figure illustrates the network model configuration. For each pair of listed interfaces, the configured interface is labeled with direction ‘out’ and represents traffic outbound from the site to the SPN cloud, and the configured peer- interface is labeled with direction ‘in’ and represents traffic inbound from the SPN cloud to the site.

The BQM features available depend on whether you are looking at the inbound or outbound directions of a given interface. This is directly related to the fact that most BQM features are supported only for traffic that is measured before queuing has occurred (pre-queuing).

In the BQM network model, pre-queuing traffic is represented by the following interfaces:

- Local site interface – outbound
- Remote site interface –inbound

Figure 4-11: Pre-queuing Traffic in the Network Model



Post-queuing traffic is represented by the following interfaces:

- Local site interface – inbound
- Remote site interface – outbound

So, assuming that all BQM features are otherwise enabled in the current configuration, the following information is available for the outbound direction of local site interfaces in and the inbound direction (peer-interface) of remote site interfaces:

- Congestion Indicator values on the **Dashboard**, **Congestion Analysis**, and **Traffic Insight** tabs.
- Corvil Bandwidth, Expected Queuing Delay, Expected Queuing Loss, and Congestion Indicator graphs on the **Congestion Analysis** tab
- Bandwidth Sizing – only pre-queuing interfaces are displayed on the **Bandwidth Sizing** tab

Microburst detection is supported for both local and remote inbound and outbound interfaces.

Selecting a Report Period

By default, the **Congestion Analysis** tab displays summary information for all configured interfaces for the last 24 hours.

Figure 4-12: Reporting Period Selection

You can choose different reporting periods by clicking the **Reporting Period** list. The following reporting periods (and associated update rates) are available:

Last 1 hour – 5 minute updates
Last 12 hours – 5 minute updates
Last 24 hours – 5 minute updates
Last 48 hours – 30 minute updates

Last 7 days – 1 hour updates
Last 30 days - 3 hour updates
Last 60 days – 6 hour updates

The text at the top of the screen indicates the last time at which an update was made.

The screen itself refreshes every five minutes, but new measurements are displayed according to the update rate listed above for each reporting period.

Defining a Custom Report Period

When you are viewing results for an individual interface, you can define a specific custom reporting period for viewing results and generating reports.

To define a custom reporting period, you do the following:

Step 1 Click **select** beside the **From Date** field and choose a date from the calendar.

Step 2 Choose a time from the list of half-hour intervals.

Step 3 Click **select** beside the **To Date** files and choose a date from the calendar.

Step 4 Choose a time from the list of half-hour intervals.

Step 5 Click **View Period**.

When the screen refreshes the displayed information is for the time period you have defined. You can view this information or generate a report for the selected time period. The global **Select Reporting Period** field is set to Custom Period.

Sorting the Congestion Analysis Table

The **Congestion Analysis** table is sorted by the **Congestion Indicator** column by default, but you can sort this table by any column. Click the heading of the column by which you want to sort. The information in the table is then arranged from highest to lowest according to that column. You can click again to reverse the order of the sort and display results from lowest to highest.

For example, to view interfaces that have the highest calculated Congestion Indicator values, you click the **Congestion Indicator** column heading to sort. The summary is rearranged according to the maximum measured microburst values per interface, with the highest value first. Click the **Congestion Indicator** column heading again to sort the summary screen again, this time with the lowest measured Congestion Indicator value first.

Filtering the Congestion Analysis Table

You can use the search facility on the **Congestion Analysis** table to display a particular interface or set of interfaces of interest. Enter the name of the required interface, or part of the name to match a group of interfaces and click **Filter**. To clear the filter text field and return to the default display of results, click **Clear**.

For example, entering 'Serial' will display all interfaces whose full names (site – router – interface – direction) contain the word 'Serial' or 'serial'.

The **Congestion Analysis** tab also provides the option to filter results based on Congestion Indicator values. Click beside the **Congestion Indicator** column heading and select an option from the list. The screen will refresh, displaying only the results relevant to the filtering option you selected.

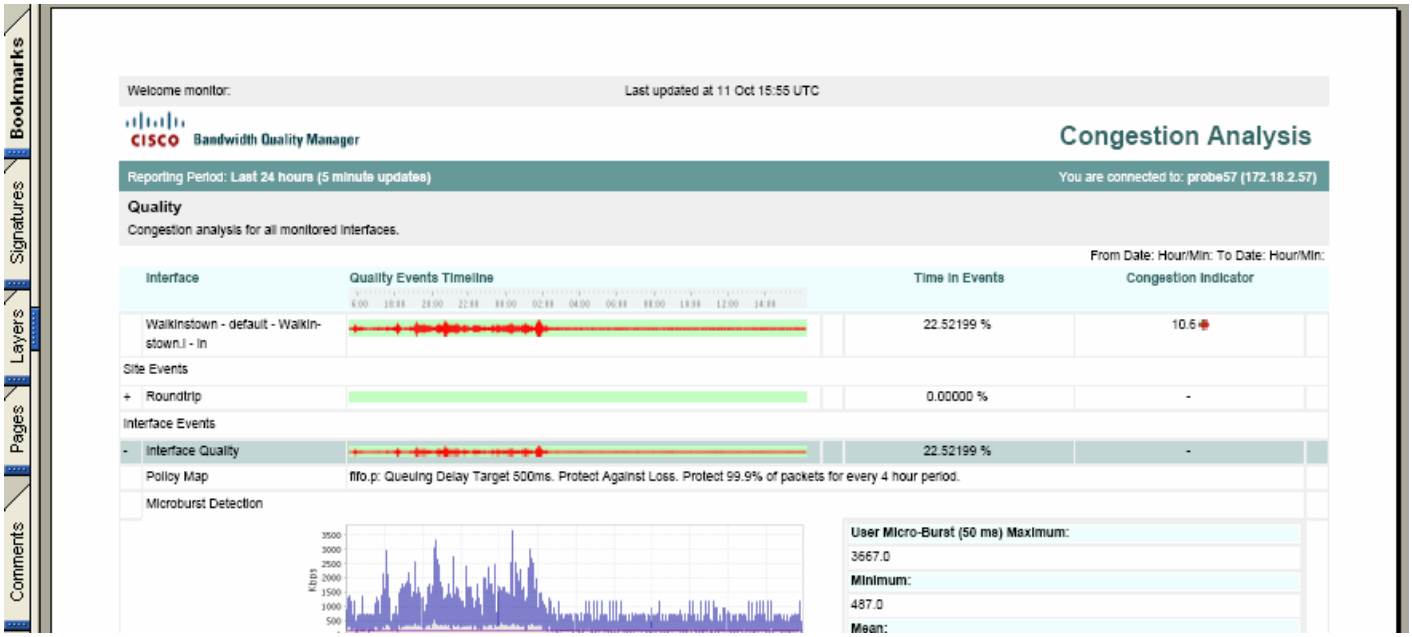
Reporting Congestion Analysis Results

You can generate a report in .pdf format at any point when viewing congestion analysis results.

To generate a report, click .

The generated report is available for download in .pdf format. Reports are not stored on the BQM.

Figure 4-13: Congestion Analysis Report



The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all outbound interfaces sorted by decreasing Congestion Indicator value over the last 48 hours. If the original results are displayed across multiple pages onscreen, then you use the View All option so that the report contains the data from all such screens. Otherwise the report will present the results displayed on the current screen only.

The time displayed at the top of each report is the configured time zone of the BQM.

Viewing Interface and Class Congestion

Click the linked interface name in the **Congestion Analysis** table to get access to graph information for site round trip, interface and class congestion events. Each interface will have at least one class, class-default, configured.

When you are viewing results for an individual outbound interface, you click **View Inbound** to view results for the inbound direction. Likewise, you can switch to viewing outbound results if you open the inbound interface information.

You can switch to the traffic statistics and bandwidth sizing results for the interface by clicking the relevant link from **Related Links**.

You can also define a custom reporting period for viewing interface results. See “Selecting a Report Period” for more information.

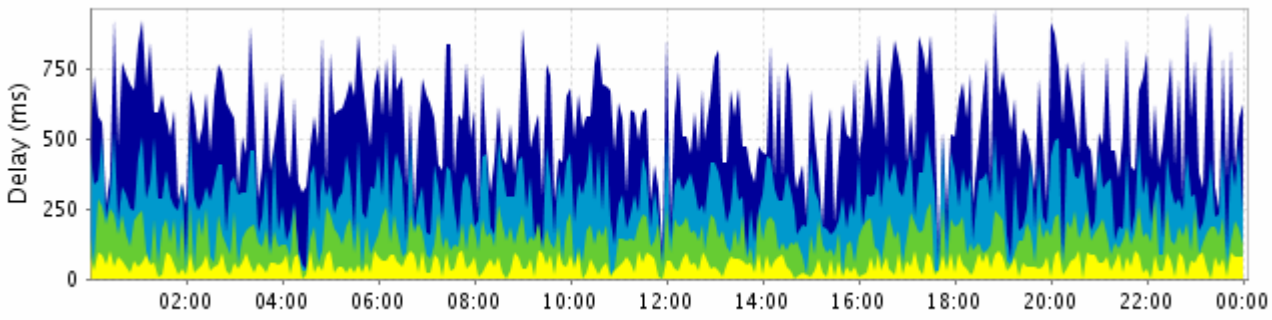
Viewing Round Trip Delay and Loss

When you expand site events, the graphs available for site round trip events are as follows:

- End-to-end delay
- End-to-end loss

The end-to-end delay graph plots the delay measured for a round trip between the chosen remote site and the local site by ICMP ping packets. The delay is displayed as a series of millisecond measurements for each packet sent on the round trip.

Figure 4-14: End-to-End Delay Results



The graph legend indicates the colors used to display the following:

Delay Threshold - indicates the value of the delay threshold configured in the monitor-end-to-end-map being applied.
Max - displays the maximum round trip time (in milliseconds) per ICMP ping packet each five minutes during the chosen reporting period.
x% - displays the x^{th} percentile of round trip times in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.

Mean – displays the mean of the round trip times for each five minutes during the chosen reporting period
Min – displays the minimum round trip time per ICMP ping packet each five minutes during the chosen reporting period.

The end-to-end loss graph plots the packet loss measured during a round trip between the chosen remote site and the local site by ICMP ping packets. The packet loss is displayed as a percentage of the total packets sent on the round trip.

Figure 4-15: End-to-End Loss Results

End-to-end delay and loss measurement is enabled, and its characteristics defined, in the monitor-end-to-end-map applied to the interface. Both graphs are available for remote sites only.

In both cases, configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

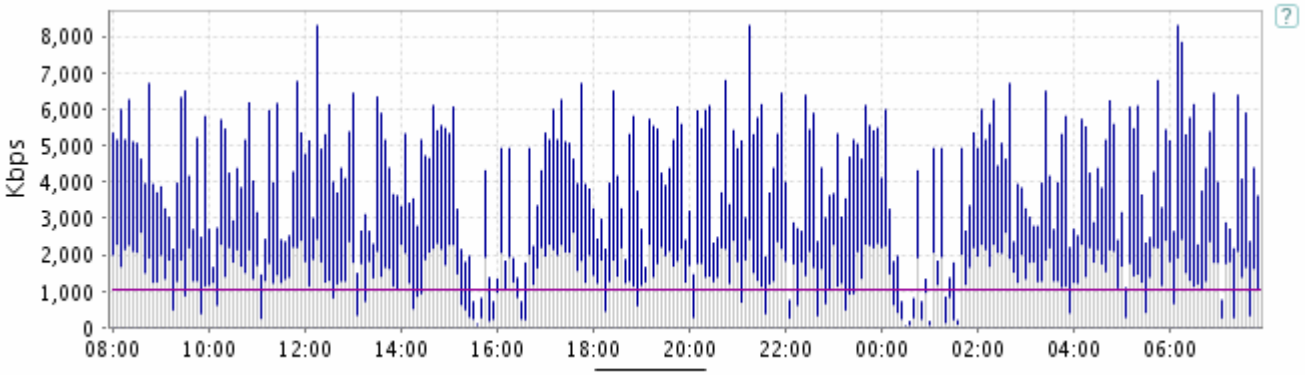
The end-to-end delay and loss plots enable you to evaluate end-to-end performance. This can complement the local queuing delay results displayed in other graphs. For example, if the end-to-end graphs show performance problems but the simulation of local queuing does not, then the problem is most likely in the service provider cloud.

Viewing Interface Microburst and Congestion Indicator Measurements

When you expand interface quality events, the Microburst Detection and Congestion Indicator graphs are displayed.

The Microburst Detection graph displays measured peak bit rates at a configurable millisecond-level resolution.

Figure 4-16: Microburst Detection



The legend below the graph identifies the color of each plotted line. The graph displays the measured peak rate based on:

- one-second measurement
- the timescale resolution configured in the monitor-queuing-map for measuring microbursts (for example, 50 ms)

The threshold configured in the monitor-queuing-map for triggering event detection on microbursts (for example, 1000 kpbs on a 1024 kbps link) is indicated on the graph, as is the capacity of the link.

So two of the plotted quantities are determined by the monitor-queuing-map being applied to the interface of interest. If you have configured specific values in each case, then these configured values form the basis for the plots you now see. Otherwise the default monitor-queuing-map values are used.

Note Under certain conditions it is possible to see higher peak values measured for larger millisecond resolutions than for smaller ones. For example, let's say you have configured a queuing delay target of 500ms and a microburst peak measurement resolution of 400ms. If traffic arrives in separate groups of packets, separated by any more than 400ms, the 400ms peak estimate does not account for two of these groups of packets, whereas the 500ms does. So, the 500ms peak measurement turns out to be greater than the 400ms peak.

This effect is more common if you have shape detection turned off. Let's say we have packets spaced by 450ms. Then the 500ms 'raw' peak will see 2 packet in 500ms, and the 400ms 'raw' peak will see 1 packet in 400ms. Hence, the 500ms raw peak will exceed the 400ms one. The effect is rarer when you have shape detection enabled, because you need to have groups of more than one packet, but, as described above, it is still possible.

If the traffic is perfectly smooth (that is, it is transmitting at a constant bit rate) then all three measurements listed above will be the same. The more bursty the traffic, the more variation there will be between these measurements. This can help you understand why an application that looks like it has very low bandwidth requirements on average may actually be causing drops in the network when it transmits very sharp short spikes.

The Congestion Indicator graph displays the values calculated every five minutes during the selected reporting period.

Note The summary Congestion Indicator value presented for the interface is based on the busy period configured in the monitor-queuing-map sizing policy. If the configured busy period is greater than five minutes, then you may see 5-minute values in the graph that exceed the displayed summary value.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets that are used to calculate and display the plotted data for each graph. For more information, see the "Configuring QoS Monitoring Features" section of the "Configuring BQM QoS Monitoring" chapter.

Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Viewing Class Measurements

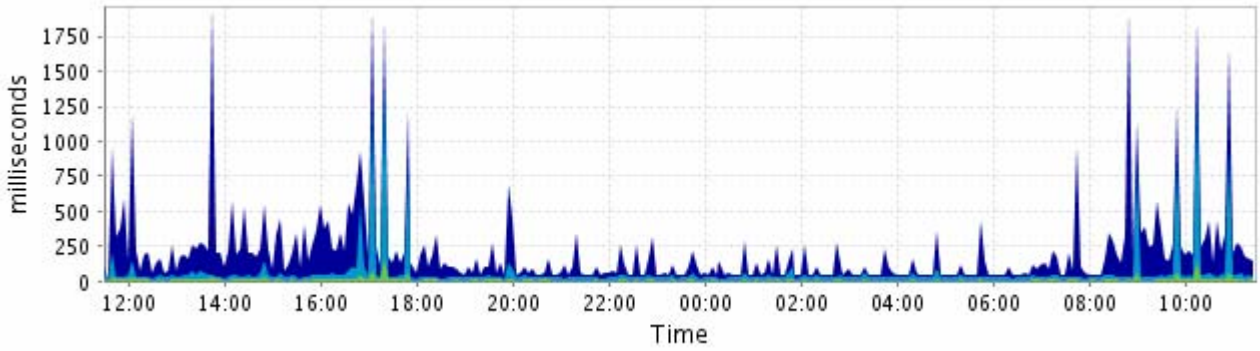
When you expand a class from the list, the relevant graphs and charts are available to view for the chosen class. The graphs available for class events are as follows:

- Expected queuing delay
- Expected queuing loss
- Microburst detection
- Congestion Indicator
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length

Expected Queuing Delay

The expected queuing delay graph plots the per-packet delay calculated by the BQM using a simulation of the chosen class traffic. The expected queuing delay is displayed as a series of millisecond values for each five minutes during the reporting period.

Figure 4-17: Expected Queuing Delay Results



The expected queuing delay calculation is made for every packet in the chosen class measured by the BQM. Then for each five-minute period, the maximum, configured percentile, mean and minimum values are plotted. The graph legend indicates the colors used to display each:

Max - displays the maximum of the expected delay values (in milliseconds) calculated each five minutes during the chosen reporting period.
x% - displays the x^{th} percentile of expected delay values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean – displays the mean of the expected delay values for each five minutes during the chosen reporting period
Min – displays the minimum of the expected delay values for each five minutes during the chosen reporting period.

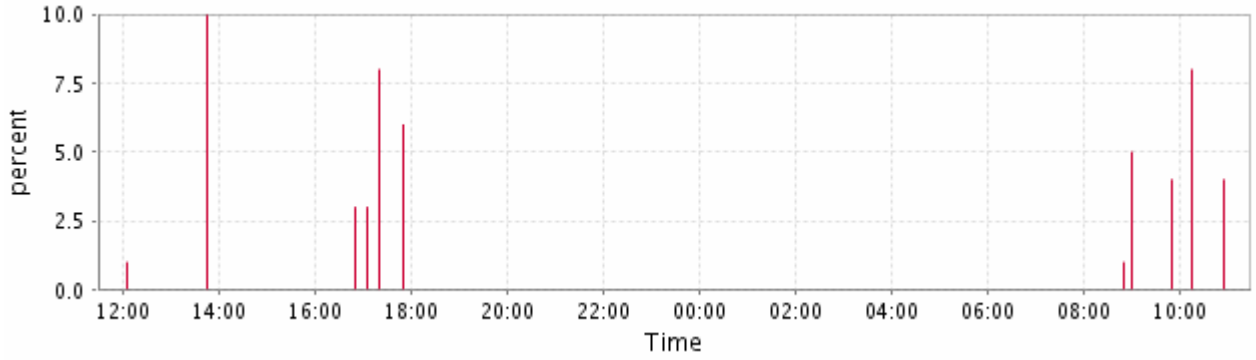
Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Expected Queuing Loss

The expected queuing loss graph plots the expected packet loss due to queue buffer overflow calculated by the BQM using a simulation of the chosen class traffic. The expected queuing loss is displayed as a percentage of the total packets measured by the BQM.

Figure 4-18: Expected Queuing Loss Results



Loss estimation is enabled, and its characteristics defined, in the monitor-queuing-map applied to the interface.

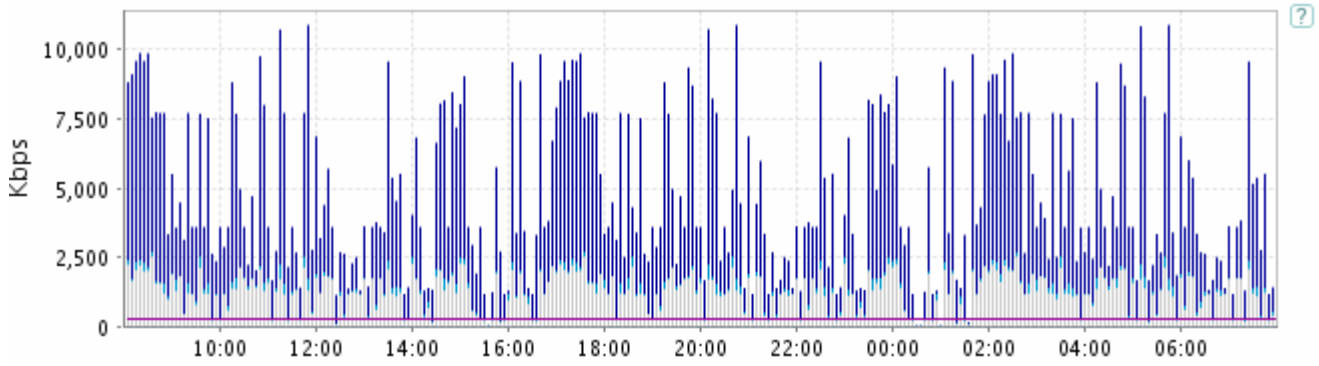
Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Microburst Detection

The Microburst Detection graph displays measured peak bit rates for the class traffic at a configurable millisecond-level resolution.

Figure 4-19: Microburst Results



The legend below the graph identifies the color of each plotted line. The graph displays the measured peak rate based on:

- one-second measurement
- (for classes only) the millisecond timescale configured in the monitor-queuing-map queuing targets for delay (for example, 500 ms)
- the timescale resolution configured in the monitor-queuing-map for measuring microbursts (for example, 50 ms)

The threshold configured in the monitor-queuing-map for triggering event detection on microbursts (for example, 1000 kpbs on a 1024 kbps link) is indicated on the graph, as is the capacity of the link.

So three of the plotted quantities are determined by the monitor-queuing-map being applied to the interface of interest. If you have configured specific values in each case, then these configured values form the basis for the plots you now see. Otherwise the default monitor-queuing-map values are used.

Note Under certain conditions it is possible to see higher peak values measured for larger millisecond resolutions than for smaller ones. For example, let's say you have configured a queuing delay target of 500ms and a microburst peak measurement resolution of 400ms. If traffic arrives in separate groups of packets, separated by any more than 400ms, the 400ms peak estimate does not account for two of these groups of packets, whereas the 500ms does. So, the 500ms peak measurement turns out to be greater than the 400ms peak.

This effect is more common if you have shape detection turned off. Let's say we have packets spaced by 450ms. Then the 500ms 'raw' peak will see 2 packet in 500ms, and the 400ms 'raw' peak will see 1 packet in 400ms. Hence, the 500ms raw peak will exceed the 400ms one. The effect is rarer when you have shape detection enabled, because you need to have groups of more than one packet, but, as described above, it is still possible.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and threshold that are used to calculate and display the plotted data. For more information, see the “Configuring QoS Monitoring Features” section of the “Configuring BQM QoS Monitoring” chapter.

Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

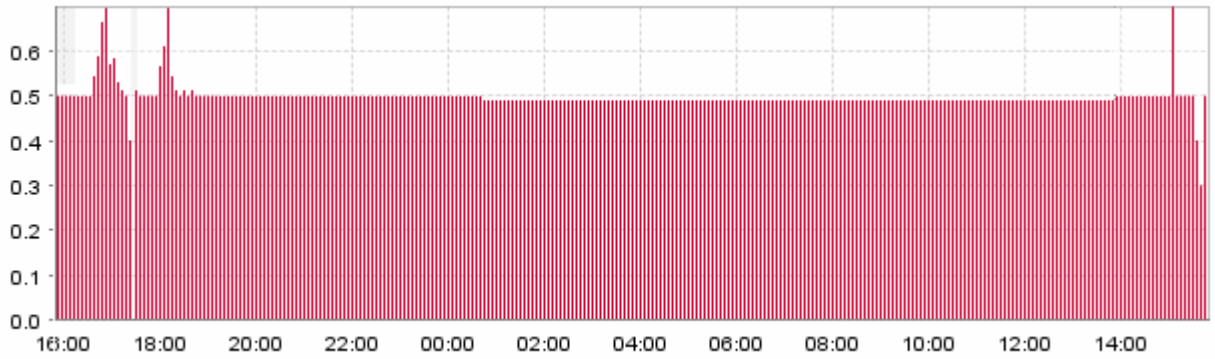
Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

If the class traffic is perfectly smooth (that is, it is transmitting at a constant bit rate) then all three measurements listed above will be the same. The more bursty the traffic, the more variation there will be between these measurements. This can help you understand why an application that looks like it has very low bandwidth requirements on average may actually be causing drops in the network when it transmits very sharp short spikes.

Congestion Indicator

The Congestion Indicator graph plots the 5-minute values calculated by the BQM for chosen class traffic during the selected reporting period.

Figure 4-20: Congestion Indicator Results



Note The summary Congestion Indicator value presented for the class is based on the busy period configured in the monitor-queuing-map sizing policy. If the configured busy period is greater than five minutes, then you may see 5-minute values in the graph that exceed the displayed summary value.

The plotted values are based on the queuing targets configured in the monitor-queuing-map being applied to the interface of interest. If you have configured specific values in each case, then these configured values form the basis for the Congestion Analysis calculations you now see. Otherwise the default monitor-queuing-map values are used.

Use the **Monitor QueuingMaps** menu in **System Administration** mode to set the quality targets that are used to calculate and display the plotted data. For more information, see the "Configuring QoS Monitoring Features" section of the "Configuring BQM QoS Monitoring" chapter.

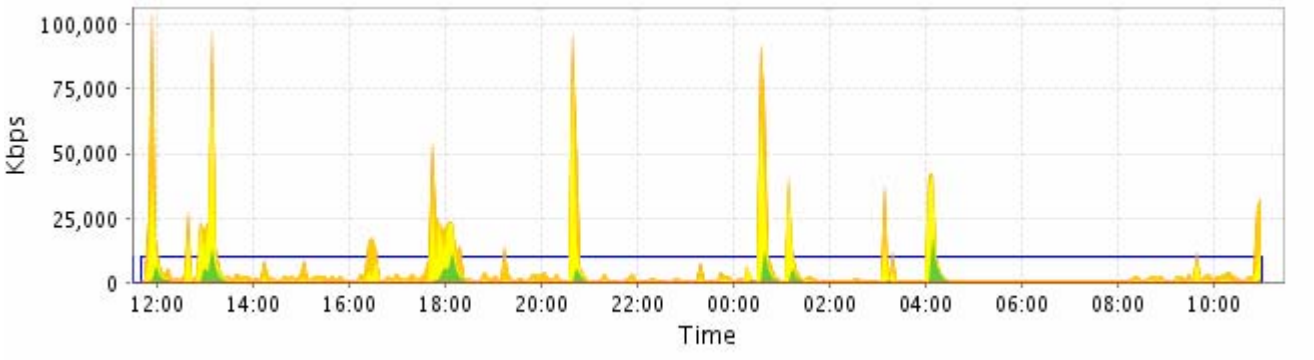
Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Corvil Bandwidth – Delay

The Corvil Bandwidth graph for delay plots the bandwidth required to meet the configured delay target for the chosen class. The delay target is configured in the monitor-queuing-map that is applied to the class. For example, if the configured delay target is 150 ms, then the graph displays the bandwidth required to ensure that no packet in the class traffic is delayed by more than 150 ms.

Figure 4-21: Corvil Bandwidth Delay Results



The Corvil Bandwidth values are displayed as a series of values in kbps for each five minutes during the reporting period. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated each five minutes during the chosen reporting period.
x% - the x^{th} percentile of Corvil Bandwidth values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean – the mean of the Corvil Bandwidth values for each five minutes during the chosen reporting period
Min –the minimum of the Corvil Bandwidth values for each five minutes during the chosen reporting period.

The threshold configured in the monitor-queuing-map for triggering event detection based on the Corvil Bandwidth delay value is indicated on the graph, as is the capacity of the link.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and threshold that are used to calculate and display the plotted data. For more information, see the "Configuring QoS Monitoring Features" section of the "Configuring BQM QoS Monitoring" chapter.

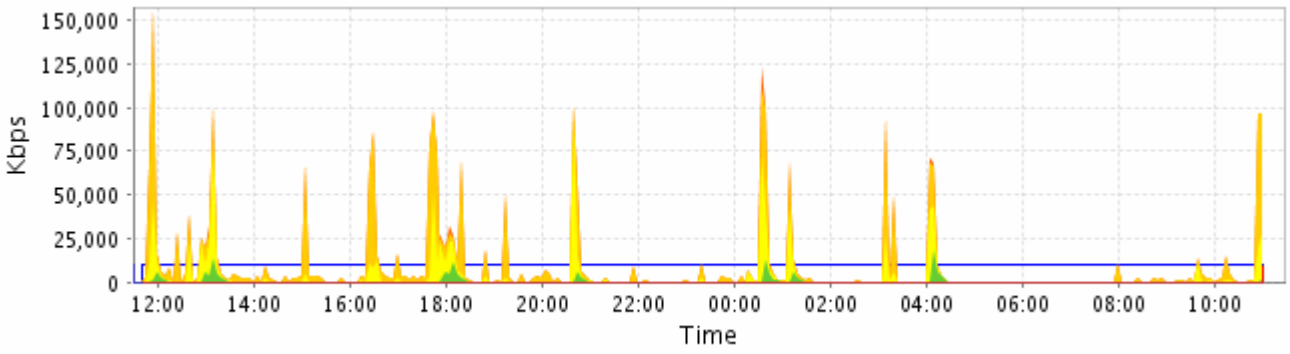
Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Corvil Bandwidth – Queue Length

The Corvil Bandwidth graph for queue length plots the bandwidth required to avoid packet loss due to queue buffer overflow. The queue length is defined as an attribute of the class in the BQM configuration. For example, if the queue length configured for the class is 64 packets, then the graph displays the bandwidth required to prevent the queue for the class traffic building up past 64 packets.

Figure 4-22: Corvil Bandwidth Queue Length Results



The graph displays a series of Corvil Bandwidth values (in kbps) for each five minutes during the chosen reporting period. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated each five minutes during the chosen reporting period.
x% - the x^{th} percentile of Corvil Bandwidth values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean –the mean of the Corvil Bandwidth values for each five minutes during the chosen reporting period
Min –the minimum of the Corvil Bandwidth values for each five minutes during the chosen reporting period.

The threshold configured in the monitor-queuing-map for triggering event detection based on the Corvil Bandwidth delay value is indicated on the graph, as is the capacity of the link.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and threshold that are used to calculate and display the plotted data. For more information, see the “Configuring QoS Monitoring Features” section of the “Configuring BQM QoS Monitoring” chapter.

Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Viewing Priority Class Results

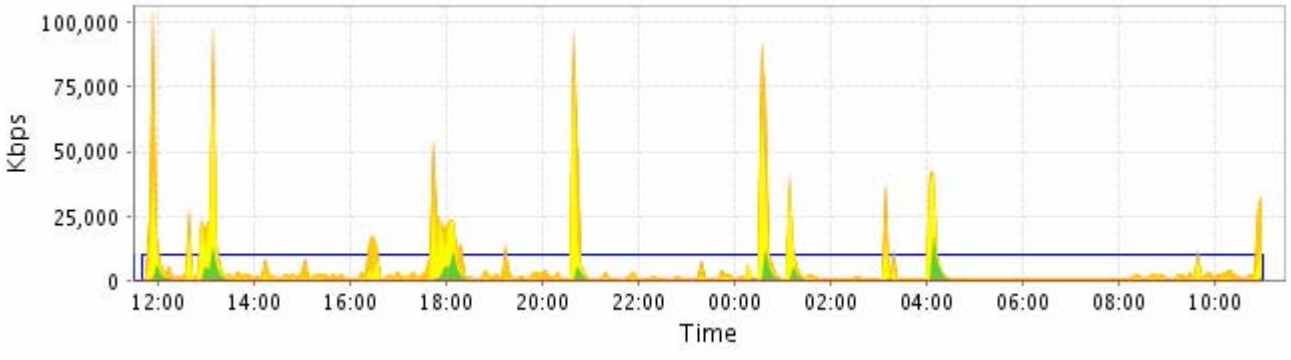
If you have configured a multiclass policy-map and assigned priority to one of the classes, such as the voice class, you can view results for the priority class.

Corvil Bandwidth - Priority

The Corvil Bandwidth - Priority graph plots the bandwidth required to avoid policer packet drops for the configured priority class traffic.

If the configured priority burst-size in bytes is smaller than a packet size, then the Corvil Bandwidth for that packet is not well defined, because changing the priority bandwidth cannot, on its own, prevent policer drop. Should this happen, the Corvil Bandwidth value will jump to a very large value. In such cases, you can examine the packet size distribution on the **Traffic Insight** screen to help choose an appropriate priority burst-size.

Figure 4-23: Corvil Bandwidth Priority Results



The graph is displayed as a series of kbps values for each five minutes during the reporting period. For each five-minute period, the maximum, configured percentile, mean and minimum values are plotted:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated each five minutes during the chosen reporting period.
xth percentile - the xth percentile of Corvil Bandwidth values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean - the mean of the Corvil Bandwidth values for each five minutes during the chosen reporting period
Min - the minimum of the Corvil Bandwidth values for each five minutes during the chosen reporting period.

The threshold configured in the monitor-queuing-map for triggering event detection based on the Corvil Bandwidth value is indicated on the graph, as is the capacity of the link.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and thresholds that are used to calculate and display the plotted data. For more information, see “Configuring QoS Monitoring Features.”

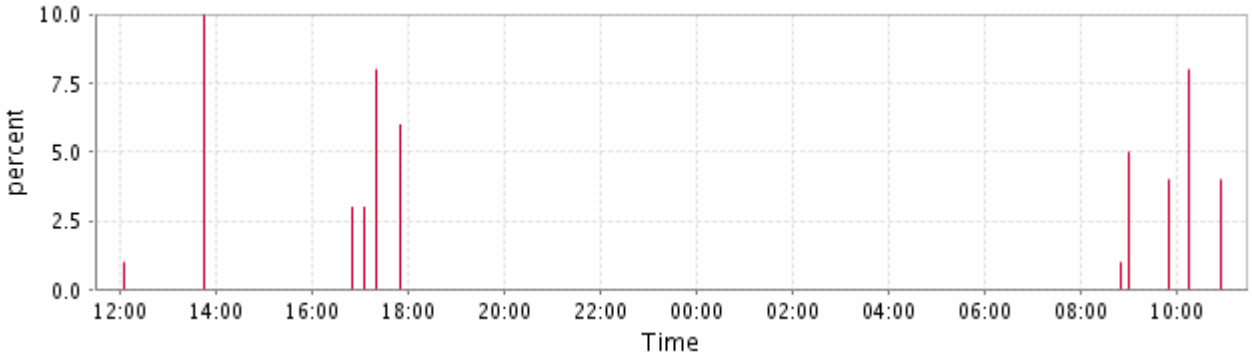
Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Expected Priority Drops

The expected priority drops graph plots the expected level of packet drops due to the action of a configured policer. The result is calculated by the BQM using a simulation based on the chosen class traffic.

Figure 4-24: Expected Priority Drop Results

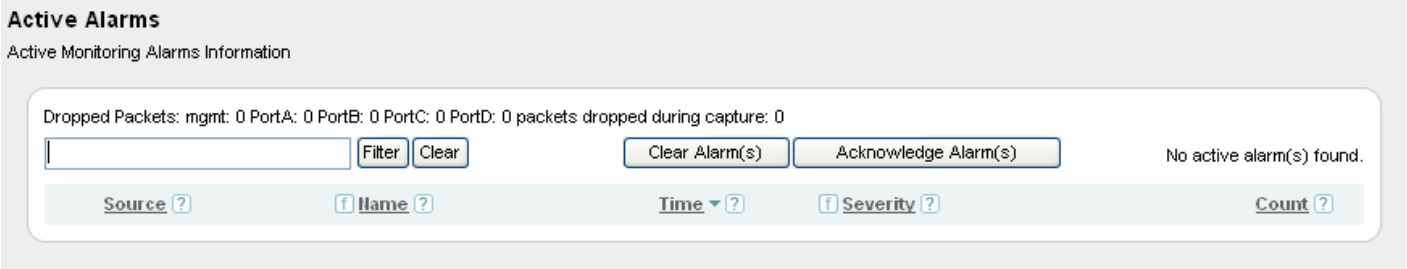


Priority drop estimation is enabled, and its characteristics defined, in the monitor-queuing-map applied to the interface.

Monitoring Quality Alarms

By default the **Quality Alarms** tab lists all active alarms triggered due to quality events in the network. Click the **Cleared Alarms** link to view the list of cleared alarms during the chosen reporting period. The summary table information is sorted by the time of the alarm. You can sort the active and cleared alarm information by column and you can drill into each alarm to view related graph data.

Figure 4-25: Quality Alarms



Note The **Quality Alarms** tab includes information about the status of dropped packets for the device, if any. The information shown here is independent of the selected reporting period. The results presented by the BQM are based on the assumption that the device has not dropped packets. If packets have been dropped then the presented results on other screens may not be an accurate reflection of the network traffic.

By default, twenty active or cleared alarms are displayed per page and if there are more than twenty alarms displayed, you use the links at the bottom of the list to navigate between pages of results. If there are many active or cleared alarms, you can also click the **View 50**, **View 100**, or **View All** links to display the corresponding number of alarms on a single page. In these cases you scroll down the page to view all the presented results.

The following table describes the information displayed in the quality alarms table:

Table 4-2: Quality Alarms Table

Column	Description
Source	Displays the full, qualified name identifying the interface or class for which the alarm was triggered: *site name – router name – interface name – direction – class name*.
Time	Displays the time at which the active alarm triggered, or at which a cleared alarm was cleared.
Name	Displays the type of quality alarm that has been triggered.

Severity	Displays the severity of the alarm. The severity levels for SNMP traps are the following: Informational – events that require notification but do not cause failures Warning – typically used for thresholds that warn of an impending failure Minor – not used for defaults Major – an event that has the potential to make the system no longer operational Severe – system no longer operational
Count	The system event detection mechanism can result in many triggers. To avoid flooding the system with alarms, these event triggers are coalesced into a single displayed alarm. This number displays the accumulated number of alarm triggers that contribute to a given reported alarm since the alarm last cleared. The count accumulates every five minutes up to a thirty-minute limit. If an alarm clears and then become active again within thirty minutes of clearing, the count for the alarm continues to accumulate. If the alarm clears and then activates again more than 30 minutes later, the count for the alarm resets.
Acknowledge	Check the check box to acknowledge an active alarm.

The following table describes the alarm types that may be displayed on the **Quality Alarms** tab:

Table 4-3: Alarm Types

Alarm Type	Description
Congestion Indicated	The Congestion Indicator crossed the configured threshold.
Corvil Bandwidth Threshold Exceeded	The Corvil Bandwidth measurement indicates the class bandwidth threshold has been exceeded.
E2E Loss Detected	Packets have been lost during end-to-end measurement.
Expected Policing Threshold Exceeded	The Expected Policing value crossed the configured threshold.
Expected Queuing Depth Threshold Exceeded	The Expected Queuing Depth crossed the configured threshold.
Expected Queuing Loss Threshold Exceeded	The Expected Queuing Loss crossed the configured threshold.
Microburst Detected	Microbursts exceeding the configured bandwidth threshold have been detected.

Sorting the Quality Alarms Table

The **Quality Alarms** table is sorted by the **Time** column by default, but you can sort this table by any column. Click the heading of the column by which you want to sort. The information in the table is then arranged from highest to lowest according to that column. You can click again to reverse the order of the sort and display results from lowest to highest.

For example, to view alarms with the highest severity rating, you click the **Severity** column heading to sort. The summary is rearranged according to the severity of alarms, with the highest severities first. Click the **Severity** column heading again to sort the summary screen again, this time with the lowest severities first.

Filtering the Quality Alarms Table

You can use the search facility on the **Quality Alarms** tab to display a particular alarm or set of alarms of interest. Enter the name of the required source, or part of a name to match a group of sources, and click **Filter**. To clear the filter field text and return to the default display of alarms, click **Clear**.

For example, entering 'Serial' will display all sources whose full names (site – router – interface – direction) contain the word 'Serial' or 'serial'.

The **Quality Alarms** tab also provides the option to filter results based on the type or severity of active or cleared alarms. Click the filter symbol beside the **Name** or **Severity** column headings and select an option from the list. The screen will refresh, displaying only the results relevant to the filtering option you selected.

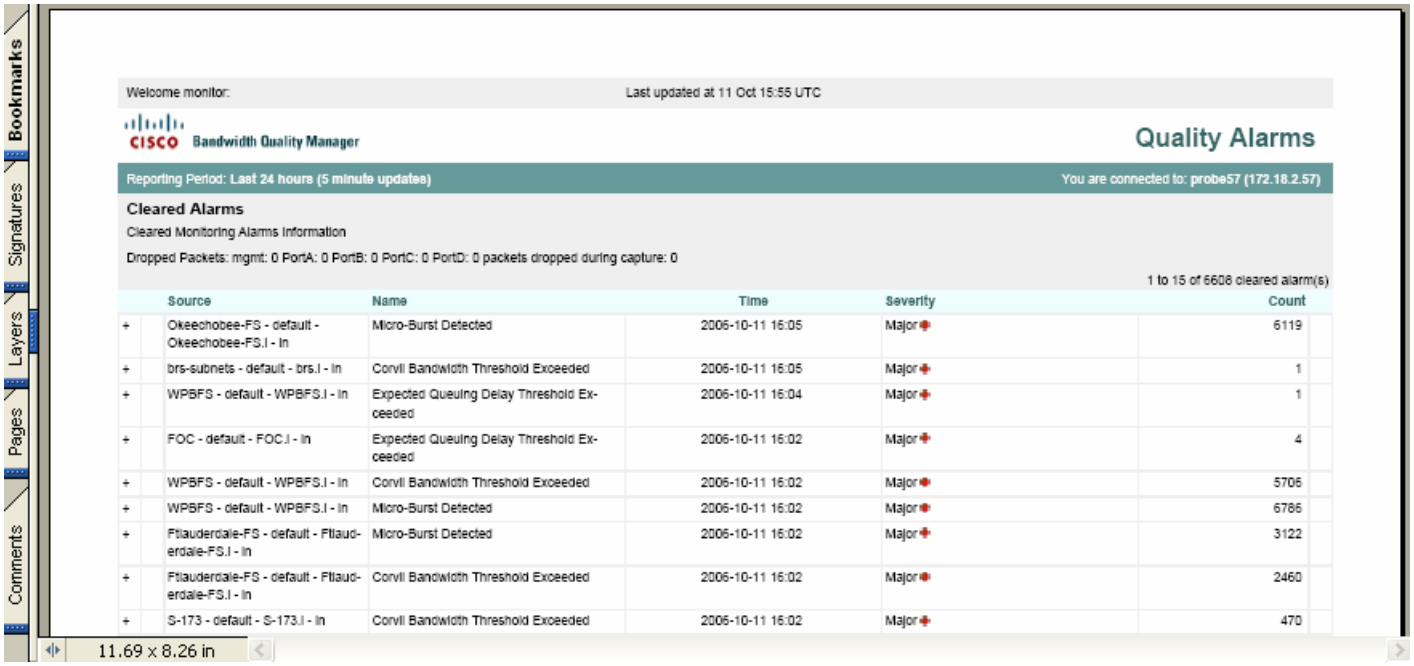
Generating a Quality Alarms Report

You can generate a report in .pdf format at any point when viewing active or cleared alarms.

To generate a report, click .

The generated report is available for download in .pdf format. Reports are not stored on the BQM.

Figure 4-26: Quality Alarms Report



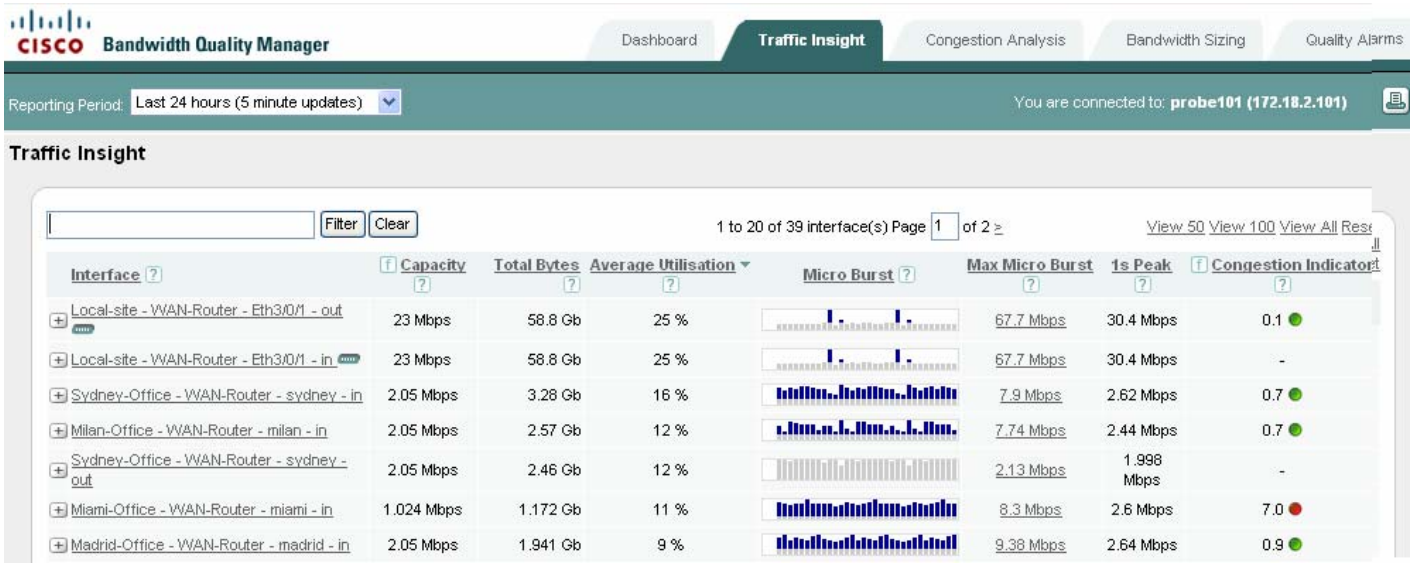
The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all cleared major alarms sorted by time over the last hour. The report presents the results displayed on the current screen only.

The time displayed at the top of each report is the configured time zone of the BQM.

Monitoring Traffic Insight Results

By default the **Traffic Insight** tab lists all of the interfaces you have configured in the BQM network model. The summary table information is sorted by interface name and provides a variety of statistics (such as maximum microburst and Congestion Indicator) for each of these interfaces.

Figure 4-27: Traffic Insight Results



You can choose from a predefined list of reporting periods up to 60 days or define a custom reporting period over which to view data. You can also sort the summary information by column and you can drill into each interface to view more details (such as class statistics and top applications). This enables you to identify the information you need.

Note The results presented by the BQM are based on the assumption that the device has not dropped packets. You can check this status on the **Quality Alarms** tab. If packets have been dropped then the presented results may not be an accurate reflection of the network traffic.

Traffic Insight Overview

By default, results for twenty interfaces are displayed per page and if there are more than twenty interfaces configured, you use the links at the bottom of the list to navigate between pages of results. If you have many interfaces configured, you can also click the **View 50**, **View 100**, or **View All** links to display the corresponding number of interfaces on a single page. In these cases you scroll down the page to view all the presented results.

The following table describes the information displayed in the traffic statistics summary table:

Table 4-4: Traffic Insight Summary Table

Column	Description
Interface	Displays the full qualified name of the configured interface (site name – router name – interface name – direction). Using the BQM network model, the direction of traffic is always represented from the perspective of a site. In the case of MPLS VPN, Internet VPN, Private VPN deployments this means that for each interface and peer interface pair configured in the network model, the configured interface represents the outbound traffic from the site (local or remote) and the peer-interface represents the inbound traffic to the site (local or remote).
Capacity	Displays the configured capacity of the interface.
Total Bytes	Displays the total number of bytes passing the interface during the chosen reporting period.
Average Utilization	Displays the average utilization of the interface bandwidth during the chosen reporting period as a percentage of the configured interface capacity.
Micro Burst	Displays a graphical representation of microburst measurements that indicates whether significant bursts have been detected.
Max Micro Burst	Displays the maximum measured microburst size during the chosen reporting period. Roll over the displayed value to see the date and time at which the maximum value was measured.
1 sec Peak	Displays the maximum measured one-second peak value during the chosen reporting period. Comparing this value with the Max Micro Burst value will give you an indication of the extent to which the traffic has experienced millisecond level bursts that would not have been 'seen' with one-second measurements.
Congestion Indicator	Indicates quality degradation issues in the network. The Congestion Indicator uses millisecond measurements to detect congestion events in the router queues based on the specified quality of service targets and sizing policy. Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and sizing policy that are used to calculate the Congestion Indicator. The Congestion Indicator value is a unitless number which reflects

	the congestion level on a link or class. For a class, it reflects the extent by which the loss and/or delay experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Congestion Indicator value seen on any class on that interface. A Congestion Indicator value greater than 1 means that loss or delay is above an acceptable level, as specified in the BQM configuration. This interface or class is not meeting its quality targets. A Congestion Indicator of less than or equal to 1 means the loss and/or delay are within the specified targets, so this interface or class is meeting its quality targets. Moreover, this means that the sizing policy has been achieved over the selected reporting period. If you have not enabled Congestion Indicator calculation in the monitor-queuing-map being applied to an interface, the status is displayed as 'Not Configured.' Congestion Indicator results are only available for local site outbound and remote site inbound interfaces.

Selecting a Report Period

By default, the **Traffic Insight** tab displays summary information for all configured interfaces for the last 24 hours. You can choose different reporting periods by clicking the **Reporting Period** list. The following reporting periods (and associated update rates) are available:

Last 1 hour – 5 minute updates
Last 12 hours – 5 minute updates
Last 24 hours – 5 minute updates
Last 48 hours – 30 minute updates
Last 7 days – 1 hour updates
Last 30 days - 3 hour updates
Last 60 days – 6 hour updates

The text at the top of the screen indicates the last time at which an update was made. The screen itself refreshes every minute, but new measurements are displayed according to the update rate listed above for each reporting period.

Defining a Custom Report Period

When you are viewing results for an individual interface, you can define a specific custom reporting period for viewing results and generating reports. To define a custom reporting period, you do the following:

Step 1 Click **select** beside the **From Date** field and choose a date from the calendar.

Step 2 Choose a time from the list of half-hour intervals.

Step 3 Click **select** beside the **To Date** files and choose a date from the calendar.

Step 4 Choose a time from the list of half-hour intervals.

Step 5 Click **View Period**.

When the screen refreshes the displayed information is for the time period you have defined. You can view this information or generate a report for the selected time period. The global **Select Reporting Period** field is set to Custom Period. If you click the **Related Links** for the interface, the defined custom period is used to display the related interface information.

Sorting the Traffic Insight Table

The **Traffic Insight** table is sorted by the **Interface Name** column, but you can sort this table by any column. Click the heading of the column by which you want to sort. The information in the table is then arranged from highest to lowest according to that column. You can click again to reverse the order of the sort and display results from lowest to highest. For example, to view interfaces that have been most impacted by millisecond traffic burst, you select the **Max Micro Burst** column heading. The summary is rearranged according to the maximum measured microburst values per interface, with the highest value first. Click the **Max Micro Burst** column heading again to sort the summary screen again, this time with the lowest measured maximum microburst value first.

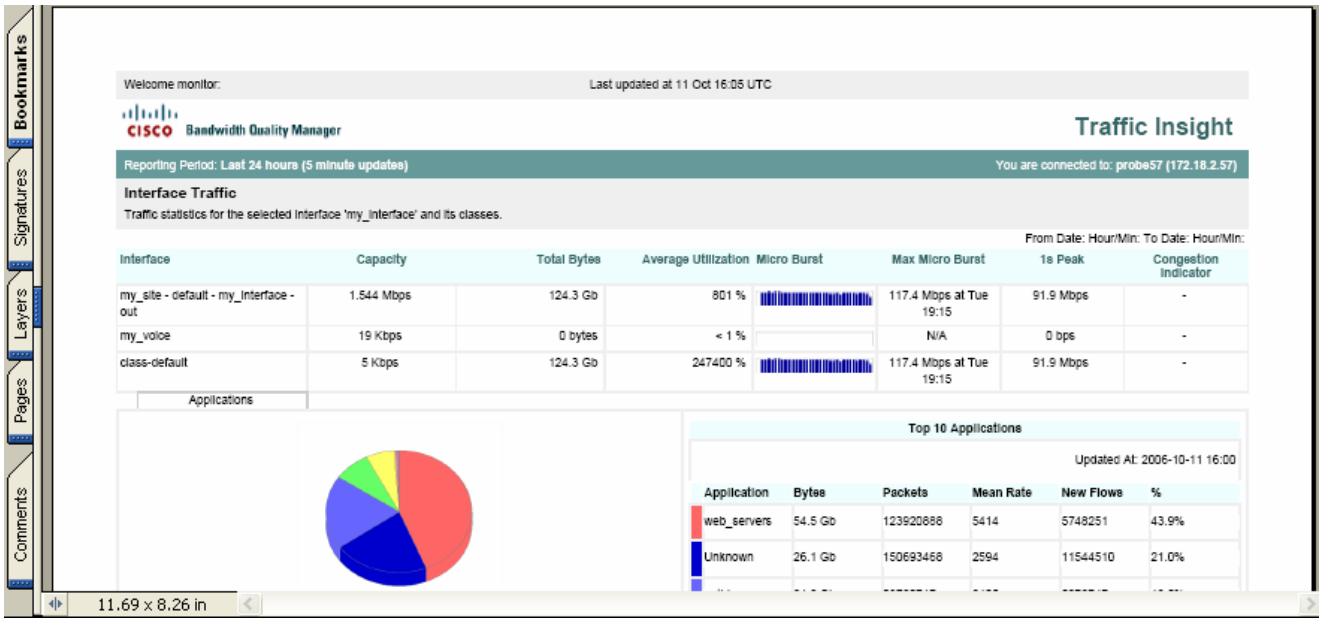
Filtering the Traffic Insight Table

You can use the search facility on the **Traffic Insight** table to display a particular interface or set of interfaces of interest. Enter the name of the required interface, or part of a name to match a group of interfaces, and click **Filter**. To clear the filter field text and return to the default display of results, click **Clear**. For example, entering ‘Serial’ will display all interfaces whose names contain the word ‘Serial’ or ‘serial’. Interfaces containing the word ‘serial’ will not be returned. The **Traffic Insight** tab also provides the option to filter results based on interface capacity or Congestion Indicator values. Click the filter symbol beside the **Capacity** or **Congestion Indicator** column headings and select an option from the list. The screen will refresh, displaying only the results relevant to the filtering option you selected.

Reporting Traffic Statistic Results

You can generate a report in .pdf format at any point when viewing congestion analysis results. To generate a report, click . The generated report is available for download in .pdf format. Reports are not stored on the BQM.

Figure 4-28: Traffic Insight Report



The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all outbound 2 Gbps interfaces sorted by decreasing Congestion Indicator value over the last 24 hours.
If the original results are displayed across multiple pages onscreen, then the report contains the data from all such screens in the order they were displayed at the time the report was generated.

The time displayed at the top of each report is the configured time zone of the BQM.

When a large report is being generated, the system issues a warning indicating that the action may take some time to complete.

Viewing Summary Interface Statistics

Each interface entry in the **Traffic Insight** table can be expanded to display micro congestion measurement plots and pie charts for top applications and top conversations for the selected reporting period. Click + beside the interface name to expand an interface.

You can change the reporting period when the interface details are being displayed to view the relevant plots and charts for the chosen period. The available interface summary information is as follows:

- Microburst detection graph
- Top applications chart
- Top conversations chart

For more information on the graphs and charts, see the following section “Viewing Interface and Class Statistics.”

Viewing Interface and Class Statistics

Clicking the linked interface name in the traffic statistics table displays more interface traffic statistic graphs and charts as well as a summary of statistics measured for any classes configured for the interface. Each interface will have at least one class, class-default, configured.

When you are viewing results for an individual outbound interface, you click **View Inbound** to view results for the inbound direction. Likewise, you can switch to viewing outbound results if you open the inbound interface information.

You can switch to the congestion analysis and bandwidth sizing results for the interface by clicking the relevant link from **Related Links**.

You can also define a custom reporting period for viewing interface results. See “Selecting a Report Period” for more information.

When you first open the screen, the traffic statistic graphs displayed for the interface are as follows:

- Micro Burst Detection
- Average Bit Rate
- Packet Rate
- Peak-to-Mean Ratio
- Packet Size Distribution

Along with the Traffic Insight tab, there are other tabs with further details that you can view for the interface:

- Applications
- Talkers
- Listeners
- Conversations

When you click on the name of a class in the Class table, the relevant graphs and charts are available to view for the chosen class.

Class Statistics Overview

The following table describes the information displayed in the class statistics summary table:

Table 4-5: Class Statistics Summary Table

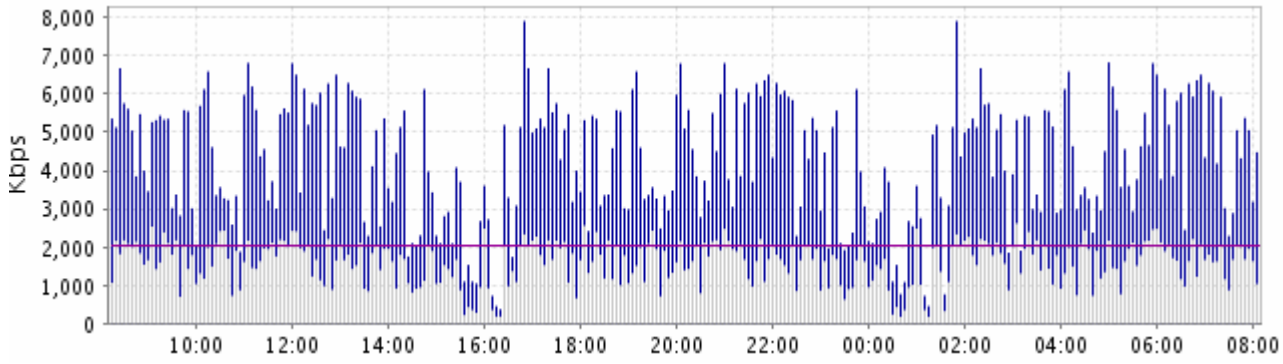
Column	Description
Class	Displays the name of the configured class.
Capacity	Displays the configured capacity reserved for the class.
Total Bytes	Displays the total number of bytes of class traffic measured during the chosen reporting period.
Average Utilization	Displays the average utilization of the reserved class bandwidth

	during the chosen reporting period as a percentage of the configured reserved class bandwidth.
Micro Burst	Displays a graphical representation of microburst measurements that indicates whether significant bursts have been detected.
Max Micro Burst	Displays the maximum measured microburst size for the class traffic during the chosen reporting period.
1 sec Peak	Displays the maximum measured one-second peak value for the class traffic during the chosen reporting period. Comparing this value with the Max Micro Burst value will give you an indication of the extent to which the traffic has experienced millisecond level bursts that would not have been 'seen' with one-second measurements.
Congestion Indicator	Indicates quality degradation issues in the network. The Congestion Indicator uses millisecond measurements to detect congestion events in the router queues based on the specified quality of service targets and sizing policy. Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and sizing policy that are used to calculate the Congestion Indicator. The Congestion Indicator value is a unitless number which reflects the congestion level on a link or class. For a class, it reflects the extent by which the loss and/or delay experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Congestion Indicator value seen on any class on that interface. A Congestion Indicator value greater than 1 means that loss or delay is above an acceptable level, as specified in the BQM configuration. A Congestion Indicator of less than or equal to 1 means the loss and/or delay are within the specified targets. Only available for local site outbound and remote site inbound interfaces and their classes. If you have not enabled Congestion Indicator calculation in the monitor-queuing-map being applied to an interface class, the status is displayed as 'Not Configured.'

Identifying Microburst Measurements

When you view the details for an interface or a class, the Micro Burst Detection plot is displayed.

Figure 4-29: Microburst Results



The legend below the graph identifies the color of each plotted line. The graph includes the following sources of data:

- the measured peak rate based on one-second measurement
- the measured peak rate based on the timescale resolution configured in the monitor-queuing-map for measuring microbursts (for example, 50 ms)
- for classes only, the graph includes the measured peak rate based on the timescale configured in the monitor-queuing-map queuing targets for delay (for example, 500 ms)

The threshold configured in the monitor-queuing-map for triggering event detection on microbursts (for example, 1000 kpbs on a 1024 kbps link) is indicated on the graph, as is the capacity of the link.

So three of the plotted quantities are determined by the monitor-queuing-map being applied to the interface or class of interest. If you have configured specific values in each case, then these configured values form the basis for the plots you now see. Otherwise the default monitor-queuing-map values are used.

Note Under certain conditions it is possible to see higher peak values measured for larger millisecond resolutions than for smaller ones. For example, let's say you have configured a queuing delay target of 500ms and a microburst peak measurement resolution of 400ms. If traffic arrives in separate groups of packets, separated by any more than 400ms, the 400ms peak estimate does not account for two of these groups of packets, whereas the 500ms does. So, the 500ms peak measurement turns out to be greater than the 400ms peak.

This effect is more common if you have shape detection turned off. Let's say we have packets spaced by 450ms. Then the 500ms 'raw' peak will see 2 packet in 500ms, and the 400ms 'raw' peak will see 1 packet in 400ms. Hence, the 500ms raw peak will exceed the 400ms one. The effect is rarer when you have shape detection enabled, because you need to have groups of more than one packet, but, as described above, it is still possible.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and threshold that are used to calculate and display the plotted data. For more information, see the “Configuring QoS Monitoring Features” section of the “Configuring BQM QoS Monitoring” chapter.

Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

If the class traffic is perfectly smooth (that is, it is transmitting at a constant bit rate) then all three measurements listed above will be the same. The more bursty the traffic, the more variation there will be between these measurements. This can help you understand why an application that looks like it has very low bandwidth requirements on average may actually be causing drops in the network when it transmits very sharp short spikes.

Note The fact that such high-level bursts in the traffic are measured raises the question of why TCP does not adjust the sending rate from the data center to match the access link speeds.

The answer appears to be that it does adjust the rate over long periods of time. However, the fact that TCP is allowed, under certain circumstances, to send a full window of data at maximum speed, gives rise to many of the extreme bursts.

When a TCP connection starts up, it begins with a very small window size, which is gradually increased as data and acknowledgements are exchanged between the server and the client. After a while the window reaches a maximum size, which is system-dependent. 64K is typically of many systems (it can be much larger on "optimized" systems). At this point the window is fully open but there is already a full window of data "in flight" between the server and the client, so the server will only send new packets when it receives acks from the client. This effectively matches the sending rate to the access link speed.

However, suppose the transaction finishes but the TCP connection is kept open, in anticipation of a further transaction. The server has now received acks for all of the data it sent, so it can now send a full window instantaneously as soon as it has more data to send. The result is 64K of data (more than 40 full-sized packets) sent at full speed.

The effect will be exacerbated if the server/client systems have been "optimized" by increasing the window size limit, allowing the server to send more data in a single burst (many TCP acceleration systems do this); and also if the application uses small packet sizes, which means a larger number of packets per burst.

Another variation of this is where a connection starts up interactively and then switches to bulk mode. The interactive phase (where the server and client "chat" to each other about what they are going to do) allows the server to open up its window (every successfully exchanged packet doubles the window size) without actually sending very much data. Again, a state is reached where the server has a fully open window but no data in flight. So when it switches to bulk mode, it can send a full window at maximum speed.

Identifying Interface and Class Traffic Patterns

The basic traffic statistic graphs displayed for the interface are as follows:

- Average Bit Rate
- Packet Rate
- Peak-to-Mean Ratio

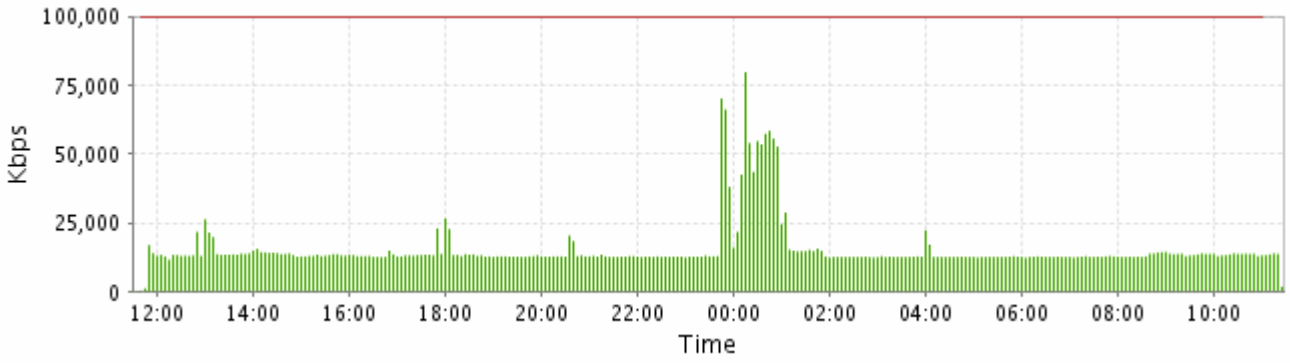
You can use these graphs to identify the traffic patterns for the chosen reporting period. For example, if values displayed in the average bit rate and packet rate graphs vary significantly, the traffic is probably bursty. Smoother traffic will tend to have fewer variations of these statistics over time. High peak-to-mean values can also indicate bursty traffic, whereas low peak-to-mean values can indicate smoother traffic.

You can also view a packet size distribution chart for the same traffic.

Average Bit Rate Graph

When you view the details for an interface or a class, the Average Bit Rate plot is displayed. The graph plots the average number of bits measured for the traffic during the selected reporting period. The capacity of the link is also indicated on the graph.

Figure 4-30: Average Bit Rate Graph

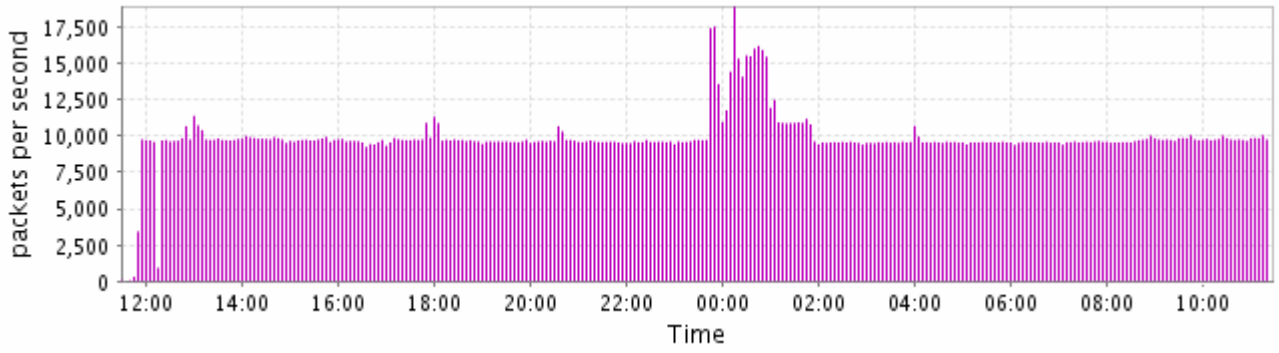


The maximum, minimum and mean values are listed beside the plot.

Average Packet Rate Graph

When you view the details for an interface or a class, the Average Packet Rate plot is displayed. The graph plots the average number of packets measured for the traffic during the selected reporting period.

Figure 4-31: Average Packet Rate Graph

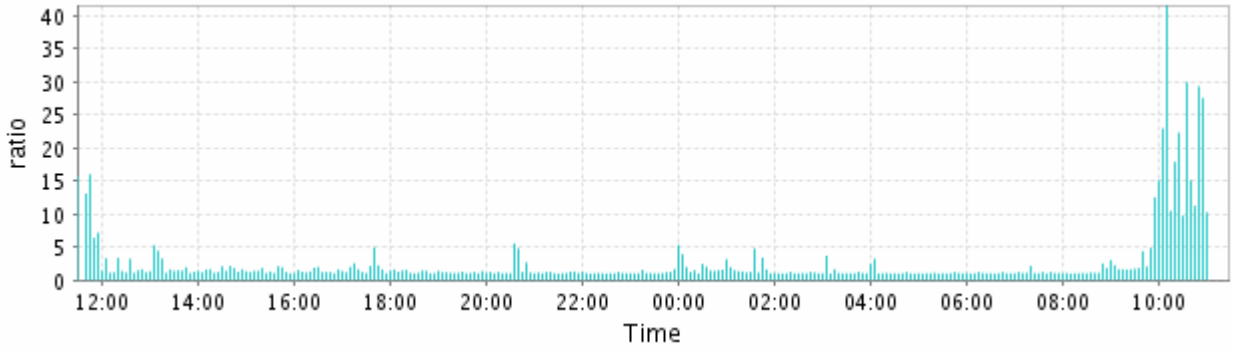


The maximum, minimum and mean values are listed beside the plot.

Peak-to-Mean Ratio Graph

When you view the details for an interface or a class, the Peak-to-Mean plot is displayed. The graph plots the peak-to-mean ratio calculated for the traffic during the selected reporting period. The peak values used in the calculation are those from microburst measurement. The graph plots the ratio of measured 5 millisecond peaks to 1 second peaks, which gives an insight into the burstiness of the traffic.

Figure 4-32:Peak-to-Mean Ratio Graph

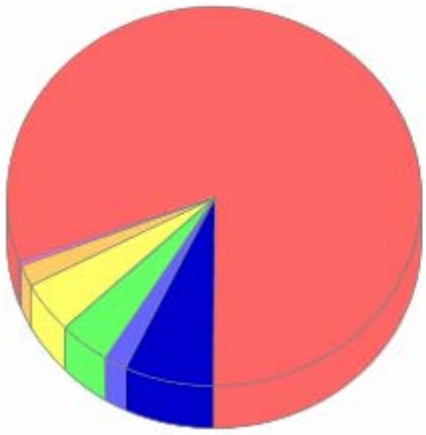


The maximum, minimum and mean values are listed beside the plot.

Packet Size Distribution Chart

When you view the details for an interface or a class, the Packet Size Distribution chart is also displayed. The graph plots the average number of bits measured for the traffic during the selected reporting period.

Figure 4-33: Packet Size Distribution Chart



Packet Size Distribution (Bytes)	
Packet Size	**Total Bytes**
0 - 64 bytes	822909
65 - 128 bytes	71601
129 - 256 bytes	18305
257 - 512 bytes	41696
513 - 1024 bytes	43873
1025 - 1480 bytes	19061
1481 - 1520 bytes	3723
1521 (and greater) bytes	1

Packet size distribution data enables you to evaluate the range of packet sizes traversing the network. The packet size distribution can have a direct impact on the efficiency of network bandwidth usage. If most of the bytes on a particular link come from large packets (those with sizes greater than half the link's maximum frame size), you can consider that part of the network to be efficient. However, if most of the bytes are coming from small packets (less than half the link's maximum frame size), the network efficiency may be an issue. If you think this is the case, you can:

- Identify problem applications - look for applications that employ many small data requests.
- Identify problem users –check for users (or groups of users) that generates an inefficient packet size distribution.
- Identify problem protocols -analyze file server and network management traffic on your network, looking for those that generate many small packets.

Identifying Traffic Leaders

The charts identifying traffic leaders for the interface are as follows:

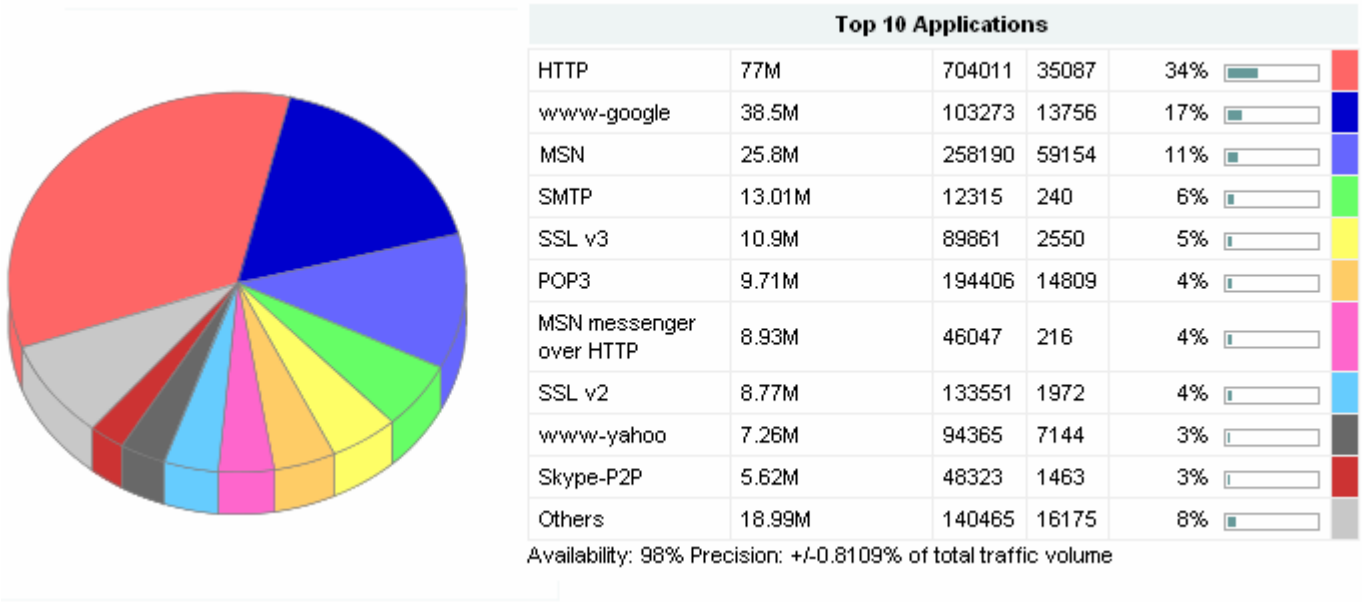
- Top applications
- Top talkers
- Top listeners
- Top conversations

You can use these charts to identify the applications comprising the largest share of network traffic and the hosts transmitting and receiving the most traffic over the chosen reporting period.

Viewing Top Applications

You can view pie charts illustrating the top applications during the selected reporting period. To view the top applications chart, click the **Applications** tab.

Figure 4-34:Top Applications



Top 10 Applications

HTTP	77M	704011	35087	34%
www-google	38.5M	103273	13756	17%
MSN	25.8M	258190	59154	11%
SMTP	13.01M	12315	240	6%
SSL v3	10.9M	89861	2550	5%
POP3	9.71M	194406	14809	4%
MSN messenger over HTTP	8.93M	46047	216	4%
SSL v2	8.77M	133551	1972	4%
www-yahoo	7.26M	94365	7144	3%
Skype-P2P	5.62M	48323	1463	3%
Others	18.99M	140465	16175	8%

Availability: 98% Precision: +/-0.8109% of total traffic volume

The pie chart shows the relative portions of bandwidth used by the most active applications on the network. This provides you with further information when monitoring traffic activity.

Details for the top applications are displayed below the pie chart:

The **Top Applications** column identifies the name of each of the top discovered applications during the selected reporting period. If the system has not had enough time to match a given set of traffic with a known application, it is listed as ‘Undetermined.’ If traffic does not belong to an application known to the system, it is added to the listed category ‘Unknown.’ Applications that fall outside the top ten are grouped under the separate heading ‘Others.’

The **Bytes** column displays the total number of bytes for the application during the selected reporting period.

The **Packets** column displays the total number of packets for the application during the selected reporting period.

The **New Flows** column displays the total number of new flows initiated for the application during the selected reporting period. This figure represents the lower bound on new flows which have been detected within the selected reporting period. Actual flow counts may be higher.

Note A flow is defined as follows: A network traffic flow is a unidirectional sequence of packets all sharing the same source and destination IP address, source and destination port, and IP protocol.

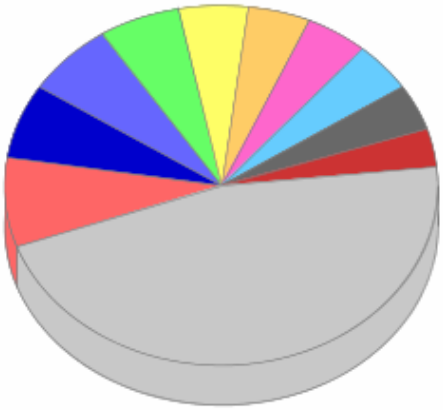
The colors match each colored segment of the chart to a listed application.

Availability and Precision statements provide information on the amount of traffic on which the results are based.

Viewing Top Talkers

You can view pie charts illustrating the top talkers during the selected reporting period. To view the top talkers chart, click the **Talkers** tab.

Figure 4-35: Top Talkers



Top Talkers

192.168.1.158	19.77M	243811	9021	8%
192.168.3.195	15.16M	225948	10625	6%
192.168.1.173	14.94M	32213	4172	6%
192.168.3.170	13.12M	120196	18079	6%
192.168.1.146	12.27M	67194	3992	5%
192.168.1.217	10.64M	76214	12750	4%
192.168.4.22	10.29M	56046	649	4%
192.168.1.179	9.15M	71193	4604	4%
192.168.1.171	8.99M	78248	5655	4%
192.168.3.100	7.64M	48371	4755	3%
Others	114.8M	967693	80720	48%

Availability: 98% Precision: +/-1.4459% of total traffic volume

The pie chart shows the relative portions of bandwidth used by the most active talkers on the network. This provides you with further information when monitoring traffic activity.

The **Address** column identifies the IP address for the hosts sending the most traffic. To resolve the IP addresses listed in the top talkers to their DNS host names, click **Resolve**.

The **Bytes** column displays the total number of bytes transmitted by each host during the selected reporting period.

The **Packets** column displays the total number of packets transmitted by each host during the selected reporting period.

The **New Flows** column displays the total number of new flows initiated for the host during the selected reporting period. This figure represents the lower bound on new flows which have been detected within the selected reporting period. Actual flow counts may be higher.

The colors match each colored segment of the chart to a listed talker.

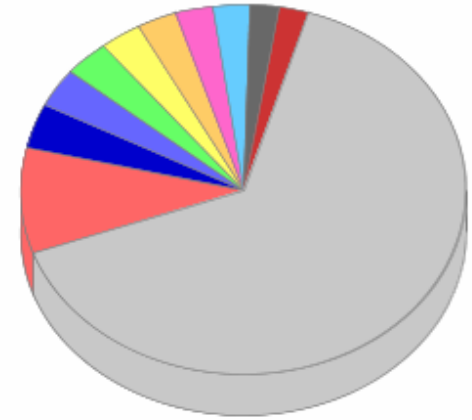
Availability and Precision statements provide information on the amount of traffic on which the results are based.

Average bit rate and packet rate graphs are available for each of the top talkers listed.

Viewing Top Listeners

You can view pie charts illustrating the top listeners during the selected reporting period. To view the top listeners chart, click the **Listeners** tab.

Figure 4-36: Top Listeners



Top Listeners

172.18.1.10	20.3M	199473	14678	8%
63.163.28.20	8.64M	159840	11	4%
82.195.135.54	7.96M	62186	1508	3%
72.14.205.19	7.72M	20170	5260	3%
72.14.205.83	7.49M	19026	4898	3%
64.233.185.19	6.94M	16926	4433	3%
64.233.185.83	6.13M	14872	4079	3%
65.54.239.141	5.28M	25541	0	2%
134.226.81.9	4.9M	4045	4	2%
216.200.21.178	4.74M	6319	2	2%
Others	159.6M	1490179	122515	67%

Availability: 98% Precision: +/-0.7156% of total traffic volume

The pie chart shows the relative portions of bandwidth used by the most active listeners on the network. This provides you with further information when monitoring traffic activity.

The **Address** column identifies the IP address for the hosts receiving the most traffic. To resolve the IP addresses listed in the top listeners to their DNS host names, click **Resolve**.

The **Bytes** column displays the total number of bytes received by the host during the selected reporting period.

The **Packets** column displays the total number of packets received by the host during the selected reporting period.

The **New Flows** column displays the total number of new flows initiated for the host during the selected reporting period. This figure represents the lower bound on new flows which have been detected within the selected reporting period. Actual flow counts may be higher.

The colors match each colored segment of the chart to a listed listener.

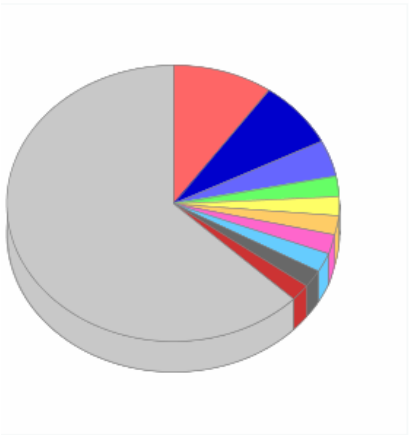
Availability and Precision statements provide information on the amount of traffic on which the results are based.

Average bit rate and packet rate graphs are available for each of the top talkers listed.

Viewing Top Conversations

You can view pie charts illustrating the top conversations during the selected reporting period. To view the top conversations chart, click the **Conversations** tab.

Figure 4-37:Top Conversations



Top Conversations

Updated At: 2006-11-06 12:15

Conversation (Resolve)	Application	Bytes	Packets	Mean Rate	New Flows	%
TCP 10.157.30.167:3454 -> 10.207.11.30:139	MS-Dynamics-CRM	121.4 Mb	92979	12	3	10.3%
TCP 10.157.31.9:1318 -> 10.207.11.100:1101	MS-Dynamics-AX	96.2 Mb	102537	9	350	8.1%
TCP 10.158.30.24:1494 -> 10.207.11.104:1212	Citrix-ICA	52.1 Mb	137070	5	1183	4.4%
TCP 10.158.30.24:1494 -> 10.207.11.112:1051	Citrix-ICA	29.9 Mb	93687	3	1413	2.5%
TCP 10.157.31.8:1313 -> 10.207.11.107:1077	MS-Dynamics-AX	27.9 Mb	24344	3	270	2.3%
TCP 10.157.31.9:1318 -> 10.207.11.111:1087	MS-Dynamics-AX	27.9 Mb	20954	3	81	2.3%
TCP 10.157.31.9:1318 -> 10.207.11.110:1052	MS-Dynamics-AX	27.9 Mb	30683	3	187	2.3%
TCP 10.157.31.14:8080 -> 10.207.11.128:2244	Web-Traffic	27.4 Mb	17358	3	7	2.3%
TCP 10.157.31.9:1318 -> 10.207.11.109:1095	MS-Dynamics-AX	25.3 Mb	25271	2	197	2.1%
TCP 10.158.30.11:1494 -> 10.207.11.2:1042	Citrix-ICA	24.1 Mb	142015	2	814	2.0%
Others	Others	778 Mb	-	0	-	61.4%

Availability: 100%. Precision: +/-0.3% of total traffic volume.

The pie chart shows the relative portions of bandwidth used by the most active conversations on the network. This provides you with further information when monitoring traffic activity.

The **Top Conversations** column identifies the source and destination address/port for the busiest traffic flows. To resolve the IP addresses listed in the top conversations to their DNS host names, click **Resolve**.

The **Application** column identifies the application (if known) that comprises the conversation between the listed hosts.

The **Bytes** column displays the total number of bytes for the conversation during the selected reporting period.

The **Packets** column displays the total number of packets for the conversation during the selected reporting period.

The **New Flows** column displays the total number of new flows initiated for the conversation during the selected reporting period. This figure represents the lower bound on new flows which have been detected within the selected reporting period. Actual flow counts may be higher.

The colors match each colored segment of the chart to a listed conversation.

5 Analyzing Network Events

This chapter describes how to use the BQM to investigate events of interest on the monitored network. This chapter contains the following sections:

- Overview
- Investigating Network Events
- Working with Manual Packet Captures

Overview

The BQM enables you to detect, record, analyze, and report on traffic events in the monitored network. You can

- identify QoS-impacting events on the network
- analyze the causes and effects of the events
- investigate a structured break-down of the events

When an event is detected by the BQM, a bar in the **Congestion Analysis** tab quality events timeline identifies the event. The BQM performs calculations on the measured event data to support detailed analysis of the event. Initially, the BQM uses default threshold values above which to trigger event detection, but you can configure the thresholds for detecting quality events in the monitor-queuing-map applied to a given interface.

If a large set of congested links or low thresholds results in a very large number of events being triggered and detected, the BQM generates an alarm if disk space is low due to the processing required. The BQM may not be able to record packet captures for many interfaces simultaneously when packet rates are high.

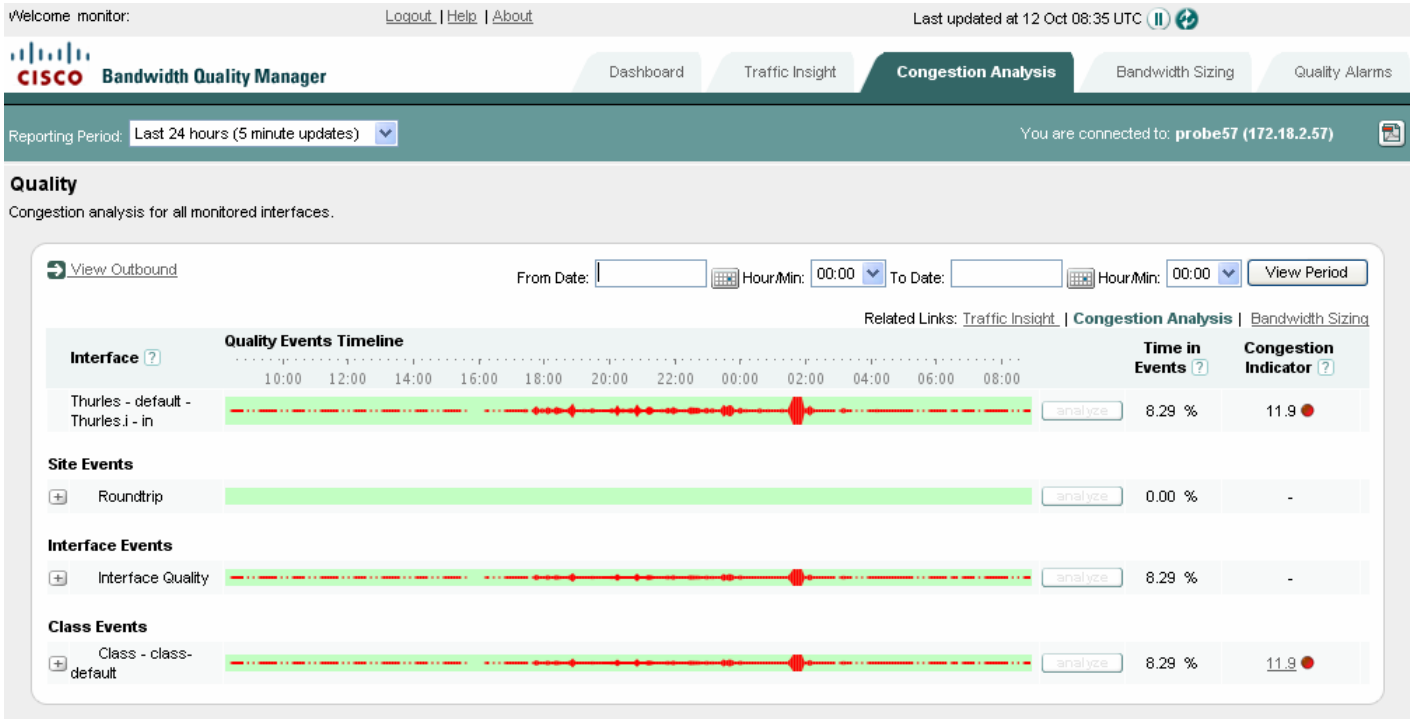
When an event has been detected, a packet capture file for the interval during which the event occurred is automatically logged to disk. This packet capture file provides the BQM with the data to support detailed analysis during event analysis. The packet capture covers the period of time over which the event was detected. In order to provide this feature a rolling, historical packet capture is provided for each interface.

You can also define and start manual packet capture sessions. The packet capture file created is this case is also made available for event analysis.

Investigating Network Events

When you open the **Congestion Analysis** tab, the complete list of interfaces configured on the BQM are displayed. Network events are indicated on the Quality Events Timeline by a mark at the time the violation (or series of violations) took place. The summary view of all interfaces allows you to quickly identify quality events on particular interfaces during the chosen reporting period.

Figure 5-1: Congestion Analysis



Choosing to analyze a particular interface or class launches the Congestion Analysis Inspection window. This window displays the Quality Events Timeline for the selected reporting period. The following series of graphs and charts containing data measured during the chosen timeline:

- Average bit rate
- Average packet rate
- Microburst detection
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length
- Expected Delay
- Expected Queue Length
- Expected Loss
- Top applications
- Top talkers
- Top listeners
- Top conversations

Analyzing an Event

To investigate a quality event, you do the following:

Step 1 Check that you have set the reporting period for the timeline in which you are interested.

Step 2 Click the interface of interest.

Step 3 Check the Quality Events Timeline to identify the time of the event of interest.

Step 4 To narrow the timeline down closer to the event of interest, click **select** beside the **From Date** field and choose the event date from the calendar.

Choose a time closely preceding the event from the list of half-hour intervals.

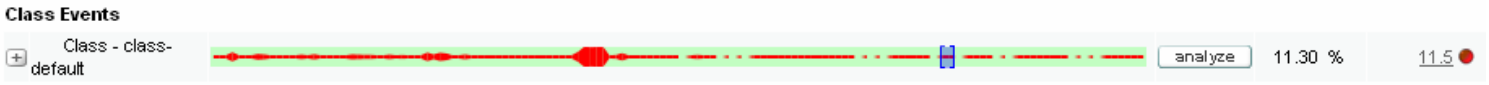
Click **select** beside the **To Date** fields and choose the event date from the calendar.

Choose a time soon after the event from the list of half-hour intervals.</step>

Click **View Period**.

When the screen refreshes the timeline and all the information on the screen is displayed for the start and end time you specified.

Figure 5-2: Selecting an Event for Analysis

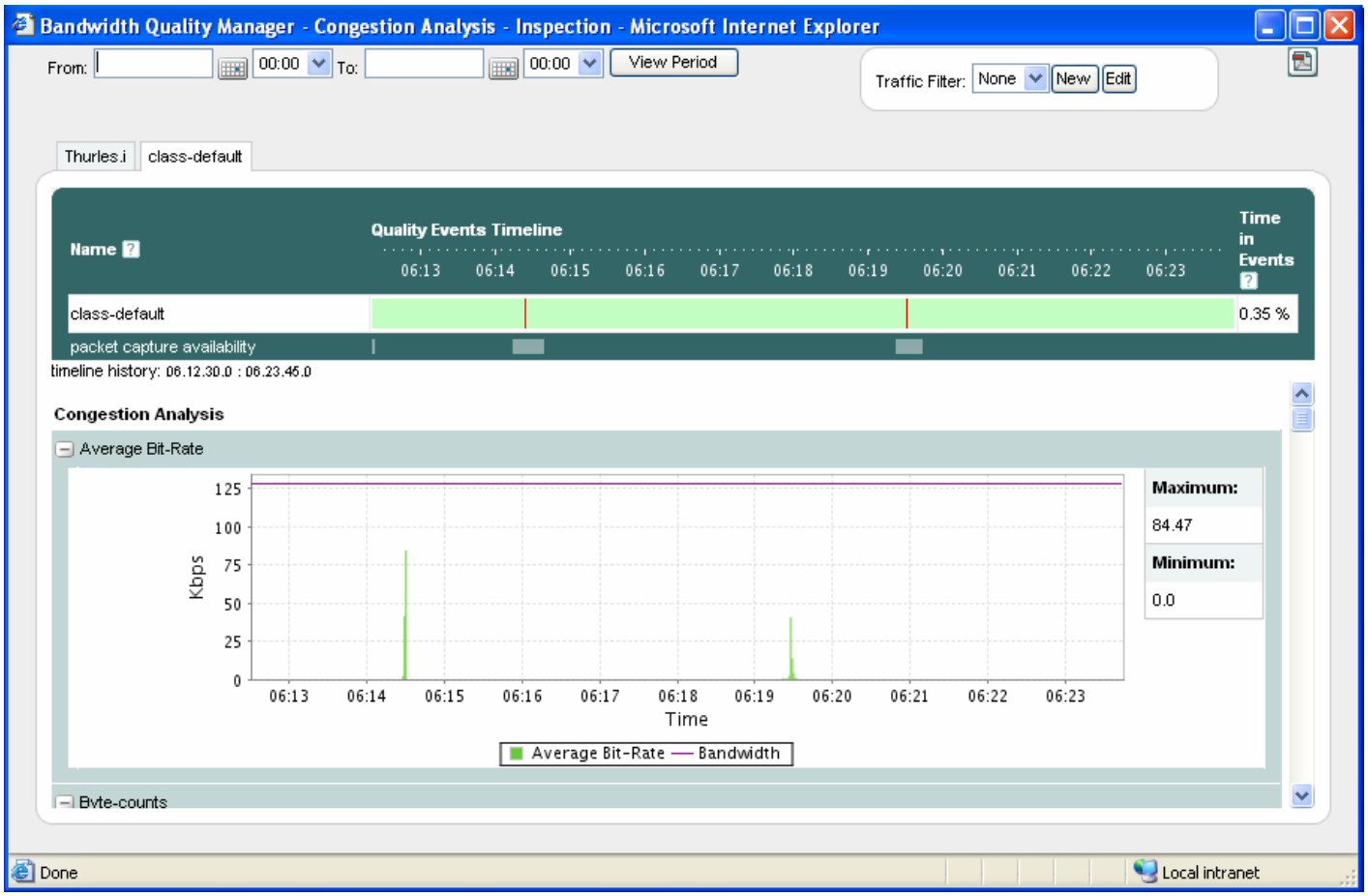


Step 5 Click and drag over the event of interest on the Quality Events Timeline and click **analyze**.

The Event Analysis inspection window is launched displaying the Quality Events Timeline for the timescale you defined by clicking and dragging. The new window also displays a series of graphs and charts containing data measured during the chosen timeline.

Each event in indicated on the timeline by a mark. Below the timeline and usually under each mark, a bar indicates the period of time for which an event packet capture is available.

Figure 5-3: Event Analysis Inspection Window

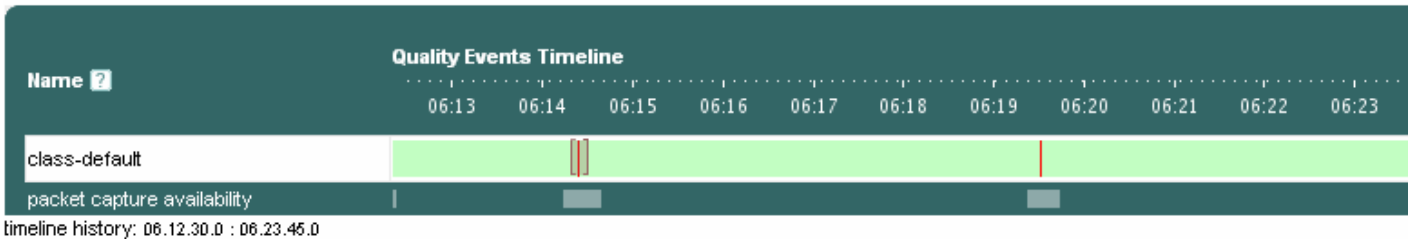


Note It is possible to see an event displayed on the quality events timeline in the Congestion Analysis screen for which Event Analysis is not available. If a data update and screen refresh occurs while a packet capture is still running to record an event, you may see an event in the Congestion Analysis quality events timeline. However, if you attempt to analyze this event, the Event Analysis screen may not yet have the packet capture information available. In such cases, you should wait a couple of minutes for the current packet capture to finish and then retry the analysis.

Step 6 Check the displayed timeline again. You can define another time period as described above to focus on a particular event. You can also use the zoom feature on the Quality Events Timeline or any of the displayed graphs to investigate the details behind the event you are troubleshooting.

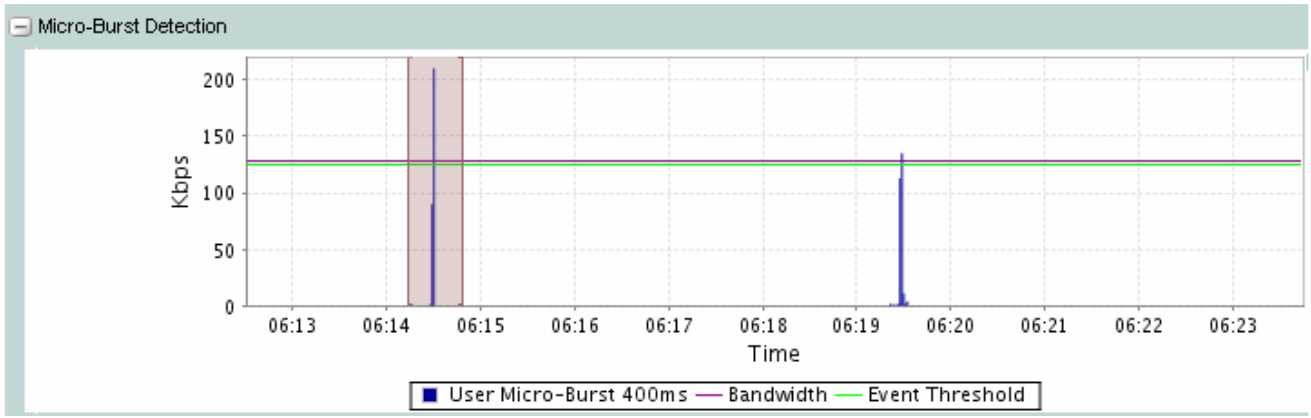
Step 7 To zoom in on the Quality Events Timeline or on a chosen graph, click and drag the mouse across a selected portion of the timeline.

Figure 5-4: Zooming in on an Event on the Timeline



Alternatively, you can zoom in on a particular graph. For example, if you initially chose a reporting period of one hour and therefore the graphs first displayed are over that timescale, you may identify a particular peak in microburst measurements during a five-minute period.

Figure 5-5: Zooming in on a Graph

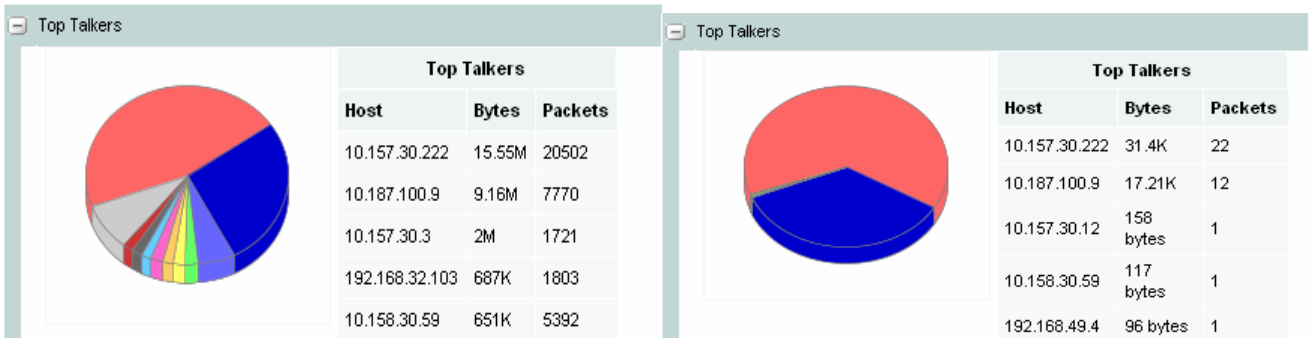


So you can click and drag across that five-minute period on the Microburst Detection graph to zoom in to the five-minute graph.

Step 8 You can use the same click-and-drag technique to zoom into a selected graph down to millisecond timescales. Zooming in to the detail at shorter timescales enables you to identify very specific traffic events. Each time you zoom in, all of the available graphs and charts are redrawn to show only the data relevant to the selected timescale.

So if, for example, you have zoomed in to the microburst detection graph to isolate a particular event at millisecond-level resolution, you can then consult the traffic leader graphs (top applications, top talkers, top listeners, top conversations) to establish the source of the traffic.

Figure 5-6: Top Talkers Before and After Zooming



You can use the timeline history links provided to jump back to different 'zoom' levels or use the **Reset** button to return the inspection screen to its original timescale.

Each of the presented graphs and plots can be expanded or contracted in any combination so you can display only those in which you are most interested.

Defining and Applying Traffic Filters to Event Analysis Results

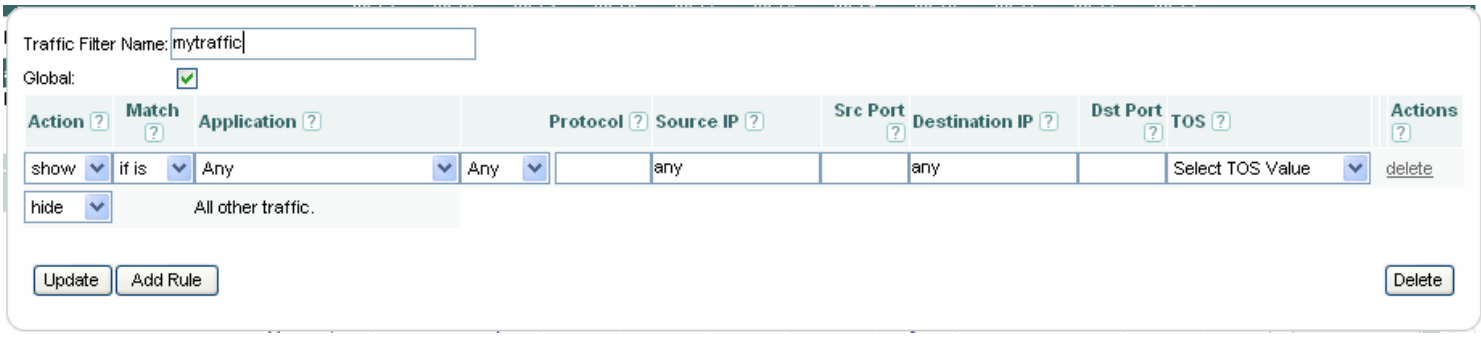
You can filter event analysis results by defining and applying a set of traffic classification rules similar to an access control list (ACL).

Figure 5-7: Event Analysis Traffic Filter

To define an traffic filter for event inspection, you do the following:

Step 1 Click **New**.

Figure 5-8: Defining an Event Analysis Traffic Filter



Step 2 Enter a name for the traffic filter in the **Traffic Filter Name** field.

Step 3 Check the **Global** check box if you want this traffic filter to be available when analyzing all interfaces being monitored by the system.

Step 4 Select an action from the **Action** list - to show or hide packets that conform to the rules you are about to define and apply.

Step 5 Select an option from the **Match** list if you want to apply the rules you specify as they are or if you want to apply a logical NOT to the rules.

Step 6 If required, choose an application from the list of automatically recognized or custom-defined applications.

Step 7 If required, select a protocol from the **Protocol** list or enter the protocol number in the adjacent field.

Step 8 If required, enter a traffic source IP address and source port number in the **Source IP** and **Src Port** fields respectively.

Step 9 If required, enter a traffic destination IP address and destination port number in the **Destination IP** and **Dst Port** fields respectively.

Step 10 If required, select a TOS value from the list to identify traffic.

Step 11 When you have completed the definition of the traffic filter, click **Save** to save the traffic filter and close the traffic filter screen.

The defined traffic filter is now available to choose from the traffic filter list. To apply the traffic filter, choose it from the list. The event analysis results are now displayed with the filter applied to the traffic under investigation. So, for example, you can use this feature to isolate particular known traffic within a class that you are analyzing.

To add another rule, click **Add Rule**.

When you have defined multiple rules, the available actions include the option to change the ordering of the defined rules. Click the up and down arrows to move the selected rule up or down in the list. To delete an individual match rule from the traffic filter, click **delete** in the **Actions** column for the selected rule.

The defined traffic filter is now available to choose from the traffic filter list. To apply the traffic filter, choose it from the list. The event analysis results are now displayed with the traffic filter applied to the traffic under investigation. So, for example, you can use this feature to isolate particular known traffic within a class that you are analyzing.

To delete the entire traffic filter and all associated rules, click **Delete**.

To edit a saved traffic filter, choose it from the traffic filter list and click **Edit**. Make the required changes to the filter definition and then click **Save**.

Viewing Event Congestion Analysis Results

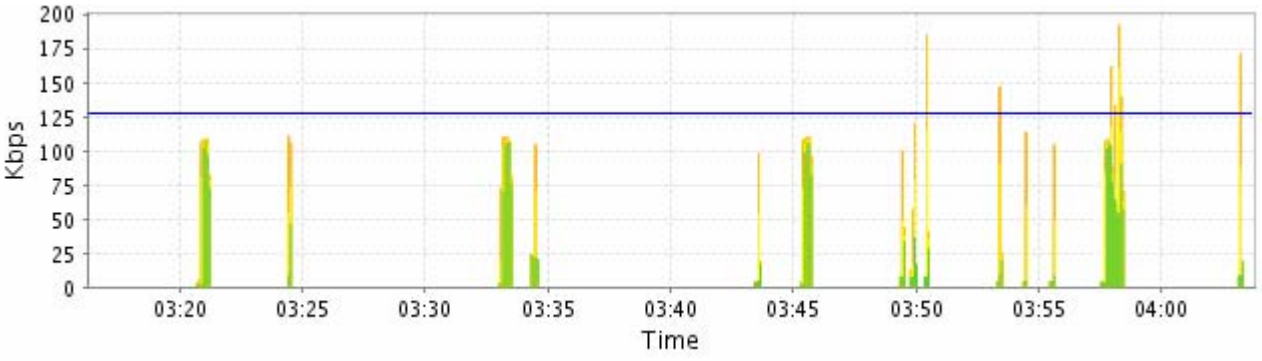
The detailed analysis for each event includes graphs of the following:

- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length
- Expected Queuing Delay
- Expected Queue Length
- Expected Queuing Loss

Corvil Bandwidth – Delay

The Corvil Bandwidth graph for delay plots the bandwidth required to meet the configured delay target for the traffic. The delay target is configured in the monitor-queuing-map that is applied to the traffic. For example, if the configured delay target is 150 ms, then the graph displays the bandwidth required to ensure that no packet in the traffic is delayed by more than 150 ms.

Figure 5-15: Event Delay Corvil Bandwidth



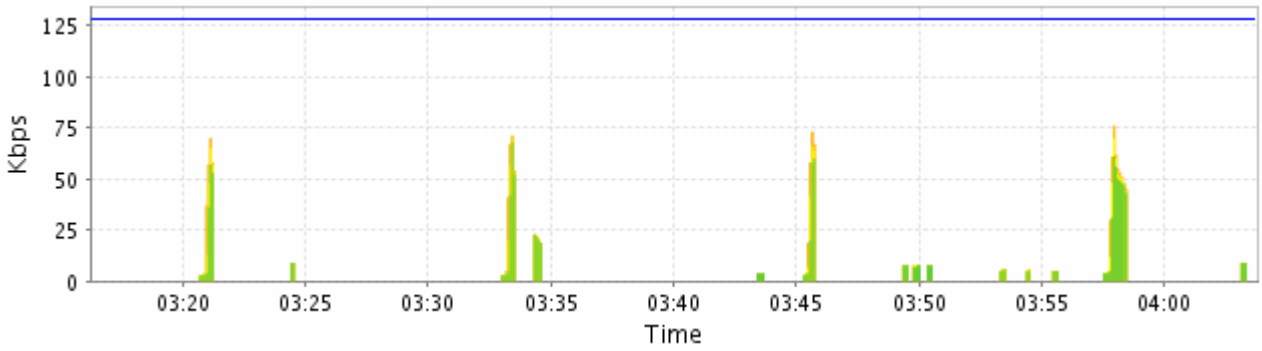
The Corvil Bandwidth values are displayed as a series of values in kbps over the selected timescale. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated during the chosen reporting period.
x% - the xth percentile of Corvil Bandwidth values. This percentile is configurable in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean –the mean of the Corvil Bandwidth values during the chosen reporting period
Min –the minimum of the Corvil Bandwidth values during the chosen reporting period.

Corvil Bandwidth – Queue Length

The Corvil Bandwidth graph for queue length plots the bandwidth required to avoid packet loss due to queue buffer overflow. For example, if the configured queue length is 64 packets, then the graph displays the bandwidth required to prevent the queue for the class traffic building up past 64 packets.

Figure 5-16: Event Queue Length Corvil Bandwidth



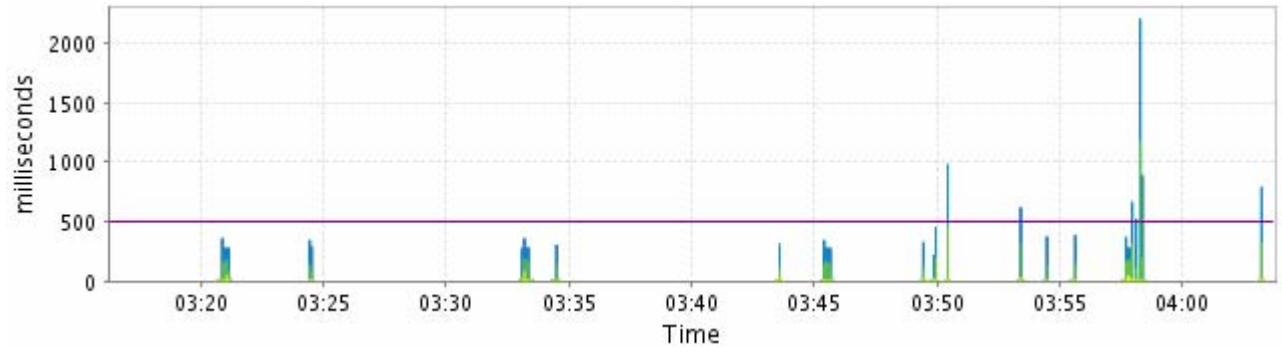
The graph displays a series of Corvil Bandwidth values (in kbps) during the chosen reporting period. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated during the chosen reporting period.
x% - the xth percentile of Corvil Bandwidth values. This percentile is configurable in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean –the mean of the Corvil Bandwidth values during the chosen reporting period
Min –the minimum of the Corvil Bandwidth values during the chosen reporting period.

Expected Queuing Delay

The expected queuing delay graph plots the per-packet delay, as calculated by the BQM. The expected queuing delay is displayed as a series of millisecond values during the reporting period. The expected queuing delay calculation is made for every packet in the traffic captured by the BQM for the quality event. Then for each period, the maximum, configured percentile, mean and minimum values are plotted.

Figure 5-17: Event Expected Queuing Delay



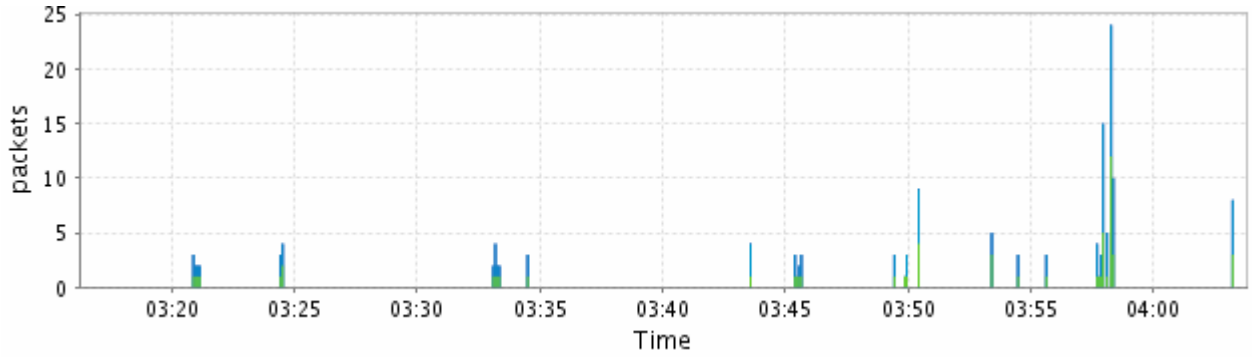
The graph legend indicates the colors used to display each:

Max - displays the maximum of the expected delay values (in milliseconds) calculated for each chosen reporting period.
x% - the xth percentile of Corvil Bandwidth values. This percentile is configurable in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean – displays the mean of the expected delay values during the chosen reporting period
Min – displays the minimum of the expected delay values during the chosen reporting period.

Expected Queue Length

The expected queue length graph plots the queue length that each packet will encounter, as calculated by the BQM. The expected queue length is displayed as a series values for the chosen reporting period. The expected queue length calculation is made for every packet in the traffic captured by the BQM for the quality event. The maximum, configured percentile, mean and minimum values are all plotted.

Figure 5-18: Event Expected Queue Length



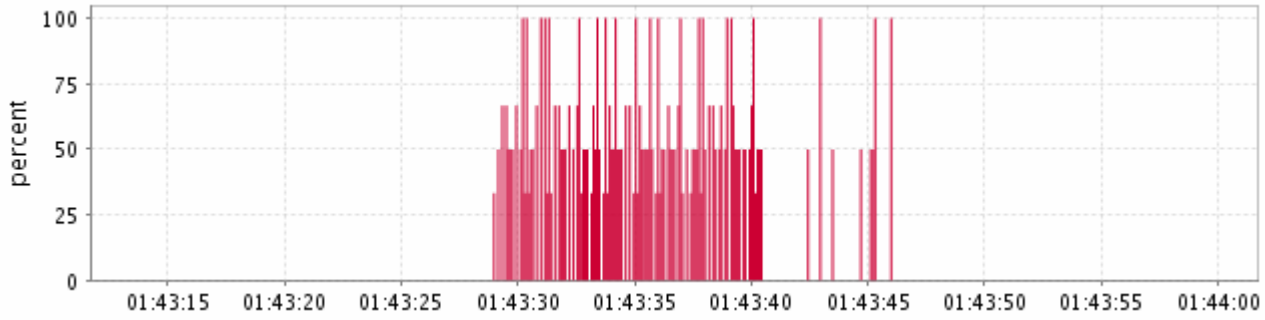
The graph legend indicates the colors used to display each:

Max - displays the maximum of the expected delay values (in milliseconds) calculated during the chosen reporting period.
x% - the xth percentile of Corvil Bandwidth values. This percentile is configurable in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean – displays the mean of the expected delay values during the chosen reporting period
Min – displays the minimum of the expected delay values during the chosen reporting period.

Expected Queuing Loss

The expected queuing loss graph plots the expected packet loss due to queue buffer overflow, as calculated by the BQM.

Figure 5-19: Event Expected Queuing Loss



The expected packet loss is displayed as a percentage of the total packets measured by the BQM for the chosen timescale.

Viewing Priority Class Event Results

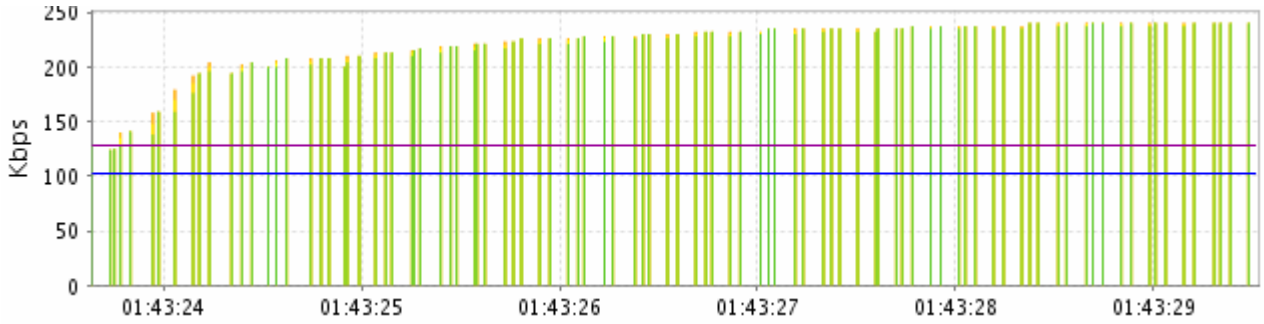
If you have configured a multiclass policy-map and assigned priority to one of the classes, such as the voice class, you can view results for the priority class.

Corvil Bandwidth - Priority

The Corvil Bandwidth - Priority graph plots the bandwidth required to avoid policer packet drops for the configured priority class traffic.

If the configured priority burst-size in bytes is smaller than a packet size, then the Corvil Bandwidth for that packet is not well defined, because changing the priority bandwidth cannot, on its own, prevent policer drop. Should this happen, the Corvil Bandwidth value will jump to a very large value. In such cases, you can examine the packet size distribution in the **Traffic Insight** screen to help choose an appropriate priority burst-size.

Figure 5-20: Event Priority Class Corvil Bandwidth



The graph is displayed as a series of kbps values for each five minutes during the reporting period. For each five-minute period, the maximum, configured percentile, mean and minimum values are plotted:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated each five minutes during the chosen reporting period.
xth percentile - the xth percentile of Corvil Bandwidth values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean - the mean of the Corvil Bandwidth values for each five minutes during the chosen reporting period
Min - the minimum of the Corvil Bandwidth values for each five minutes during the chosen reporting period.

The threshold configured in the monitor-queuing-map for triggering event detection based on the Corvil Bandwidth value is indicated on the graph, as is the capacity of the link.

Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and thresholds that are used to calculate and display the plotted data. For more information, see "Configuring QoS Monitoring Features."

Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Expected Priority Drops

The expected priority drops graph plots the expected level of packet drops due to the action of a configured policer. The result is calculated by the BQM using a simulation based on the chosen class traffic.

Figure 5-21: Event Priority Class Packet Drops

Priority drop estimation is enabled, and its characteristics defined, in the monitor-queuing-map applied to the interface.

Identifying Event Traffic Leaders

The charts identifying traffic leaders for the event are as follows:

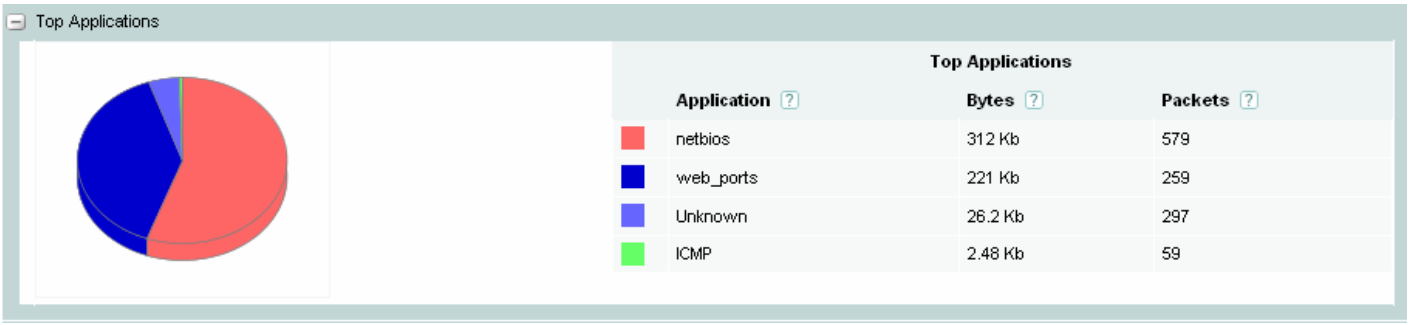
- Top applications
- Top talkers
- Top listeners
- Top conversations

You can use these charts to identify the applications comprising the largest share of network traffic and the hosts transmitting and receiving the most traffic as you zoom in on a particular quality event.

Viewing Top Applications

You can view pie charts illustrating the top applications over the selected timescale. The pie chart shows the relative portions of bandwidth used by the most active applications on the network at the time.

Figure 5-22: Event Top Applications



The **Top Applications** column identifies the name of each of the top discovered applications during the selected timescale. If the system has not had enough time to match a given set of traffic with a known application, it is listed as 'Undetermined.' If traffic does not belong to an application known to the system, it is added to the listed category 'Unknown.'

The **Bytes** column displays the total number of bytes for the application during the selected timescale.

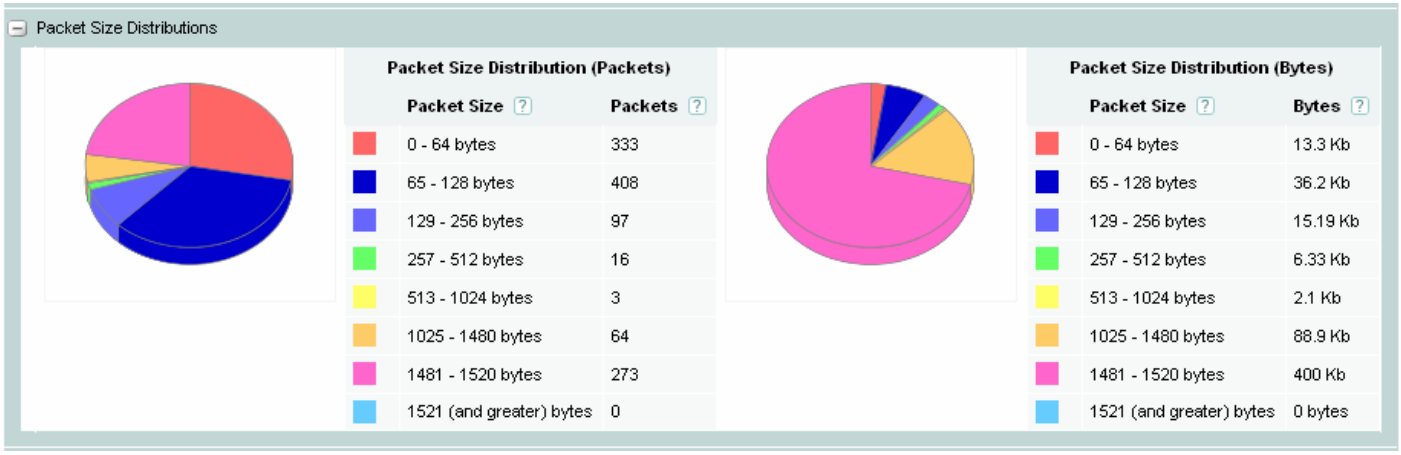
The **Packets** column displays the total number of packets for the application during the selected timescale.

The colors match each colored segment of the chart to a listed application.

Viewing Packet Size Distributions

You can view pie charts illustrating the packet size distribution in terms of both packets and bytes for the network traffic over the selected timescale.

Figure 5-23: Event Packet Size Distributions



The **Packet Size** column displays the ranges of packet sizes.

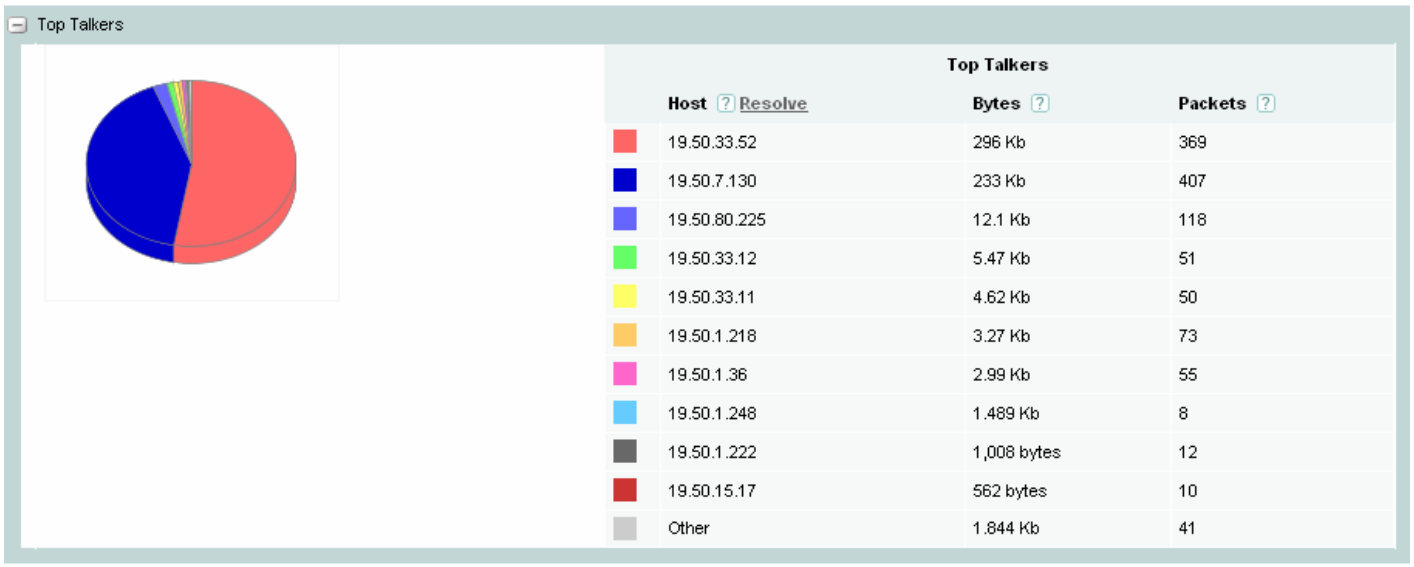
The **Packets** column displays the total number of packets of each size transmitted by each host during the selected timescale.

The **Bytes** column displays the total number of bytes transmitted during the selected timescale of each packet size.

Viewing Top Talkers

You can view pie charts illustrating the top talkers during the selected timescale.

Figure 5-24: Event Top Talkers



The pie chart shows the relative portions of bandwidth used by the most active data transmitters on the network at the time.

The **Address** column identifies the IP address for the hosts sending the most traffic during the selected timescale

The **Bytes** column displays the total number of bytes transmitted by each host during the selected timescale.

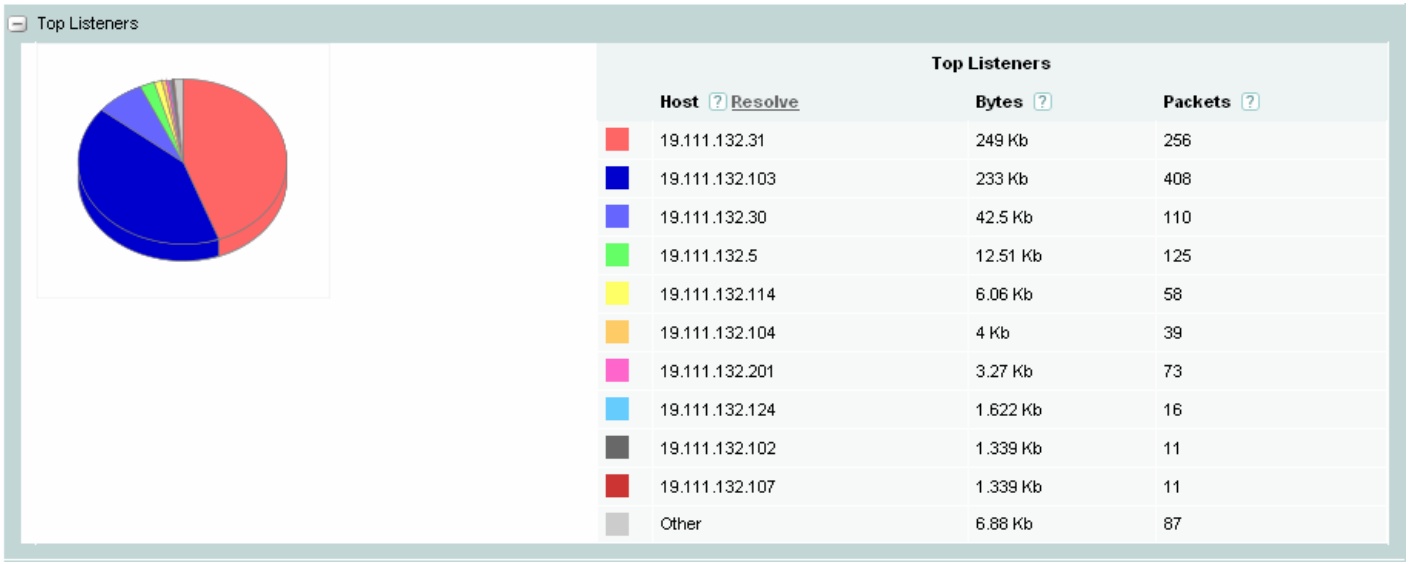
The **Packets** column displays the total number of packets transmitted by each host during the selected timescale.

The colors match each colored segment of the chart to a listed talker.

Viewing Top Listeners

You can view pie charts illustrating the top listeners during the selected reporting period. To view the top listeners chart, click the **Listeners** tab.

Figure 5-25: Event Top Listeners



The pie chart shows the relative portions of bandwidth used by the most active listeners on the network.

The **Address** column identifies the IP address for the hosts receiving the most traffic during the selected timescale.

The **Bytes** column displays the total number of bytes received by the host during the selected timescale.

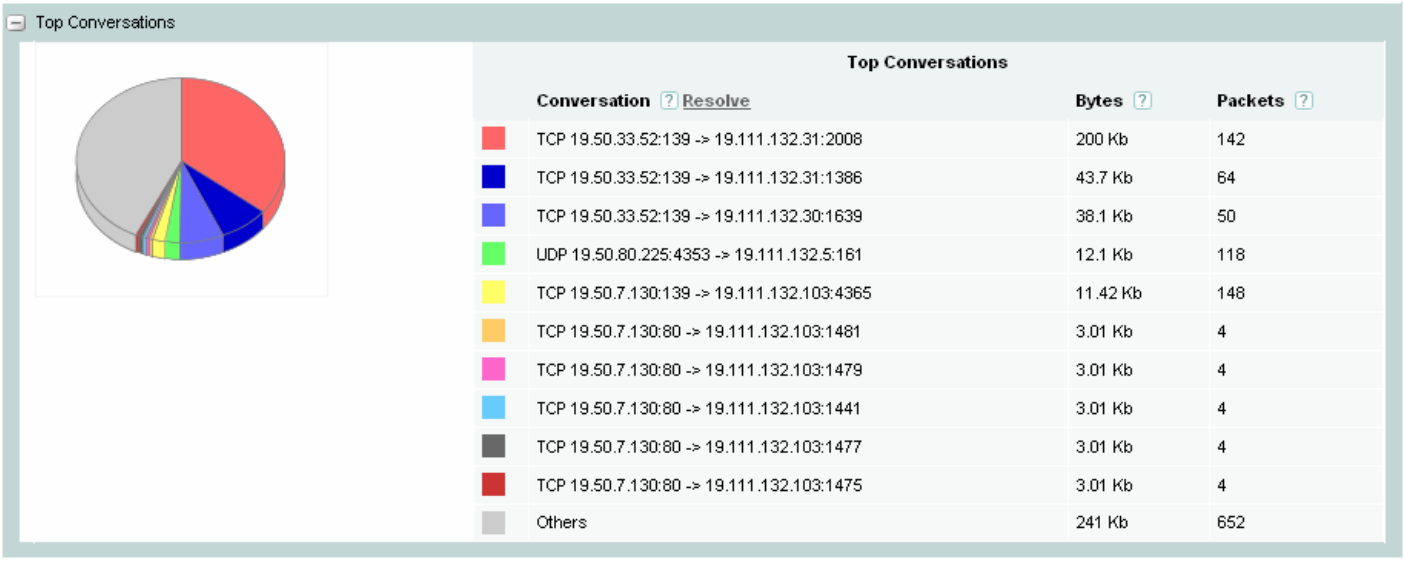
The **Packets** column displays the total number of packets received by the host during the selected timescale.

The colors match each colored segment of the chart to a listed listener.

Viewing Top Conversations

You can view pie charts illustrating the top conversations during the selected timescale.

Figure 5-26: Event Top Conversations



The pie chart shows the relative portions of bandwidth used by the most active conversations on the network.

The **Top Conversations** column identifies the source and destination address/port for the busiest traffic flows during the selected timescale.

The **Application** column identifies the application (if known) that comprises the conversation between the listed hosts.

The **Bytes** column displays the total number of bytes for the conversation during the selected timescale.

The **Packets** column displays the total number of packets for the conversation during the selected timescale.

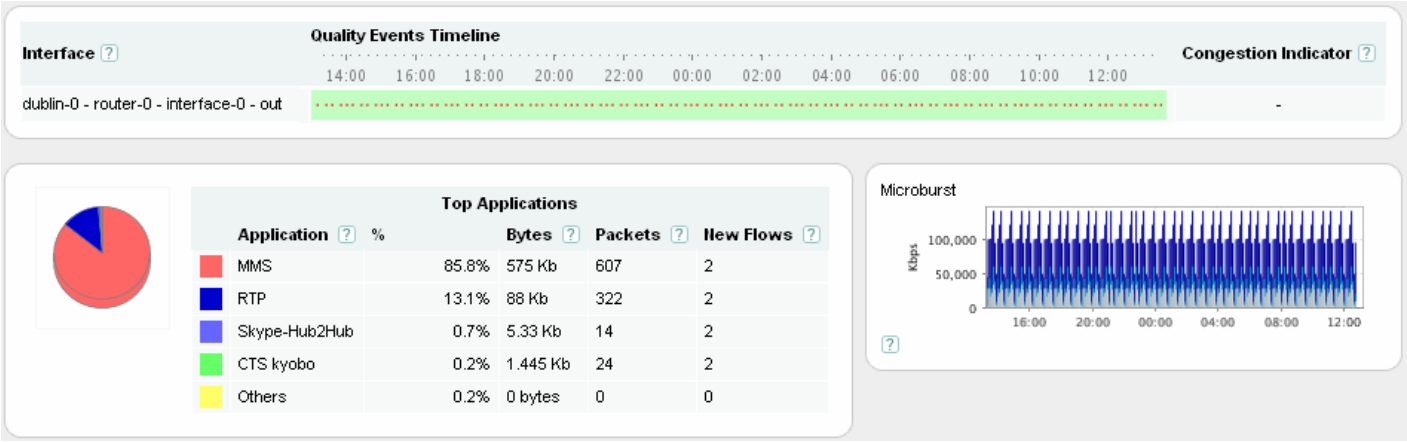
The colors match each colored segment of the chart to a listed conversation.

Identifying the Source of Application Performance Problems

The following example scenario shows how you can use the BQM to troubleshoot application performance issues. Let's suppose customers are complaining about performance at a remote site and the router is showing some loss.

We go to the **Dashboard** tab, filter for the remote site name and view the information for the interface. In this example, the Quality Events Timeline is showing events in the outbound direction.

Figure 5-27: Events and Microburst

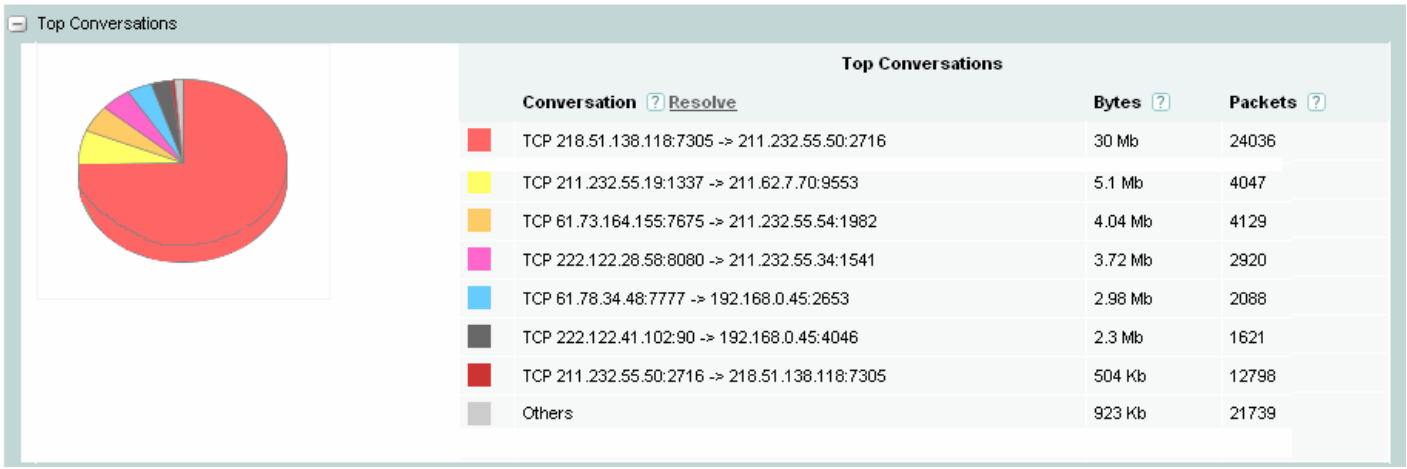


Also, in this example, the micro-burst plot shows that the traffic is peaking to line rate frequently.

In this case there is a threshold set to 90% of link rate, so we navigate to the **Congestion Analysis** tab from the Dashboard. On the **Congestion Analysis** tab, there are many micro-burst events in the data class for that branch office that the we have chosen to analyze. We then zoom in to a period that contains many events.

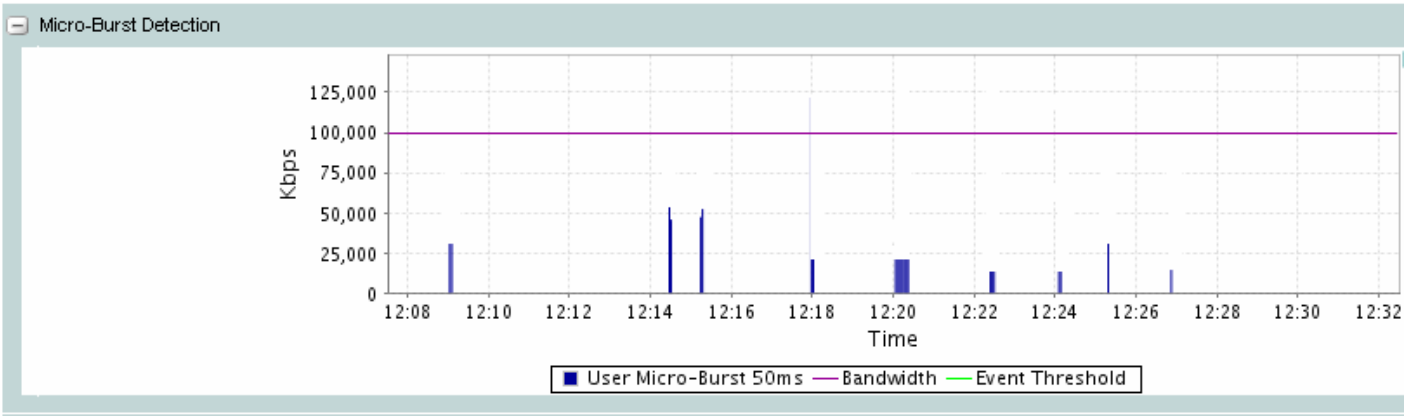
The event top conversations shows one particular application as THE top user of the link. This indicates that the application is the most active when the link is bursting.

Figure 5-28: Top Conversations



For confirmation, we create a traffic filter to exclude that specific IP address.

Figure 5-29: Traffic Filter Excludes High Burst Application



This is effectively a “what-if” exercise where we model the situation where this application is not on the network. In this case, the micro-bursts are eliminated.

Identifying Event Traffic Patterns

The basic traffic statistic graphs displayed for the event are as follows:

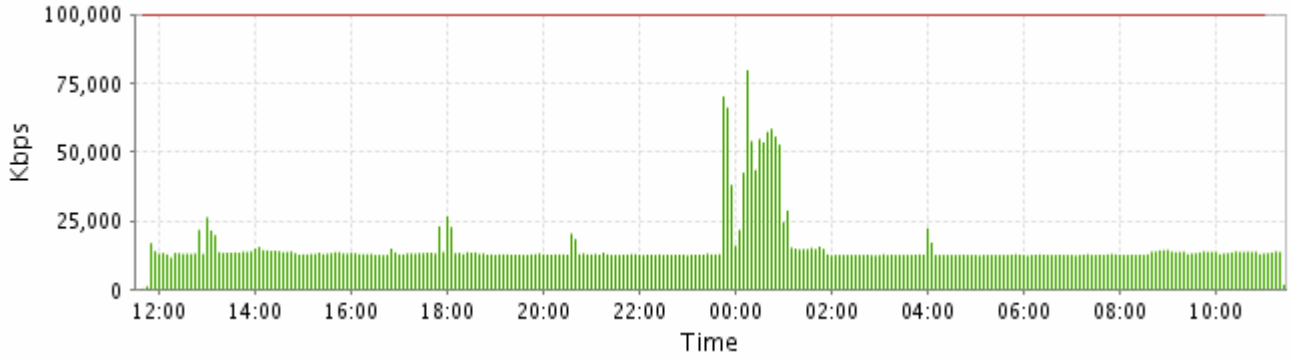
- Average Bit Rate
- Byte-counts
- Packet Rate
- Packet-counts
- Active Connections

You can use these graphs to identify the traffic patterns for the chosen zoom level. For example, if the values displayed in these graphs vary significantly, the traffic is probably bursty. Smoother traffic will tend to have fewer variations of these statistics over time.

Average Bit Rate and Byte-counts Graphs

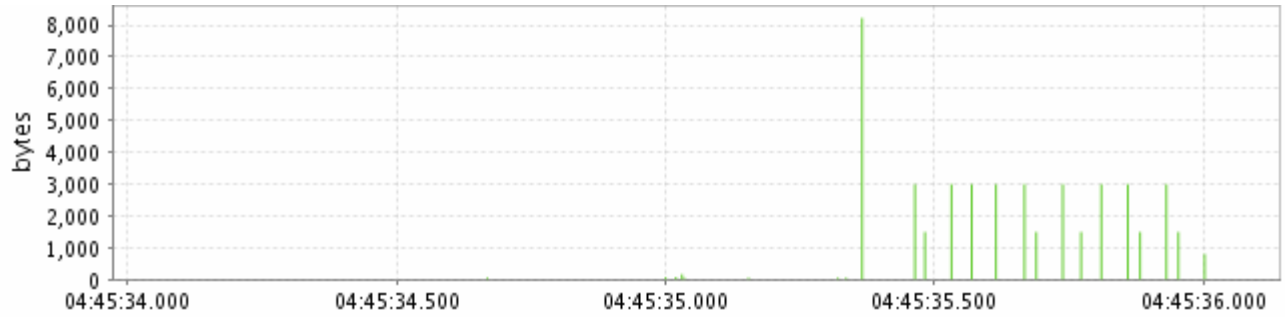
The Average Bit Rate graph plots the average number of bits measured for the traffic during the selected reporting period.

Figure 5-9: Event Bit Rate Graph



As you zoom in on shorter and shorter timescales, it can make more sense to view the Byte-counts graph.

Figure 5-10: Event Byte-counts Graph

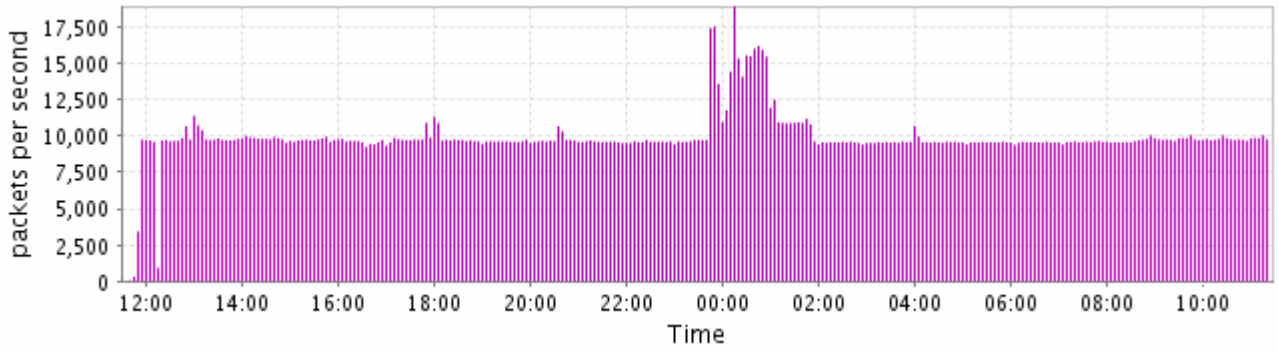


The Byte-counts graph plots the number of bytes measured for the traffic during the selected time interval.

Average Packet Rate and Packet-counts Graphs

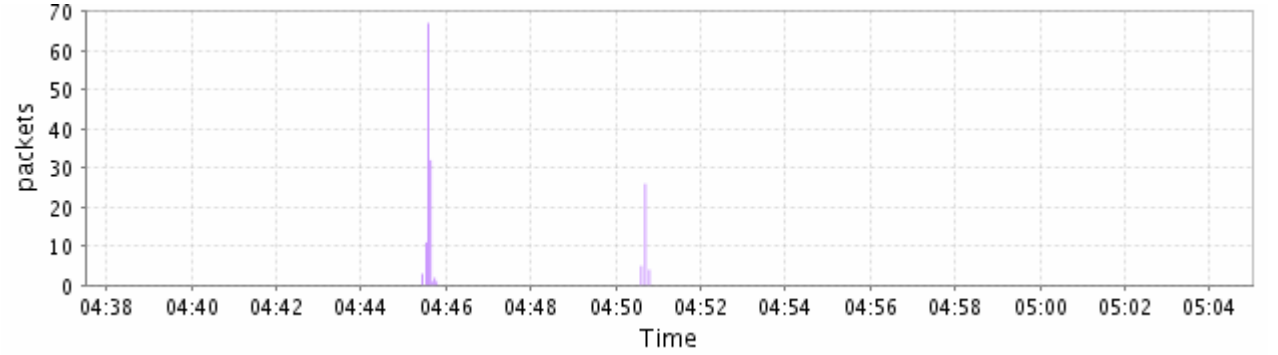
The Average Packet Rate graph plots the average number of packets measured for the traffic during the selected reporting period.

Figure 5-11: Event Packet Rate Graph



As you zoom in on shorter and shorter timescales, it can make more sense to view the Packet-counts graph.

Figure 5-12: Event Packet-counts Graph

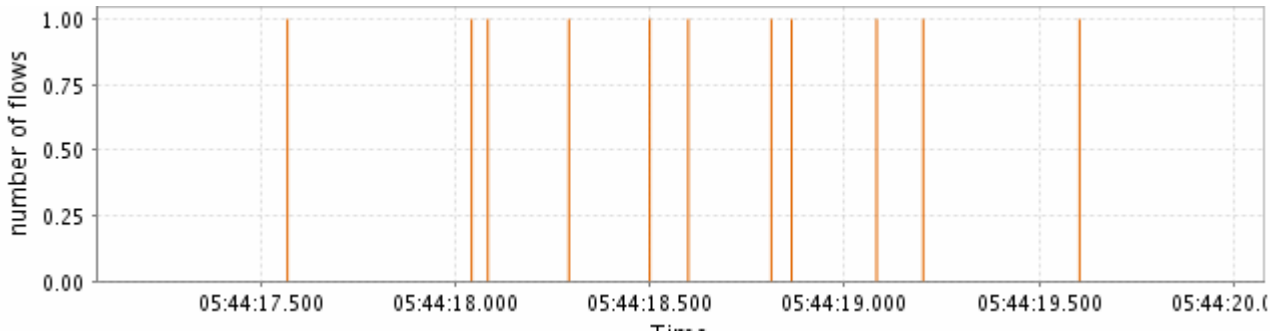


The Packet-counts graph plots the number of packets measured for the traffic during the selected time interval.

Active Flows Graph

The Active Flows graph plots the number of active flows during the selected time interval.

Figure 5-13: Event Active Flows Graph



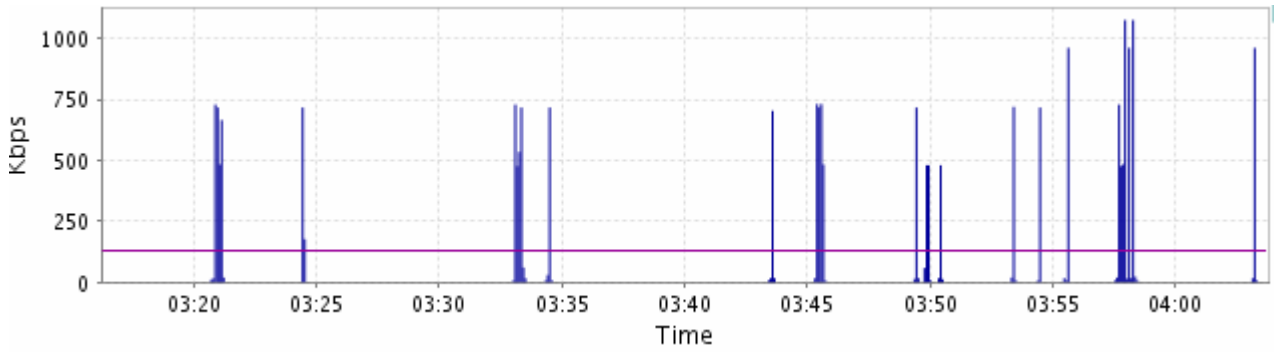
There may be other flows open, but at the selected timescale, you see only the number of flows that are actively transmitting data.

Identifying Event Microburst Measurements

The Micro Burst Detection graph includes the following sources of data:

- the measured peak rate based on the timescale resolution configured in the monitor-queuing-map for measuring microbursts (for example, 50 ms)
- the threshold configured in the monitor-queuing-map for triggering event detection on microbursts (for example, 1000 kpbs on a 1024 kbps link)

Figure 5-14: Event Microburst Graph



The legend below the graph identifies the color of each plotted line.

Identifying Network Delay Problems

The following example scenario shows how you can use the BQM to identify and analyze the potential impact of delay on network performance. Suppose in this case that an expected queuing delay alarm is displayed on the dashboard.

We click this alert and see from the detail that a large delay spike has just occurred for a particular remote site.

Next, we navigate to the **Congestion Analysis** tab and filter for the remote site of interest.

We navigate through to event analysis and zoom in to determine the top applications and top talkers during the event. The results can help you identify the potential impact of the delay spike.

Disabling Event Detection on Selected Interfaces

Event detection is enabled by default on all interfaces, but it may not make sense to keep the automatic, trigger-based packet capture enabled for every single interface at all times. The **trace-events** command is used from the BQM CLI to disable event detection on a selected interface, or to re-enable event detection on an interface where it has been disabled.

Because the default is to have event detection enabled, so there is no need to use a **trace-events** command unless a **no trace-events** command has previously been issued.

For example to enable automatic tracing of detected events on interfaces to which the policy-map named pmap is applied:

```
policy-map high_speed
  trace-events
```

To disable automatic tracing of detected events:

```
policy-map high_speed
  no trace-events
```

Working with Manual Packet Captures

Assuming you have a BQM license with the manual packet capture feature enabled, you can capture all the packets from a specified set of interfaces into a set of capture files (one interface capture per file). You can create up to eight separate capture instances. You then transfer the resulting files to an accessible location for further processing. Both config and admin users can perform packet captures and transfer the resulting capture file(s) to a remote machine.

All of the packets processed by a packet capture session are logged to the BQM disk. To view the current set of capture files you do the following:

```
host(config)$ dir capture:
```

Each file name is the same as the defined capture instance and has the file extension appropriate to the configured file format.

Note The use of pcap format files means that a pcap header is also logged for each packet stored to disk. This pcap header contains the packet timestamp, packet length in bytes (on the wire), and capture length. This adds 16 bytes to the size of each packet stored.

Step 1 Before you start the packet capture, check the available free space on the BQM:

```
host(config)# show file-systems
```

```
File system    Size (KB)       Used  Available  Used%
disk0:         70499556    3170948   67328608     4%
```

Step 2 Create a new capture instance. In this example, the capture instance is named ‘default_serial0’:

```
host(config)# capture default_serial0
```

Step 3 Assign an interface (or peer-interface) to the capture instance. The interface name must be configured on the BQM. In the following example, the site router interface named sanfran_hq – default – serial0 has previously been configured:

```
host(config-capture)# attach interface sanfranhq default
serial0
```

Step 4 Set the packet payload size limit in megabytes for the packet capture. If you do not set a packet payload size limit, there is no explicit limit set on the size of captured data. In this example the size limit is set to 30MB:

```
host(config-capture)# size 30
```

Note In packet captures with a configured size limit, the last packet may be truncated. The capture file may still be used, but you may see a warning raised against the truncated packet when processing the file (for example, using Ethereal).

Step 5 Set the time limit for the packet capture in minutes and the file format. If you do not set a time limit, the default is to continue the packet capture indefinitely, until you stop the capture manually, or the file size limit is reached, or you run out of disk space. If you run out of disk space, packet capture will stop. In this example, the time limit is set to one hour:

```
host(config-capture)# duration 60 minutes
```

In this example configuration, a further two packet captures are set up. In each case the interfaces have been already configured on the BQM:

```
host(config-capture)# capture default_serial1
host(config-capture)# attach interface sanfranhq default
serial1
host(config-capture)# size 30
host(config-capture)# duration 60 minutes
host(config-capture)# capture default_peer
host(config-capture)# attach peer-interface sanfranhq default
serial1
host(config-capture)# size 30
host(config-capture)# duration 60 minutes
host(config-capture)# exit
```

Step 6 Start all of the configured packet captures using the global **start capture** command:

```
host(config)# start capture
```

Alternatively, if you use the **start** command in the `config-capture` context, you can start the specific packet capture that you have just configured.

Step 7 Check the current status of the capture process:

```
host(config)$ show capture

capture serial0
  started
  size 30 MB
  duration 1 hours
  file name /disk0/capture/serial0
  attach interface sanfranhq default serial0

  state: capturing to disk

  Disk capture stats:
  captured: packets: 977, len: 65953, caplen: 60574
  dropped:  packets: 0, len: 0, caplen: 0

capture default_serial1
  started
  size 30 MB
  snaplength 38 (default)
  duration 60
  file name /disk0/capture/default_serial1
  attach interface sanfranhq default serial1

  state: capturing to disk

  Disk capture stats:
    captured:   packets: 1008, len: 68383, caplen: 62496
    dropped:    packets: 0, len: 0, caplen: 0

capture default_peer
  enabled
  size 30 MB
  snaplength 38 (default)
  duration 60
  file name /disk0/capture/default_peer
  attach peer-interface sanfranhq default serial1

  state: capturing to disk

  Disk capture stats:
    captured:   packets: 1008, len: 68383, caplen: 62496
    dropped:    packets: 0, len: 0, caplen: 0
```

The **show capture** command displays the following information:

Capture configuration details
Current capture state
Size of the capture data
Number of captured/dropped frames
Total number of bytes in captured/dropped frames

Note The default number of bytes captured from the beginning of Ethernet frames (the snapshot length) is 38 bytes. You can change this value with the **snaplength** command. For more information on the **snaplength** command, see the Command Reference chapter.

The following table describes the displayed packet capture states.

Table 5-1 Packet Capture States

Packet Capture State	Description
Idle	Packet capture not active; capture session paused (by **no start** command) or not yet started (by **start** command)
Capturing to disk	Packet capture in progress
Size reached	Packet capture stopped because the file size limit has been reached. You need to manually stop packet capture before performing other tasks with the capture file (for example, compressing or copying the capture file.)
Time reached	Packet capture stopped because the file size limit has been reached. You need to manually stop packet capture before performing other tasks with the capture file (for example, compressing or copying the capture file.)
Write error	BQM disk full

Step 8 To manually stop all packet capture sessions, you use the global **no start** command:

```
host(config)# no start capture *
```

Alternatively, you can stop a specific packet capture using the `config-capture` context **no start** command when in the context of the selected packet capture:

```
host(config-capture)# no start
```

Note Stopping a packet capture session and then restarting the same session appends data to the same capture file.

Step 9 Examine the packet capture files:

```
host(config)# dir capture:
capture:/
        Size  Name
      116512  serial0
      170258  default_serial1
      113496  default_peer
```

The listed sizes of the packet capture files are usually greater than any configured size limit. The size limit determines an upper limit on the amount of payload captured, but the final capture files include other data, such as event analysis metadata, which increases the file size considerably.

Note If the BQM loses power during a packet capture session and is subsequently powered up again, a temporary packet capture file is created to avoid corruption of the main capture file. Temporary capture files are named as follows:

<*capturename*>.@capturing@.cpc.gz

If you see a temporary capture file listed when you finish a packet capture, you should copy the temporary file along with the main capture file off the BQM so that you have all captured data available. The temporary file contains data up to the point that the BQM lost power.

Step 10 Copy the capture files to a tftp or ftp server, or using scp for further processing. There is an upper file size limit of 2 Gigabytes on tftp transfers.

```
host(config)# copy capture:serial0
scp://admin@192.168.3.4:serial0
host(config)# copy capture:default_serial1
scp://admin@192.168.3.4:default_serial1
```

Note When you export a packet capture file off the BQM the file is automatically compressed. Following an unzip you may see that the capture file size is different from that when the file was on the BQM because a certain amount of the additional data appended to the file for use in event analysis on the BQM is removed. The file size may be greater than the configured size limit during the packet capture. The size limit determines the upper limit on the amount of payload captured.

You can only copy capture files for completed packet capture sessions. While a capture file is in use by an active capture session, the file permissions are set to 'not readable' and a lock file is also present.

If you have set a packet capture password you are prompted for it when you attempt to copy the capture file from the BQM. See the section "Setting a Packet Capture Password" for more information.

Note As an alternative to "pushing" the captures files from the BQM to a remote server, you can also "pull" them from the BQM from a remote machine that uses scp to contact the BQM ssh server.

If you have physical access to a BQM, the winscp client program is recommended for transferring files to a directly-connected Windows laptop. This program allows the available capture files on the BQM to be listed and shows the file permissions so you can tell which files are actually available for download. When looking at the captured file list using winscp you can only determine that a file is available and ready for transfer (that is, not currently being captured to) by noting the presence or absence of a `.lock` file with the same root filename, or by noting that the file permissions are set to "not readable."

Step 11 When you have verified the successful transfer of the files, remove the capture files from the BQM:

```
host(config)# delete capture:*
Delete filename [serial0] (y/n) ? y
Delete filename [default_serial1] (y/n) ? y

host(config)#
```

Alternatively, you can use the following to delete the files:

```
host(config)# delete /force capture:*
host(config)#
```

Finally, you can check that the deletion has been successful by displaying the disk status:

```
host(config)# show file-systems

File system    Size (KB)       Used  Available  Used%
disk0:         70499556    3170948   67328608     4%
```

Setting Disk Space Quota for Manual and Event Analysis Packet Captures

The BQM employs a separate hard disk for storing packet capture files. Packet capture files generated automatically by BQM event analysis in response to event triggers and those generated by manual packet capture share the same disk.

You use the **capture-settings event-trace-quota** command to allocate a certain percentage of the disk to capture files generated by event analysis to be adjusted between one and 100 percent:

capture-settings event-trace-quota percent <1-100 | **default**>

In the following example, the percentage of disk space allocated to event analysis packet capture is 60%, so the remaining 40% is available for manual packet capture:

```
host(config-capture)$ capture-settings event-trace-quota percent 60
host(config-capture)$
```

Normally the disk is split equally between event analysis and manual capture files, that is, the default value for disk allocation for event analysis capture files is 50%. The remaining disk space is used by manual capture files. Management of these files is performed automatically. You must be logged in to the BQM CLI as an admin user to use this command.

Setting a Packet Capture Password

You can use the **capture-settings password** command from the BQM CLI to establish or reset a password for use with the **copy capture** command, when copying packet capture files to a remote server.

```
host(config)$ capture-settings password
Changing password for capture
New password:
Re-enter new password:
Password changed
```

The password should be at least six characters long with a mixture of letters and numbers.

If no capture password is configured, then the packet capture file that is copied will not be password protected. See the **copy capture** command for more information.

Using Manual Packet Capture to Identify Events

The following example scenario shows how you can use manual packet capture. In this example, let's say that you have been receiving a lot of complaints for the same remote site every morning around 10am for the past week.

From the dashboard, using the filter feature, we navigate to the remote site and find that there are no events visible on the Quality Events Timeline for the interface in either direction. In this example we have not configured any thresholds to report events and trigger packet captures.

We start a manual packet capture around 9:00 am for 3 hours with a snap length of 1500 bytes to capture entire packets.

In this case, we use event analysis to discover that around 10:00 am both large delays and high Corvil Bandwidth are being reported.

We analyze this period and identify the top talkers, top listeners, top conversations and top applications.

We can then export this packet capture for further analysis using a PCAP analyzer to determine TCP server response time verses network delay for the top conversations identified by the BQM.

6 Bandwidth Sizing

This chapter describes how to use the BQM to estimate the interface bandwidth required to prevent queuing delay and loss in excess of the configured targets. The chapter contains the following sections:

- Overview
- Viewing Sizing Results

Overview

By default the **Bandwidth Sizing** tab lists all of the network model pre-queuing interfaces (local site outbound and remote site inbound) you have configured in the BQM network model.

After you have completed configuration of the BQM network model to reflect your network, you typically should allow the system to measure traffic for at lest a week before considering the bandwidth sizing results. In many cases, you would wait until the system has accumulated a month's worth of measurements.

The summary table information is sorted by interface name and provides a guide to bandwidth utilization on network links. You can choose from a predefined list of reporting periods up to 60 days or define a custom reporting period over which to view data. You can also sort the summary information by column and you can drill into each interface to view more details (such as class bandwidth requirements). This enables you to identify candidates for bandwidth upgrade.

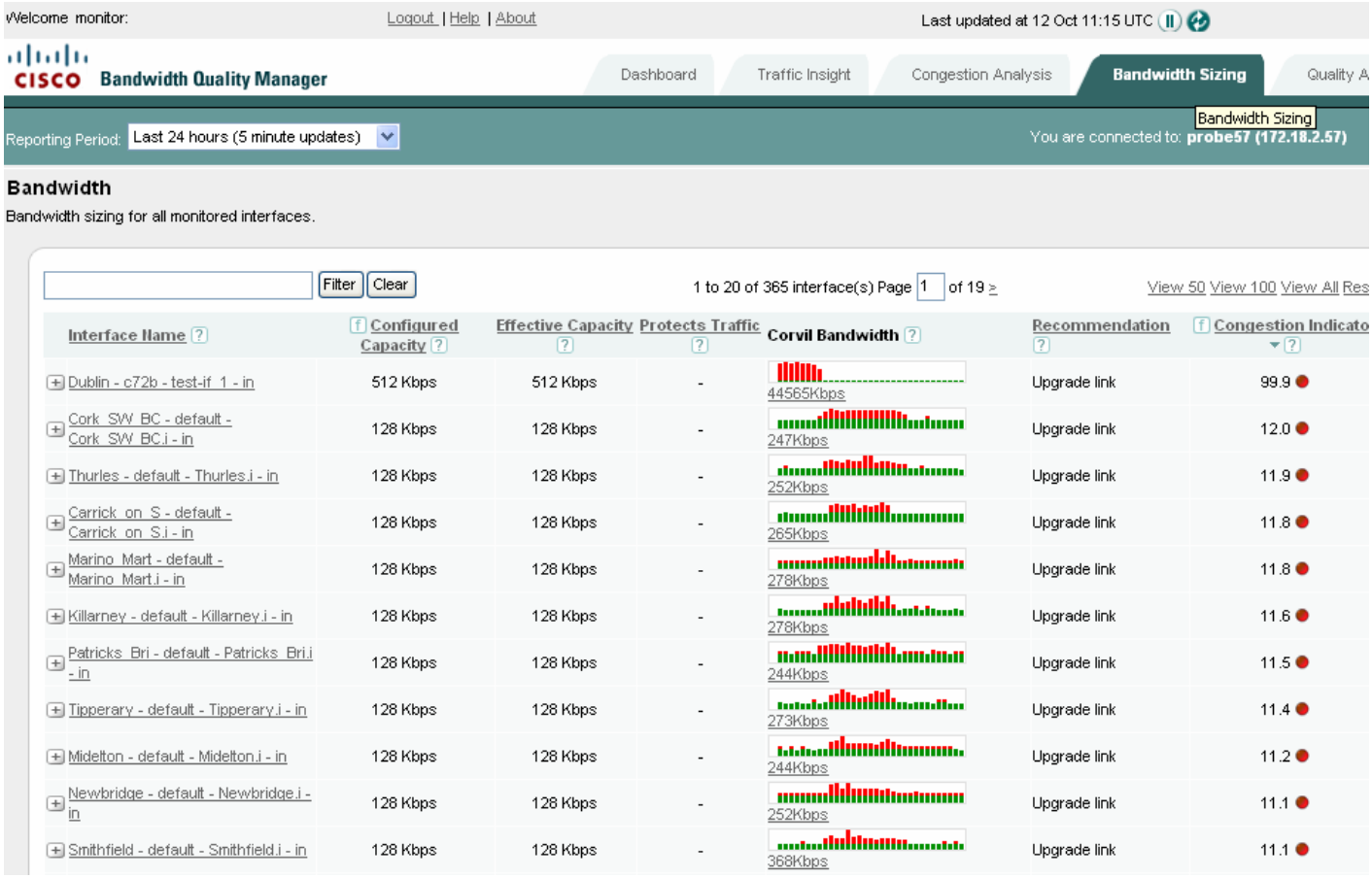
Note . To enable bandwidth sizing as a feature, you must enable Corvil Bandwidth measurement, and configure both a set of queuing targets and a sizing policy, in the monitor-queuing-map that is applied to the class.

For more information on queuing targets and the sizing policy in the class monitor queuing map, see "Enabling QoS Monitoring Features".

Bandwidth Sizing Summary Table

By default, results for twenty interfaces are displayed per page and if there are more than twenty interfaces configured, you use the links at the bottom of the list to navigate between pages of results.

Figure 6-1: Bandwidth Sizing Summary



If you have many interfaces configured, you can also click the **View 50**, **View 100**, or **View All** links to display the corresponding number of interfaces on a single page. In these cases you scroll down the page to view all the presented results.

The following table describes the information displayed in the bandwidth sizing summary table:

Table 6-1: Bandwidth Sizing Summary Table

Column	Description
Interface	Displays the full, qualified name identifying the interface and the direction of the traffic (inbound or outbound) being measured by the interface: *site name – router name – interface name – direction*. The site name, router name and interface name are those that have been configured in the BQM network model. The direction of traffic is always represented from the perspective of a site in the BQM network model. In the case of MPLS VPN, Internet VPN, Private VPN deployments this means that for each interface and peer interface pair configured in the network model, the configured interface represents the outbound traffic from the site (local or remote) and the peer-interface represents the inbound traffic to the site (local or remote).
Configured Capacity	Displays the configured capacity value of the interface or class.
Effective Capacity	Displays the configured capacity of the interface or class in single-class configurations. In multiclass configurations, the effective capacity is the minimum bandwidth a given class in a multi-class configuration can expect to receive taking into account the bandwidth assigned to all the other classes.
Protects	Displays the percentage of traffic to which the listed recommendation and Congestion Indicator calculation applies. The percentage value here is configurable as part of defining the sizing policy for and interface. The sizing policy is configured in the monitor-queuing-map applied to the interface and its classes. Permitting a certain fraction of the packets to violate the queuing targets reduces the bandwidth required from that needed to guarantee no loss or delay for every single packet. For example, by protecting 99% of traffic, the resulting bandwidth requirement calculated by the BQM ensures that 99% of arriving packets encounter - a total per-hop delay no greater than the queuing-targets delay value defined in the monitor-queuing-map - a queue length no greater than the configured queue limit defined for the class
Corvil Bandwidth	The graphic illustrates the Corvil Bandwidth values measured during the selected reporting period. The Corvil Bandwidth is the bandwidth required to meet the queuing quality targets configured for the chosen class traffic. The displayed bandwidth (in kbps) is sufficient to ensure the configured percentage of packets is

	protected from excessive delay and loss in every busy-period in the displayed interval.
Recommendation	Displays the recommended course of action based on the calculated bandwidth requirement for the interface and class. See the section “Viewing Sizing Results” for more information on the displayed recommendations.
Congestion Indicator	Indicates quality degradation issues in the network. The Congestion Indicator uses millisecond measurements to detect congestion events in the router queues based on the specified quality of service targets and sizing policy. Use the **Monitor Queuing Maps** menu in **System Administration** mode to set the quality targets and sizing policy that are used to calculate the Congestion Indicator. The Congestion Indicator value is a unitless number which reflects the congestion level on a link or class. For a class, it reflects the extent by which the loss and/or delay experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Congestion Indicator value seen on any class on that interface. A Congestion Indicator value greater than 1 means that loss or delay is above an acceptable level, as specified in the BQM configuration. This interface or class is not meeting its quality targets. A Congestion Indicator of less than or equal to 1 means the loss and/or delay are within the specified targets, so this interface or class is meeting its quality targets. Moreover, this means that the sizing policy has been achieved over the selected reporting period. A low Congestion Indicator value could indicate a candidate for bandwidth downgrade. If you have not enabled Congestion Indicator calculation in the monitor-queuing-map being applied to an interface, the status is displayed as ‘Not Configured.’

Note Summary results are based on the selected reporting period and do not take recent configuration changes into account If you have made configuration changes, you need to wait an appropriate period of time before checking for new summary results (for example, wait 24 hours if you want to use the 24-hour reporting period). Alternatively, you can define a custom reporting period to view data only since the configuration change.

Each interface entry in the **Bandwidth Sizing** table can be expanded to display class bandwidth utilization information. Click **+** beside the interface name to expand an interface.

Selecting a Report Period

By default, the **Bandwidth Sizing** tab displays summary information for all configured interfaces for the last 24 hours. You can choose different reporting periods by clicking the **Reporting Period** list. The following reporting periods (and associated update rates) are available:

Last 1 hour – 5 minute updates
Last 12 hours – 5 minute updates
Last 24 hours – 5 minute updates
Last 48 hours – 30 minute updates
Last 7 days – 1 hour updates
Last 30 days - 3 hour updates
Last 60 days – 6 hour updates

The text at the top of the screen indicates the last time at which an update was made.

The screen itself refreshes every minute, but new measurements are displayed according to the update rate listed above for each reporting period.

Defining a Custom Report Period

When you are viewing results for an individual interface, you can define a specific custom reporting period for viewing results and generating reports.

To define a custom reporting period, you do the following:

Step 1 Click **select** beside the **From Date** field and choose a date from the calendar.

Step 2 Choose a time from the list of half-hour intervals.

Step 3 Click **select** beside the **To Date** files and choose a date from the calendar.

Step 4 Choose a time from the list of half-hour intervals.

Step 5 Click **View Period**.

When the screen refreshes the displayed information is for the time period you have defined. You can view this information or generate a report for the selected time period. The global **Select Reporting Period** field is set to Custom Period. If you click the **Related Links** for the interface, the defined custom period is used to display the related interface information.

Sorting the Bandwidth Sizing Table

The **Bandwidth Sizing** table is sorted by the **Interface Name** column by default, but you can sort this table by any column. Click the heading of the column by which you want to sort. The information in the table is then arranged from highest to lowest according to that column. You can click again to reverse the order of the sort and display results from lowest to highest.

For example, to view interfaces that have the highest calculated Congestion Indicator values, you click the **Congestion Indicator** column heading to sort. The summary is rearranged according to the maximum measured microburst values per interface, with the highest value first. Click the **Congestion Indicator** column heading again to sort the summary screen again, this time with the lowest measured maximum microburst value first.

Filtering the Bandwidth Sizing Table

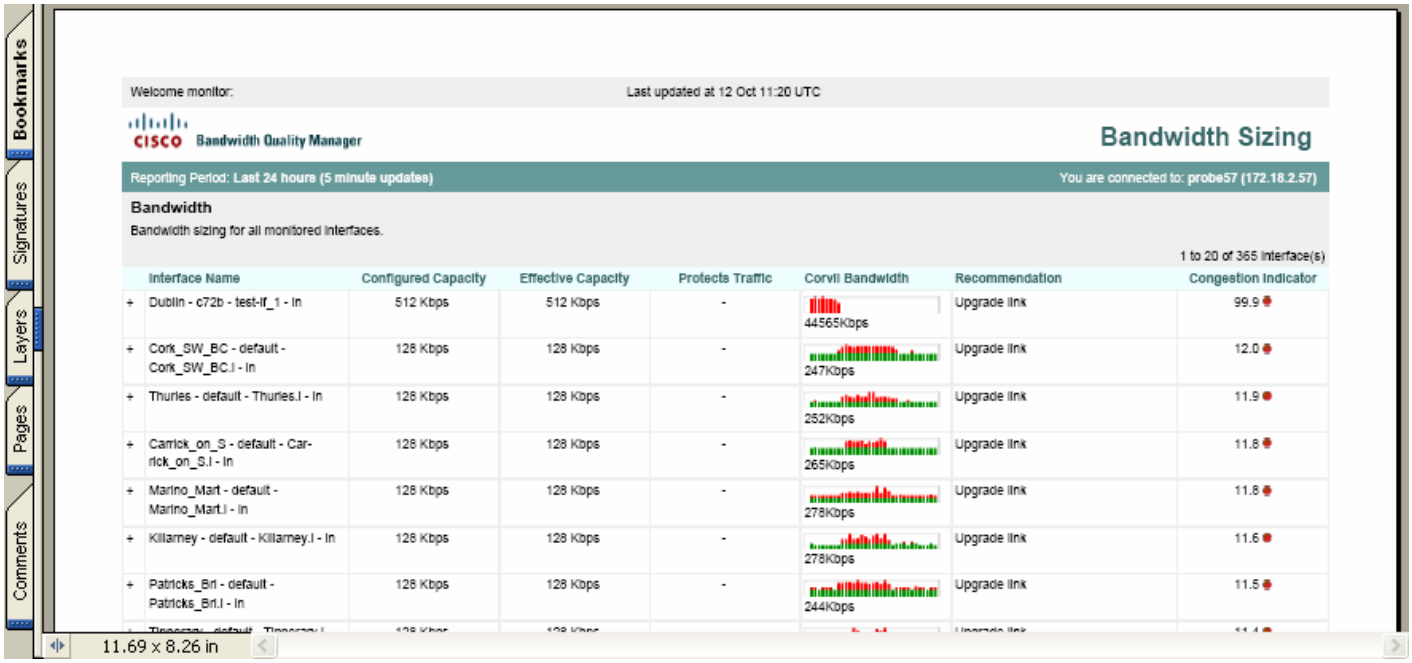
You can use the search facility on the **Bandwidth Sizing** table to display a particular interface or set of interfaces of interest. Enter the name of the required interface, or part of a name to match a group of interfaces, and click **Filter**. To clear the filter field text and return to the default display of results, click **Clear**.

The **Bandwidth Sizing** tab also provides the option to filter results based on current interface capacity or Congestion Indicator values. Click the filter symbol beside the **Current Capacity** or **Congestion Indicator** column headings and select an option from the list. The screen will refresh, displaying only the results relevant to the filtering option you selected.

Reporting Bandwidth Sizing Results

You can generate a report in .pdf format at any point when viewing congestion analysis results. To generate a report, click . The generated report is available for download in .pdf format. Reports are not stored on the BQM.

Figure 6-2: Bandwidth Sizing Report



The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all outbound 2 Gbps interfaces sorted by decreasing Congestion Indicator value over the last 7 days.
If the original results are displayed across multiple pages onscreen, then the report contains the data from all such screens in the order they were displayed at the time the report was generated.

The time displayed at the top of each report is the configured time zone of the BQM.

When a large report is being generated, the system issues a warning indicating that the action may take some time to complete.

Viewing Sizing Results

Clicking the linked interface name in the bandwidth sizing table displays the sizing information for that interface and its associated classes.

You can switch to the **Congestion Analysis** and **Traffic Insight** tab results for the interface by clicking the relevant link from **Related Links**.

You can also define a custom reporting period for viewing interface results. See “Selecting Report Period” for more information.

Note Corvil Bandwidth measures the bandwidth required by the traffic currently existing on your network to achieve the stated QoS targets. If the bandwidth available in the network changes, then the traffic may also change in response. For example, if a network is upgraded then bandwidth-limited TCP flows may increase their sending rate, or users may make more active use of particular applications. Corvil Bandwidth does not make predictions about the effect these changes could have on network QoS. Consequently, the target QoS may not be achieved after an upgrade, because of heavier network use by applications and users.

These effects are most likely to be seen in networks where QoS is currently poor, so that the network is the limiting factor for application performance. In these case the Corvil Bandwidth value does always indicate the minimum bandwidth required to meet the targets, since even the existing traffic will not achieve the targets at lower bandwidths.

If upgrading the network bandwidth results in heavier network use, so that the targets are still not achieved, then the Corvil Bandwidth value will indicate that a further upgrade is neccessary. We recommend that the Corvil Bandwidth value should be monitored continuously before and after an upgrade, in order to verify that the desired network performance is achieved.

Bandwidth Sizing Recommendations

The Bandwidth Sizing tab includes a Recommendation column indicating any required actions based on the BQM calculations. Recommended actions are available for each of the following:

- Single-class configurations
- Multi-class configurations
- Priority classes in multi-class configurations

In all cases, the recommendation is based on the Congestion Indicator values calculated for each class. In turn the Congestion Indicator calculation is based on the queuing delay target and sizing policy (for example, protect 99.9% of traffic in every 4-hour period), as configured in the associated monitor-queuing-map.

The displayed Corvil Bandwidth values can be used as a guide to bandwidth requirement if interface or class capacity upgrade is recommended or otherwise to gain insight into class bandwidth utilization. If a class receives service of at least its Corvil Bandwidth requirement, it will achieve its sizing policy and will have a Congestion Indicator of less than one.

Note In a multi-class configuration it is possible to see reported Corvil Bandwidth values that exceed both the configured and effective minimum capacities of classes, but where Congestion Indicator values are low (less than one) and no particular action is recommended. In such cases, the class is receiving more than its guaranteed share of the bandwidth due to bandwidth sharing, and is achieving its sizing policy.

Single class Configuration Recommendations

In single class configurations, the same recommendation is displayed for both the interface and the single class.

No action required - The sizing policy has been achieved.

Upgrade link – In this case the Congestion Indicator is greater than one and the sizing calculation is dominated by the delay target. The recommendation reflects the fact that if the interface capacity is increased to the displayed Corvil Bandwidth, then the sizing policy will be achieved.

Increase buffer – In this case the Congestion Indicator is greater than one and the sizing calculation is dominated by loss. The loss is due to packets being dropped because of queue buffer overflow, so the recommended action is to increase the buffer size. The current buffer size is displayed with the sizing graph. The displayed Corvil Bandwidth indicates the bandwidth required to achieve the sizing policy using the current buffer size.

Multi-class Configuration Recommendations

In multi-class configurations, the following recommendations may be displayed:

No action required - The sizing policy has been achieved.

Adjust policy or upgrade link – This message is shown at the interface level for a multi-class configuration, and indicates that one or more classes have not achieved the sizing policy. Expand the interface to learn more about the specific class recommendations. No Corvil Bandwidth values are displayed at the interface level in multi-class configurations.

Class requires more bandwidth - In this case the Congestion Indicator for the class is greater than one and the sizing calculation is dominated by the delay target. The queuing delay can be reduced to the target levels by increasing the bandwidth available to the class, hence the recommendation. The Corvil Bandwidth for the class gives the actual bandwidth required by the class to achieve the sizing policy. In a multi-class case, a class is guaranteed to receive its effective capacity, but typically receives more than this due to bandwidth sharing between classes.

Increase buffer - In this case the Congestion Indicator is greater than one and the sizing calculation is dominated by loss. The loss is due to packets being dropped because of queue buffer overflow, so the recommended action is to increase the buffer size. The current buffer size is displayed with the sizing graph. The displayed Corvil Bandwidth is the actual bandwidth required to achieve the sizing policy using the current buffer size. Note that due to bandwidth sharing between classes, the actual bandwidth received by a class will usually exceed the guaranteed minimum effective capacity.

Priority Class in a Multi class Configuration Recommendations

The Bandwidth Sizing results also provide recommendations for configured priority classes in LLQ systems:

Adjust policer parameters – In this case the BQM calculations predict policer drops in excess of those permitted by the sizing policy. This indicates that, depending on the existing configuration, the problem is due either to an insufficient priority bandwidth or an insufficient burst-size value in the associated policy-map. In most cases, you can use the reported Corvil Bandwidth value as a guide to the required priority bandwidth value to avoid policer drops.

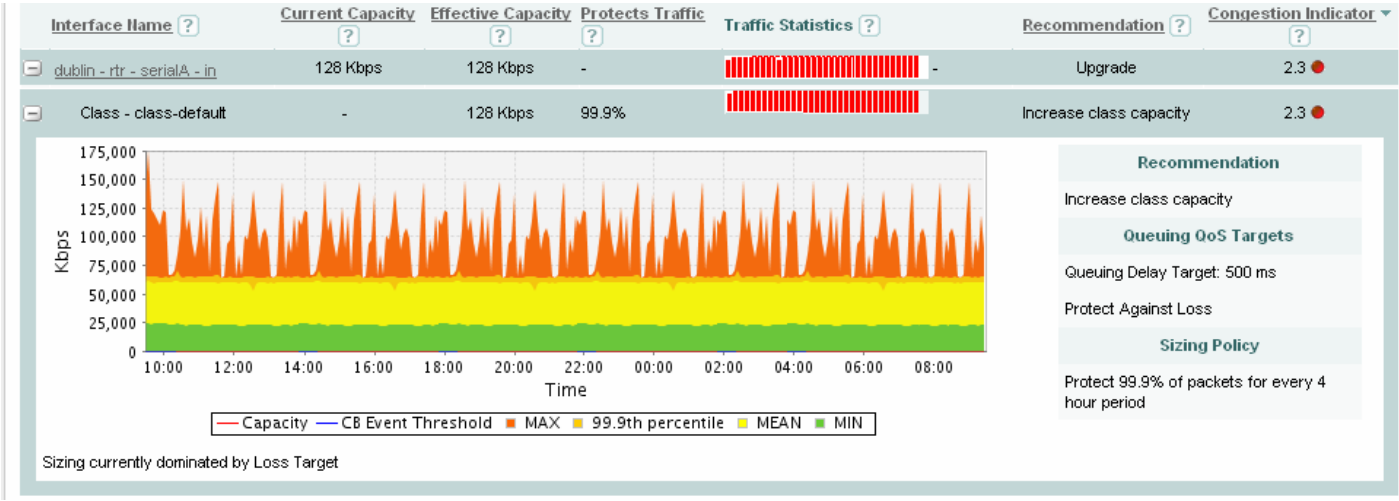
Increase burst-size – This case typically means that there are packets that are larger than the configured policer burst size. To avoid dropping these packets, it is necessary to increase the policer burst size. The packet-size distribution for the LLQ class can be used to determine an appropriate burst-size.

Adjust policer parameters and upgrade link or **Increase burst size and upgrade link** – In certain situations, the BQM calculations may show that, in addition to expected policer drops, priority class packets are being delayed beyond the delay threshold. Changing the priority bandwidth does not affect delay, so an additional recommendation to upgrade the interface bandwidth is made in this case.

Viewing the Sizing Graph

When you expand a class from the list, the relevant graphs and charts are available to view for the chosen class.

Figure 6-3: Bandwidth Sizing Graph



The Corvil Bandwidth graph plots the bandwidth required to meet the configured delay target, protect against packet loss due to queue buffer overflow for the chosen class, or protect against policer drops in the case of a configured priority class. The text below the graph indicates whether meeting the configured delay target or protecting against packet loss is driving the plotted Corvil Bandwidth values.

The current configured queuing targets and sizing policy are listed beside the graph. For example, if the configured delay target is 150 ms, and the sizing policy protects 99.9% of traffic in every four-hour period, then the summary Corvil Bandwidth value displays the bandwidth required to ensure that no more than 0.1% of packets in the class traffic is delayed by more than 150 ms in any four-hour period.

Each bar on the Corvil Bandwidth graph shows the bandwidth required to protect packets in the time interval covered by that bar. The summary Corvil Bandwidth value shown for the class is the bandwidth required to protect the configured parentage of packets in every busy period included in the reporting period, where the busy period is specified in the associated monitor-queuing-map.

The Corvil Bandwidth values are displayed as a series of values in kbps for each five minutes during the reporting period. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values (in kbps) calculated each five minutes during the chosen reporting period.
x% - the x^{th} percentile of Corvil Bandwidth values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the monitor-queuing-map being applied to the class. If none has been configured, the system defaults to the 99th percentile.
Mean –the mean of the Corvil Bandwidth values for each five minutes during the chosen reporting period
Min –the minimum of the Corvil Bandwidth values for each five minutes during the chosen reporting period.

If you make a configuration change, for example, adjusting the sizing policy in the monitor-queuing-map, then the graph is marked at the point at which the configuration change occurred.

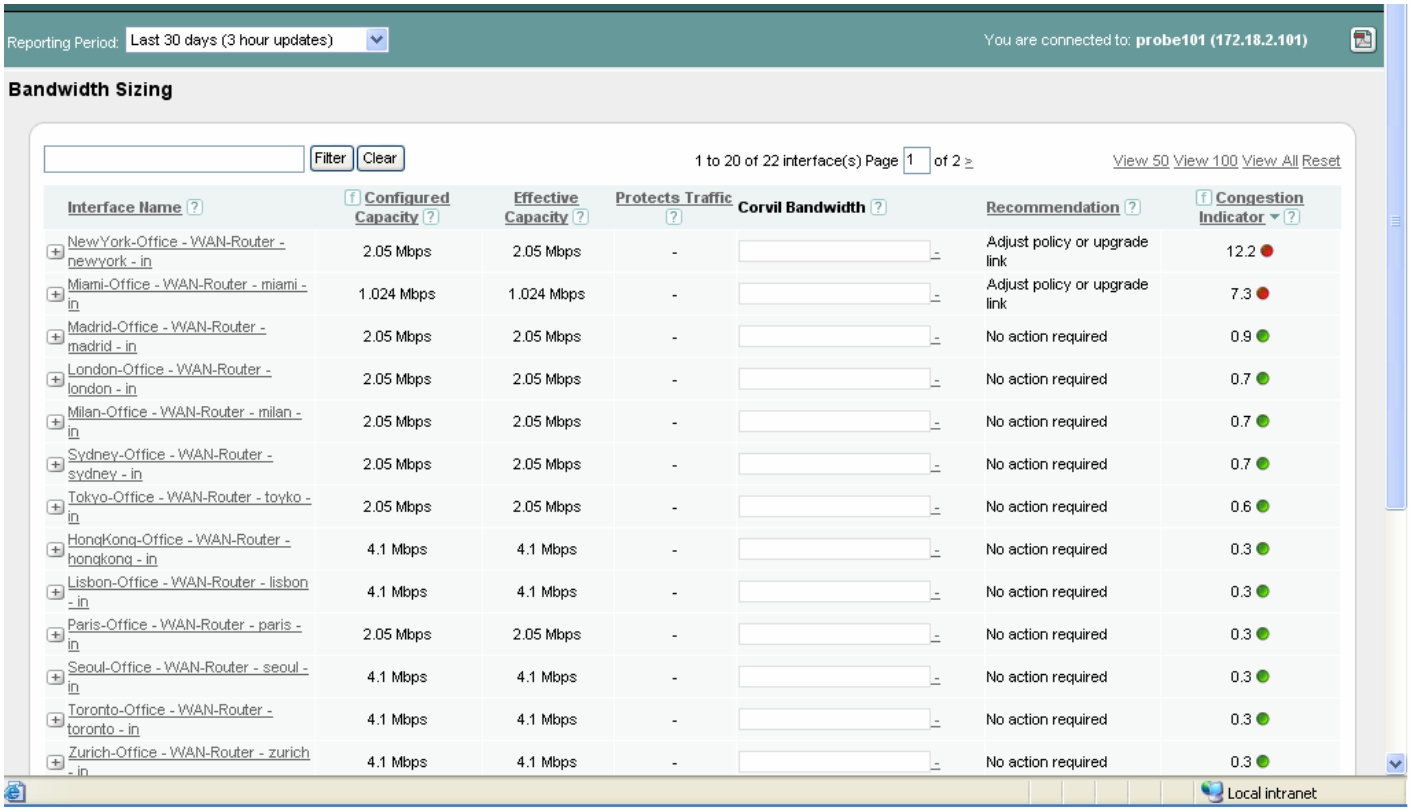
Note . The summary data (including recommendations) displayed for an interface or class does not take configuration changes into account immediately. The displayed summary data is based on the reporting period, so you need to wait until an appropriate period of time has passed after a configuration change before checking recommendations and Corvil Bandwidth values.

Monitoring Single-class Sizing Requirements

The following example scenario shows how you can use the BQM to monitor bandwidth resource requirements on a single-class network. Each quarter, we look at the **Bandwidth Sizing** tab and select the 30-day reporting period.

We sort the view to determine the branches currently showing thegreatest Congestion Indicator values.

Figure 6-4: Bandwidth Sizing



In this example we decide to investigate the worst 10 for this quarter. For each branch remote site, we check top talkers and top applications for normal usage patterns.

In this case, one of the sites shows a rogue application consuming significant bandwidth for which we take corrective action. The other sites are upgraded as recommended.

We expand these results (shown in the default class) and view the Corvil Bandwidth plot, the sizing policy, and the individual busy period driving the Corvil Bandwidth result.

Monitoring Multi-class Sizing Requirements

The following example scenario shows how you can use the BQM to monitor bandwidth resource requirements on a multi-class network. Some classes in the multi-class network are recommending an upgrade but the corresponding Congestion Indicator is less than one. This can happen when the class is actually served more bandwidth than the reserved bandwidth.

You can check this situation by clicking the related link to the **Congestion Analysis** tab and examining the expected queuing delay and expected queuing loss plots.

If these are both showing no issues, the recommendation can be ignored.

If a class is experiencing greater than one, then this class needs greater reserved bandwidth.

If other classes have a Congestion Indicator significantly less than one, the reserved bandwidth may be reduced. Thus by balancing the reserved bandwidth, you may be able to achieve the required quality on all classes without an bandwidth upgrade.

Otherwise, you must upgrade the link and then perform the balancing.

Identifying New Class Resource Requirements

The following example scenario shows how you can use the BQM to identify class resource requirements on a multi-class network.

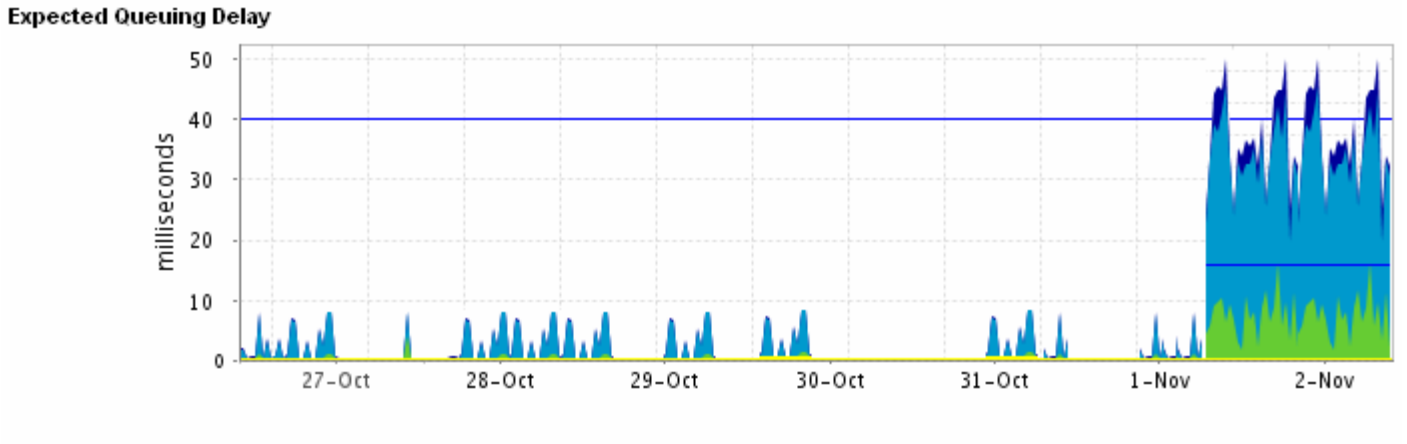
Figure 6-4:Branch Office Dashboard Congestion Indicator

In this example, the dashboard is showing a remote site representing a branch office as having a Congestion Indicator of 2.2.

Next, we navigate to the **Congestion Analysis** tab for the branch remote site.

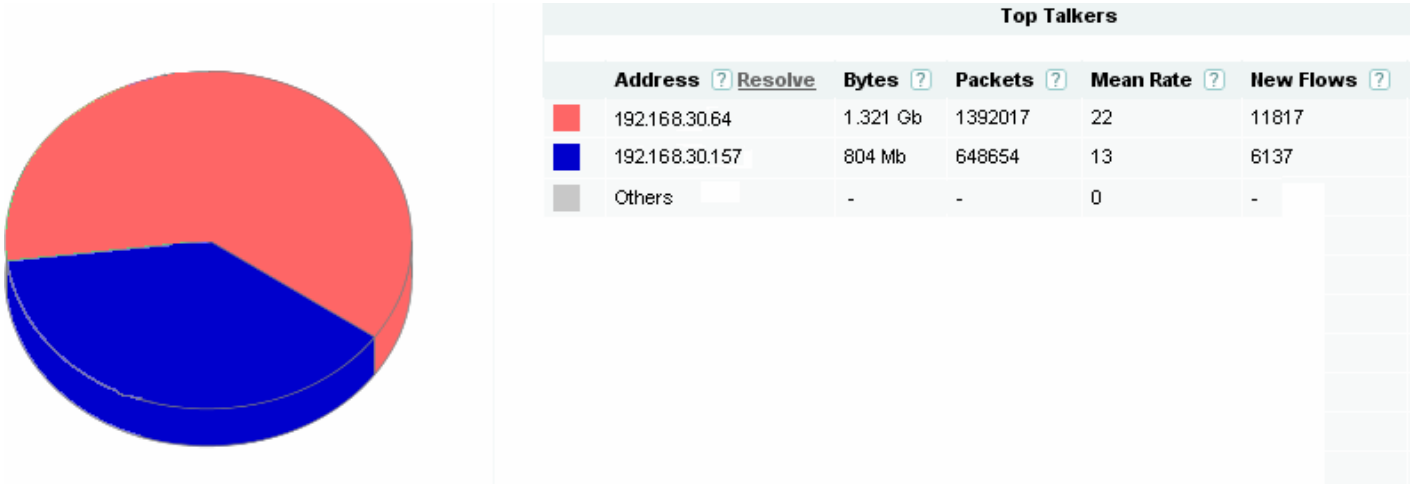
The Congestion Indicator value is caused by the delay in the video class being above the specified threshold of 40 ms. We expand the reporting period to 7 days, and this shows a steep increase in the delay being experienced from 24 hours earlier.

Figure 6-5:Increased Delay



We navigate to the **Traffic Insight** tab using the **Traffic Insight** related link and see that the top talkers in the video class show two IP source addresses, rather than the expected one.

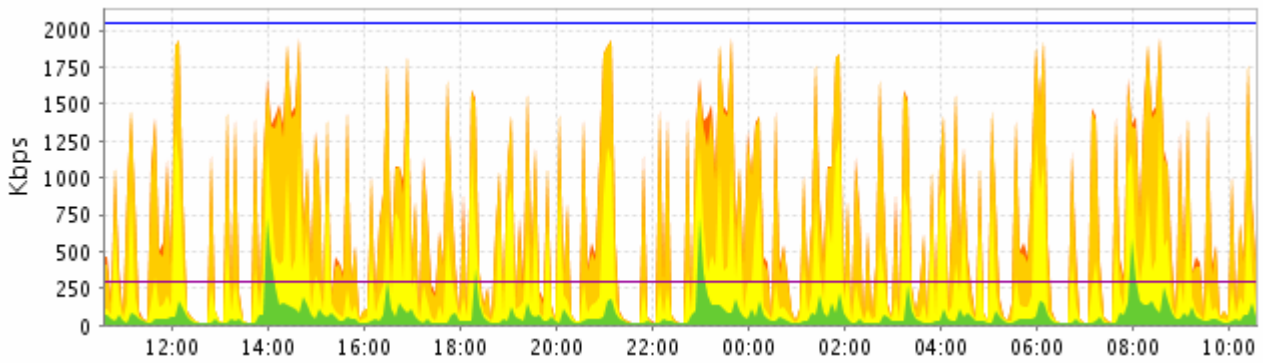
Figure 6-6:Top Applications



In this example, someone had installed a second video conference unit without notifying networks.

We navigate to the bandwidth sizing related link and views sizing information for the video class over the past 24 hours.

Figure 6-7: 24-hour Class Sizing Results



We can then submit a network change to increase the size of the video class.

7 Using the Command Line Interface (CLI)

This chapter introduces the main features of the BQM command line interface (CLI):

- Introduction to CLI modes
- Using the Help Feature
- Completing a Partial Command Name
- Using the Show command to review the BQM configuration
- Using the Status command to review the BQM operational information
- Continuing Output at the - -More- - Prompt
- Deleting Configuration Objects and Entries
- Saving and Restoring Configuration Changes

You use the CLI to access and configure the BQM. Because the CLI is divided into different configuration modes, the commands available to you at any given time depend on the mode you are currently in. You can use the **help** command at the CLI prompt to display a brief description of each available command as well as the context from which it comes. For more information on the commands available in each mode, see *BQM Commands*.

Introduction to the CLI

You use the BQM CLI to configure the device. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

You can log in to the BQM as one of the following users:

- admin
- config

When you log in to the CLI, you are in global configuration mode. To have access to all commands, you must enter the other configuration modes. Configuration modes allow you to make changes to the running configuration. All valid changes to the running configuration are automatically stored and used when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter a variety of other modes.

The following modes are available in the BQM command line interface (CLI):

- Configuration mode
- Monitor-queuing-map configuration mode
- Monitor-end-to-end-map configuration mode
- Custom application configuration mode
- Class-map configuration mode
- Policy-map configuration mode
- Policy-map class configuration mode
- Local and Remote site, router and interface configuration modes
- Packet capture configuration mode
- SNMP-server configuration mode

If you log in as a config user you have access to the basic set of administrative commands. If you log in as an admin user, you also have additional administration commands available. When you log in as an admin user, the CLI prompt ends in a dollar ($) symbol. If you are logged in as a config user, the CLI prompt ends with the hash (#) symbol. The idle/inactivity timeout period on the BQM is 20 minutes. So after 20 minutes without interacting with the BQM CLI you will be automatically logged out.

The configuration mode allows you to make changes to the BQM configuration. Valid configuration changes are automatically saved and these changes are restored when the BQM is rebooted.

You can quit out of policy-map, class-map, policy-map class, or interface configuration mode back to the global configuration mode at any time by pressing Ctrl+Z.

Using the Help Feature

You can use the BQM CLI help features to find out more information about the commands available in a given mode, and what each command does. Entering a question mark (**?**) at the CLI prompt displays a list of all commands available in the current mode, including those inherited from parent modes.

You get a brief description of these commands by using the **help** command in the following way:

```
host(config)$ help
  allow                Restricts network access to the device.
  capture              Configures a packet capture instance
  class-map            Configure a class-map
  clear                Reset functions
  clock                Configure time-of-day clock.
  local-site             Configure a local-site
  copy                 Copy from a source to a destination
  custom-application   Configure a custom-application
  delete               Delete files from a filesystem
  dir                  List files on a filesystem
  enable               Enables a configured packet capture instance
  end                  Returns to base context
  exit                 Exit configuration mode or EXEC
  help                 Lists commands that can be run
  license              Displays the license file
  log                  Displays the end of the local system log file.
  logging              Configures parameters of the remote logging system.
  logout               Logs out a user
  monitor-queuing-map  Configure a monitor-queuing-map
  no                   Reverses next command, such as creation of a class-
map.
  ntp                  Configures Network Time Protocol Services.
```

```
  password            Sets your login password
--More--
```

To get a brief description of an individual command, in this example the **class-map** command, use the form **help** <command name>:

```
host(config)# help class-map
class-map:
usage:       class-map [match-any|match-all] <name>

Creates a class-map entry.  The class-map can be 'match-any' where only
one of the rules need match for the class-map to be matched. 'match-all'
class-maps require that all rules in the class-map be matched. The default
is 'match-any'.

<name> must be a unique class-map name.

Use 'no class-map <name>' to delete a class-map. Use ‘no class-map *’ to
delete all class-maps
host(config)#
```

Completing a Partial Command Name

To reduce the amount of typing you have to do, enter the first few letters of the command, then press the Tab key.

The CLI will recognize a command if you have entered enough characters to make the command unique.

For example, if you enter **sho** the CLI will be able to associate your entry with the **show** command, because only the **show** command begins with **sho**:

```
host(config)# sho<Tab>
host(config)# show
```

When you use the command completion feature the CLI displays the full command name. The command is not executed until you press Enter. This way you can modify the command if necessary.

In the current release short commands names are not available. For example, to run the **show version** command you must type the full command, typing ‘sh ver’ or other abbreviation will not work.

Using the Show Command

You can use the **show** command to review the complete configuration on the BQM and verify its operation. The **show** command output includes the contents of the class-map, interface, and policy-map lists. You can use this output to review match rule configuration for each class-map within the class-map list. You can also check that measurements have been configured for each class in the policy-map list.

You can see whether the configuration on the BQM is active, and review the configured information. The displayed information includes a status for each measurement (green or amber), and an incremental byte and packet count. So you can use the **show** command to check if byte and packets counts are incrementing. In other words, you can verify traffic measurement is taking place.

You can also see the administration details at the end of the output. This information includes the remote logging status, access control information, interface configuration information, and the configured SNMP

details. For more information on BQM logging and SNMP information, see the chapter “System Administration.”

You use the **show config** command to list the configuration changes made to the default configuration.

Using the Status Command

You can use the **status** command to check the status of the BQM. The **status** command returns information about the BQM, such as the software version, CPU information, and memory usage details.

For more information on the information you can get from the status command, see the chapter “System Administration.”

Continuing Output at the --More-- Prompt

When you are using the BQM CLI, output may extend beyond the visible terminal screen length. For cases where output continues beyond the bottom of the screen, such as with the output of ?, **show**, or **status** commands, the output is paused and a --More-- prompt is displayed at the bottom of the screen. To resume output, press Enter to scroll down one line, or press the Spacebar to display the next full screen of output. To cancel command output and go back to the command prompt, press q, Ctrl+Z, or Ctrl+C.

Deleting Configuration Objects and Entries

Nearly all BQM configuration commands have a **no** form. In general, you use the **no** form of the command to delete an object or entry. Note that an object that is being used by another object cannot be deleted. So an interface using a certain policy-map must be deleted before that policy-map, and in turn, a policy-map using a certain class-map must be deleted before that class-map. Similarly, when nesting class-maps, the containing class-map must be deleted before any class-map nested within it.

For example, to delete a class-map named class_map1, use the **no** form of the **class-map** command:

```
host(config)# no class-map class_map1
```

You can also use the ‘delete all’ form using the wildcard symbol (*), for example **no class-map *,** to delete a number of objects at the same time. See “BQM Commands” for more details about using the **no** command.

To restore the default configuration and delete any configuration changes that have been made with a single command, you use the **clear config** command.

```
host(config)# clear config
Are you sure you want to clear config (y/n)?
```

Saving and Restoring Configuration Changes

You use the **copy** command in configuration mode to save the current configuration. This will be the configuration used by the BQM if it is shut down and rebooted.

To save the current configuration, you use the following command:

```
copy config
```

Logging Out of the BQM CLI

Enter the **logout** command at any time to end your configuration session and log out of the BQM:

```
host(config)# logout
```

If the current in-memory configuration (running configuration) is different from that stored on disk (startup configuration), the system displays a warning message indicating that there are unsaved changes and asking if you want to save them by entering 's', cancel the logout by entering 'c', or logout without saving by entering 'l':

```
The configuration has unsaved changes. Please choose one of the following:
save changes and logout (s), cancel logout (c), logout without saving (l)?
```

Configuring the BQM Using the CLI

As is the case when using the GUI, you configure the BQM in a certain order with monitor-queuing-maps configured first, class-maps configured before policy-maps, and all of these configured before sites, routers and interfaces. Custom applications can be configured outside this necessary ordering.

Defining a Monitor-Queuing-Map

The purpose of a monitor-queuing-map is to enable BQM measurements and define QoS targets to apply to those measurements. The monitor-queuing-map can also be used to define measurement thresholds at which event detection is triggered. You use the **monitor-queuing-map** configuration command to create a monitor-queuing-map. The syntax of the class-map command is as follows:

monitor-queuing-map *name*
no monitor-queuing-map *name*

The following table describes the configuration commands available from the monitor-queuing-map context:

Table 7-1 Monitor-Queuing Map QoS Commands

Command	Description
`description`	Specifies a text description for the monitor-queuing-map.
`estimate-service-level`	Specifies that calculation of Congestion Indicator, Expected Delay and Expected Loss is enabled and sets optional event detection thresholds based on configured queuing targets (delay).
`measure-bandwidth [event-threshold {bandwidth` *`kbps`* `| percent` *`percent`*`}]`	Specifies that Corvil Bandwidth measurement is enabled based on the configured queuing targets, and sets an optional threshold at which to trigger event detection.
`measure-microburst milliseconds` *`msecs`* `[event-threshold {bandwidth` *`kbps`* `| percent` *`percent`*`}]`	Specifies that microburst measurement is enabled at the specified resolution (in milliseconds), and sets an optional threshold at which to trigger event detection.

`queuing-targets [delay-milliseconds` *`msecs`*`]`	Specifies the delay target in milliseconds and enables loss tracking for Corvil Bandwidth calculation, expected service level and bandwidth sizing.
`size-for`	Specifies the percentile and busy period values for bandwidth sizing. The configured percentile value is also used to display graph data.

For more details on the full syntax and examples of the use of each command, see the "Command Reference" chapter of this document.

In the following example, a monitor-queuing-map named realtime is created with Corvil Bandwidth explicitly enabled, a microburst measurement and queuing targets configured. Microbursts down to 150 milliseconds in duration will be measured and the delay target which must be met when calculating Corvil Bandwidth values is 150 milliseconds:

```
monitor-queuing-map realtime
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
```

No thresholds for triggering event detection are configured in this example.

Defining a Monitor End to End Map

The purpose of a monitor-end-to-end-map is to define the required end-to-end QoS monitoring features, and associated quality event detection thresholds, for traffic from the local site to remote sites. A monitor-end-to-end-map comprises the following: a name, ping interval and packet size settings, and associated delay and loss event detection thresholds. A monitor-end-to-end-map establishes an end-to-end delay and loss-based event detection policy or traffic between the local site and remote sites.

The system provides a default monitor-end-to-end-map, named end2end-target-default. The default monitor-end-to-end-map cannot be deleted.

You use the **monitor-end2end-map** configuration command to create a monitor-end-to-end-map. The syntax of the class-map command is as follows:

monitor-end2end-map *name*
no monitor-end2end-map *name*

The following table describes the configuration commands available from the monitor-end2end-map context:

Table 7-2 Monitor-End-to-End-Map QoS Commands

Command	Description
`description`	Specifies a text description for the monitor-end2end-map.
`measure-ping`	Specifies the ICMP ping packets parameters and optional thresholds at which to trigger event detection.

For more details on the full syntax and examples of the use of each command, see the “Command Reference” chapter of this document.

In the following example, a monitor-end2end-map named Dublin-NYC is defined. If any packets are lost, event detection is triggered:

```
monitor-end2end-map Dublin-NYC
    measure-ping interval-milliseconds 10000 size-bytes 36 availability-threshold 10
    event-thresholds loss
```

Defining a Class Map

You configure class-maps to classify traffic and establish the traffic classification scheme to be used in the defined traffic policy (policy-map) for an interface. You use the **class-map** configuration command to create a traffic class.

A class-map comprises the following: a name, a series of match rules, and, if more than one match rule is defined, an instruction on how to evaluate these match commands. The match rules are used to specify various criteria for classifying packets. If a packet matches the specified criteria, that packet is considered a member of the class and is processed according to the QoS specifications set in the traffic policy. Packets that do not meet any of the configured match rules are classified into the default traffic class.

The system provides a default class, named class-default. This default class is automatically applied when you define a single-class policy-map. The default class cannot be deleted.

If you are modeling a multi-class configuration on the router of interest, you define multiple class-maps as appropriate. These class-maps are then each referenced in the multi-class policy-map that you define.

The syntax of the class-map command is as follows:

class-map [match-any | match-all] *class-name*
no class-map [match-any | match-all] *class-name*

The match all and match any options need to be specified only if more than one match rule is configured in the traffic class. The class-map can be 'match-any' where only one of the rules need match for the class-map to be matched. A 'match-all' class-map requires that all rules in the class-map be matched. The default is 'match-any'.

You use the **match not** command to specify a match rule that prevents a packet from being classified as a member of the class. For example, if the **match not ip dscp 6** command is issued while you configure the traffic class, the packets with a dscp setting of 6 are not considered a successful match. All other ip dscp values would be successful match criteria.

For additional information on using the match-any and match-all options, see the “Class-maps and Classification” Appendix of this document.

To create a traffic class containing match criteria, use the **class-map** configuration command to specify the traffic class name, and then use the following **match** commands in class-map configuration mode, as needed:

Table 7-3 Class match Commands

Command	Description
`match any`	Specifies that all packets will be matched.
`match application`	Specifies the name of an application to be used as a matching rule.
`match not` *`match-criteria`*	Specifies a match rule value that prevents packets from being classified as members of a specified traffic class. All other values of that particular match rule belong to the class.
`match class-map` *`class-name`*	Specifies the name of a traffic class to be used as a matching rule (for nesting traffic classes [nested class-maps] within one another).
`match ethertype` *`ethertype value`*	Specifies the ethertype value used to match traffic based on Ethernet Type field of the Ethernet MAC header (assuming Ethernet Type II frames).
`match ip`	Configures the match criteria for a class-map to be successful for IP packets, subject to certain specified conditions
`match ip dscp` *`ip-dscp-value`*	Specifies up to 21 well-known differentiated services code point (DSCP) values used as match criteria, or alternatively a numeric value. The value of each service code point is from 0 to 63.
`match ip precedence` *`ip-precedence-value`*	Specifies up to eight well-known IP Precedence values used as match criteria, or alternatively a numeric value from 0 to7.
`match mpls` *`match-criteria`*	Specifies the Multiprotocol Label Switching (MPLS) values to use as match rule against which packets are checked to determine if they belong to the class.
`match tcp` *`match-criteria`*	Configures the match criteria for a class-map to be successful for TCP traffic, subject to certain specified conditions.
`match udp` *`match-criteria`*	Configures the match criteria for a class-map to be successful for UDP traffic, subject to certain specified conditions.
`match vlan` *`vlan-id`*	Configures the match criteria for a class-map to be successful for encapsulated VLAN traffic.

For more details on the full syntax and examples of the use of each command, see the “Command Reference” chapter of this document.

In the following example, two traffic classes are created and their match criteria are defined. For the first traffic class called class1, the match rule is configured to be successful for IP packets with source address 172.16.1.10. For the second traffic class called class2, the match criterion is IP packets with source address 172.16.1.10. Packets are checked against these match rules to determine if they belong to the class:

```
class-map class1
     match ip src=172.16.1.10
```

```
class-map class2
      match ip src=172.16.1.11
```

Using Nested Class-maps

There are two reasons to use the **match class-map** command:

- Combining “match-all” and “match-any” statements in a single traffic class
- Maintenance - if a long traffic class currently exists, using the **match class-map** match rule requires less effort than retyping the same traffic class configuration.

Combining match-all and match-any Statements

The usual reason for using the **match class-map** command is to combine match-any and match-all statements in the same traffic class. To do this you create a traffic class using one match criteria evaluation instruction (either match-any or match-all) and then use this traffic class as a match rule in a traffic class that uses a different match criteria type. The only method of mixing “match-all” and “match-any” statements in a traffic class is through the use of the traffic class match rule.

Consider the following example. Suppose A, B, C, and D are all separate match rules, and you want to define a traffic class matching the following:

A, B, or C and D (A OR B OR [C AND D])

Using a “match-all” set of match rules results in the following:

A AND B AND C AND D.

Using a “ match-any” set of match rules results in the following:

A OR B OR C OR D.

So you cannot combine "AND" (match-all) and "OR" (match-any) statements within the traffic class.

The solution is to create a single “match-all” traffic class for C and D. For the purposes of this example, call it rule E. You then create a new “match-any” traffic class using A, B, and E. The new traffic class would have the correct evaluation sequence (A OR B OR E, which is equivalent to A OR B OR [C AND D]).
The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command.

The result of traffic class class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class class1:
source IP address 172.16.1.10 and mpls experimental value four, or destination IP address 10.1.2.15, or source IP address 172.16.0.0.

In this example, only the traffic class called class4 is used with the traffic policy called policy1.

```
class-map match-all class3
      match ip src=172.16.1.10
      match mpls experimental 4

class-map match-any class4
      match class-map class3
      match ip dst=10.1.2.15
      match ip src=172.16.0.0/16

policy-map policy1
      class class4
```

```
            bandwidth percent 10
          queue-limit 64
```

Maintenance

In the following example, the traffic class called netmgmt includes some of the characteristics of traffic class snmp, as well as a number of other tcp and udp port number rules. Rather than configuring the snmp port numbers again, line by line, the match class-map command is used. This command allows all of the characteristics in the traffic class called snmp to be included in the traffic class called netmgmt, and the additional network management port numbers can be accounted for without reconfiguring the entire traffic class.

```
class-map snmp.c
      match tcp port=161
      match udp port=161
      match tcp port=162
      match udp port=162

class-map netmgmt.c
      match class-map=snmp.c
      match tcp port=23
      match tcp port=22
      match udp port=514
      match udp port=67:68
```

Converting Network-Based Application Recognition (NBAR) Configurations

If you are using Network-Based Application Recognition (NBAR) on the router being modeled in the BQM configuration, you need to convert the NBAR match rules from the router configuration to equivalent BQM match rules. In general this involves replacing NBAR **match protocol** commands in the router configuration with **match tcp port=**<*port-number*> or **match udp port=**<*port-number*> commands in the BQM configuration as appropriate.

The following tables identify the NBAR protocols using well-known port numbers and the equivalent BQM command required:

Table 7-4: Converting NBAR Configuration – Non-TCP and Non-UDP Protocols

Protocol	Type	Well-Known Port Number	BQM Command(s)	Description
egp	IP	8	match ip protocol=8	Exterior Gateway Protocol
gre	IP	47	match ip protocol=47	Generic Routing Encapsulation
icmp	IP	1	match ip protocol=1	Internet Control Message Protocol
ipinip	IP	4	match ip protocol=4	IP in IP
ipsec	IP	50, 51	match ip protocol=50 match ip protocol=51	IP Encapsulating Security Payload/Authentication Header
eigrp	IP	88	match ip protocol=88	Enhanced Interior Gateway Routing Protocol

Table 7-5: Converting NBAR Configuration – TCP and UDP Static Port Protocols

Protocol	Type	Well-Known Port Number	BQM Command(s)	Description
BGP	TCP/UDP	179	match tcp port=179 match udp port=179	Border Gateway Protocol
CU-SeeMe	TCP/UDP	7648, 7649	match tcp port=7648 match udp port=7648 match tcp port=7649 match udp port=7649	Desktop videoconferencing
CU-SeeMe	UDP	24032	match udp port=24032	Desktop videoconferencing
DHCP/Bootp	UDP	67, 68	match udp port=67 match udp port=68	Dynamic Host Configuration Protocol/Bootstrap Protocol
DNS	TCP/UDP	53	match tcp port=53 match udp port=53	Domain Name System
Finger	TCP	79	match tcp port=79	Finger User Information Protocol
Gopher	TCP/UDP	70	match tcp port=70 match udp port=70	Internet Gopher Protocol
HTTP	TCP	80	match tcp port=80	Hypertext Transfer Protocol
HTTPS	TCP	443	match tcp port=443	Secured HTTP
IMAP	TCP/UDP	143, 220	match tcp port=143 match udp port=143 match tcp port=220 match udp port=220	Internet Message Access Protocol
IRC	TCP/UDP	194	match tcp port=194 match udp port=194	Internet Relay Chat
Kerberos	TCP/UDP	88, 749	match tcp port=88 match udp port=88 match tcp port=749 match udp port=749	The Kerberos Network Authentication Service
L2TP	UDP	1701	match udp port=1701	L2F/L2TP Tunnel
LDAP	TCP/UDP	389	match tcp port=389 match udp port=389	Lightweight Directory Access Protocol
MS-SQLServer	TCP	1433	match tcp port=1433	Microsoft SQL Servertop videoconferencing
NetBIOS	TCP	137, 139	match tcp port=137 match tcp port=139	NetBIOS over IP (Microsoft Windows)

NetBIOS	UDP	137, 138	match udp port=137 match udp port=138	NetBIOS over IP (Microsoft Windows)
NFS	TCP/UDP	2049	match tcp port=2049 match udp port=2049	Network File System
NNTP	TCP/UDP	119	match tcp port=119 match udp port=119	Network News Transfer Protocol
Notes	TCP/UDP	1352	match tcp port=1352 match udp port=1352	Lotus Notes
NTP	TCP/UDP	123	match tcp port=123 match udp port=123	Network Time Protocol
PCAnywhere	TCP	5631, 65301	match tcp port=5631 match tcp port=65301	Symantec PCAnywhere
PCAnywhere	UDP	22, 5632	match udp port=22 match udp port=5632	Symantec PCAnywhere
POP3	TCP/UDP	110	match tcp port=110 match udp port=110	Post Office Protocol
PPTP	TCP	1723	match tcp port=1723	Point to Point Tunneling Protocol
RIP	UDP	520	match udp port=520	Routing Information Protocol
RSVP	UDP	1698,1699	match udp port=1698 match udp port=1699	Resource Reservation Protocol
SFTP	TCP	990	match tcp port=990	Secure FTP
SHTTP	TCP	443	match tcp port=443	Secure HTTP
SIMAP	TCP/UDP	585, 993	match tcp port=585 match udp port=585 match tcp port=993 match udp port=993	Secure IMAP
SIRC	TCP/UDP	994	match tcp port=994 match udp port=994	Secure IRC
SLDAP	TCP/UDP	636	match tcp port=636 match udp port=636	Secure LDAP
SNNTP	TCP/UDP	563	match tcp port=563 match udp port=563	Secure NNTP
SMTP	TCP	25	match tcp port=25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161, 162	match tcp port=161 match udp port=161 match tcp port=162 match udp port=162	Simple Network Management Protocol
SOCKS	TCP	1080	match tcp port=1080	Firewall security protocol

SPOP3	TCP/UDP	995	match tcp port=995 match udp port=995	Secure POP3
SSH	TCP	22	match tcp port=22	Secured Shell
STELNET	TCP	992	match tcp port=992	Secure TELNET
Syslog	UDP	514	match udp port=514	System Logging Utility
Telnet	TCP	23	match tcp port=23	Telnet Protocol
X Windows	TCP	6000-6003	match tcp port=6000 match tcp port=6001 match tcp port=6002 match tcp port=6003 or match tcp port=6000:6003	X11, X Windows

Defining a Policy Map

The purpose of a policy-map is to establish a traffic policy that applies the required QoS features to the classified traffic. A policy-map comprises the following: a name, one or more traffic classes (previously defined by class-maps) and the QoS policies and associated quality event detection thresholds (previously defined by monitor-queuing-maps). To configure a traffic policy, you use the **policy-map** command to specify the traffic policy name. You use the **class** command to associate a previously defined class-map with the traffic policy. You must use the **class** command in policy-map configuration mode. When you have entered a **class** command, you are automatically brought to policy-map class configuration mode. This is also where the QoS policies defined in the monitor-queuing-map are associated with the class using the **monitor-queuing** command.

The syntax of the policy-map command is as follows:

policy-map *policy-name*
no policy-map *policy-name*

The syntax of the class command is as follows:

class *class-name*
no class *class-name*

The syntax of the monitor-queuing command is as follows:

monitor-queuing *monitor-queuing-map-name*
no monitor-queuing *monitor-queuing-map-name*

All traffic that fails to meet the matching criteria belongs to the default traffic class. You can edit the configuration of the default class, but you cannot delete it.

To create a traffic policy, use the following commands:

Table 7-4 Policy-map Commands

Command	Description
`policy-map` *`policy-name`*	Specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
`class` *`class-name`*	Specifies the name of a predefined traffic class, which was configured with the class-map command, used to classify traffic to the traffic policy.
`class class-default`	Configures the properties of the default class created as part of the traffic policy.
`bandwidth {`*`bandwidth-kbps`* `|remaining percent` *`percent`* `| percent` *`percent`*`}`	Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. A minimum bandwidth guarantee can be specified in kbps, a relative percentage of unknown available bandwidth or by an absolute percentage of the known available bandwidth for a bandwidth class.
`class-adjust`	Specifies how much (in bytes) to adjust the size of a packet that matches the current class.
`priority {`*`kbps`* `| percent` *`percent`*`} [`*`burstbytes`*`]`	Specifies the guaranteed allowed bandwidth, in kbps or percentage, for priority (time-sensitive) traffic. The optional bytes argument controls the size of the burst allowed to pass through the system without being considered in excess of the configured kbps or percentage rate.
`priority-level {high | medium | normal | low}`	Specifies the strict priority level of a class within a policy-map.
`queue-limit` *`packets`*	Specifies the maximum number of packets queued for a traffic class.

For more details on the full syntax and examples of the use of each command, see the “Command Reference” chapter of this document.

In the following example, a traffic policy named high-speed is defined to contain policy specifications for the two classes real_time_traffic and transact_traffic. The match criteria for these classes were defined in the traffic class-maps (see the section “Defining a Traffic Class” in this chapter).

For real_time_traffic, the policy includes a monitor-queuing-map reference, a bandwidth allocation request and a maximum packet count limit for the queue reserved for the class. For transact_traffic, the policy specifies a monitor-queuing-map and a bandwidth allocation request.

```
policy-map high-speed

       class real_time_traffic
         monitor-queuing realtime
         bandwidth 3000
         queue-limit 32


       class transact_traffic
         monitor-queuing transactional
         bandwidth 2000
```

You configure measurement of the parameters specified by a monitor-queuing-map by applying the latter with a **monitor-queuing** command inside a policy-map, for example:

```
policy-map pmap
       monitor-queuing mq1
       class cls
              monitor-queuing mq1
```

It is important to note the positioning of **monitor-queuing** commands within a policy-map. For example, in the following policy-map's configuration the indentation of the fragment suggests that the user intends for the monitor-queuing-map named mq1 to apply to the policy-map as a whole. But the last line is interpreted as part of the class named cls, and not part of the policy-map context:

```
policy-map pmap
       class cls
              bandwidth percent 10
       monitor-queuing mq1
```

This results in mq1 being applied to class cls only. To achieve the desired effect, you insert an explicit exit command between the bandwidth and monitor-queuing commands. For greater clarity, the **monitoring-queue mq1** command should be placed in the policy-map before any class configuration, as shown below:

```
policy-map pmap
       monitor-queuing mq1
       class cls
              bandwidth percent 10
```

Although a monitor-queuing-map enables Corvil Bandwidth and service-level estimation, these quantities are not always computed. In particular, they are never computed at the interface level and they are never computed in any class on peer-interfaces for a local site (inbound direction of an interface from the perspective of a site (either local or remote), downstream of queuing). Nevertheless, there is no restriction on the use of monitor-queuing-maps in these contexts; where bandwidth and service-level targets are specified, they will generate a warning to the user that they cannot be applied, and will be ignored.

When a configuration containing these inappropriate applications of QoS-targets is reloaded, the warnings will be reissued.

There is a single global default monitor-queuing-map which cannot be deleted. It is named monitor-queuing-default by analogy with class-default. If no **monitor-queuing** command is used within a class, the default is applied. If no **monitor-queuing** command is used within policy-maps, no monitor-queuing is applied. That is, the following configuration fragment

```
policy-map pmap
  class cls
```

results in the same policy-map being created as the more explicit one

```
policy-map pmap
  no monitor-queuing
  class cls
   monitor-queuing monitor-queuing-default
```

The parameters of monitor-queuing-default can be changed with the **monitor-queuing-map** command. For example, the default peak-rate timescale can be changed to 100ms with the following CLI fragment:

```
monitor-queuing-map monitor-queuing-default
  measure-microburst milliseconds 100
```

Note that this also disables peak-rate triggers by default.

The default QoS-targets will be most useful when they configure all the possible QoS measurements, but such a broad configuration will not be appropriate in all contexts.

Warnings on inappropriate application of queuing targets are generated only for user-created monitor-queuing-maps, and never for monitor-queuing-default.

Defining a Remote Site, Router, and Interface

To build the network model, you configure remote sites. You then configure routers for each remote site and interfaces for each router, according to your own deployment details.

You use the **site** configuration command to create and name a unique remote site in the network model.

You use the no form of the command to delete a remote site. The site command syntax is as follows:

site *site-name*
no site *site-name*

You use the **router** command in site configuration mode to create and name a unique model router for a site in the network model.

You use the no form of the command to delete a router. The router command syntax is as follows:

router *router-name*
no router *router-name*

You use the **interface** command in site router configuration mode to create and name a unique model interface for a site router.

You use the no form of the command to delete an interface. The interface command syntax is as follows:

interface *interface-name*
no interface *interface-name*

To define and configure remote sites, routers and interfaces, use the following commands in interface configuration mode, as needed:

The following table describes the commands you use to configure site routers:

Table 7-5 Router Commands

`attached-port`	Specifies which physical ports (PortA, PortB, PortC, PortD) are used for traffic measurement by the default local site.
`description`	Specifies a text description of the router.
`interface`	Specifies the name of an interface on a router.
`peer-interface`	Specifies the name of a peer interface on a router in native IP deployments.

The following table describes the commands you use to configure site router interfaces:

Table 7-6 Interface Commands

`bandwidth`	Specifies a bandwidth allocation for the model interface. The system creates a default bandwidth value for each interface that you create.
`connects-to`	Specifies the local site interface to which a remote site interface is connected in a point-to-point deployment.
`description`	Specifies a text description of the interface.
`filter-class`	Specifies routing information for an interface.
`link-adjust`	Sets the link adjustment for an interface.
`max-reserved-bandwidth`	Specifies the maximum reservable bandwidth as percentage of interface bandwidth.
`service-policy`	Specifies the name of a peer interface on a router in native IP deployments.
`subnet-filtering`	Enables packet filtering by subnet on an interface.

For more details on the full syntax and examples of the use of each command, see the command reference in the "Command Reference" chapter of this document.

The following example shows a remote site named New York being configured with the following details:

Subnet: 192.168.5.0/24
Router: branch1
Router interface: Serial1/0

```
host(config)# site New York
host(config-site)# description "New York branch office"
host(config-site)# subnet 192.168.5.0/24
host(config-site)# router branch1
host(config-site-router)# interface Serial0/1
host(config-site-router-if)# description "Link to Data Center"
host(config-site-router-if)# bandwidth 512
host(config-site-router-if)# service-policy output low-speed
```

Depending on the type of deployment you are configuring, you complete the network model configuration for the router by either specifying the interface to which the new interface is connected or defining a separate peer interface to represent the provider router to which the interface is connected. In this point-to-point example, the remote site router interface Serial1/0 is connected to the local site router interface named DataCenter core 1 Serial1/0.

```
host(config-site-router-if)# connects-to DataCenter core1 Serial0/1
```

Attaching a Policy Map to an Interface

You use the **service-policy** interface configuration command to attach a policy-map to the output direction of an interface. The traffic policy defined by the policy-map evaluates all traffic leaving that interface.

You use the no form of the command to detach a policy-map from an interface. The **service-policy** command syntax is as follows:

service-policy output *policy-map-name*
no service-policy output *policy-map-name*

For more details on the full syntax and examples of the use of each command, see the "Command Reference" chapter in this document.

The following example shows how to attach an existing traffic policy (which was created in the preceding section) to an interface. After you define a traffic policy with the policy-map command, you can attach it to one or more interfaces to specify the traffic policy for those interfaces by using the service-policy command in interface configuration mode. Although you can assign the same traffic policy to multiple interfaces, each interface can have only one traffic policy attached at the output.

```
interface eth1_1
       service-policy output policy1
interface serial1_0
       service-policy output policy1
```

Saving Configurations

When you have configured the BQM, you have to save your changes. To save a new configuration, you use the copy command:

```
copy config
```

Working with Configuration Files

The BQM file system contains a timestamped copy of each original BQM configuration file at the first change after user login or the last time the current active configuration was saved. The configurations due to changes after login are automatically generated, current active configuration changes are saved using the following command:

```
copy config
```

You use the **dir cfg:** command to view the current list of configuration files. The file names include date/time stamping, and are located in the directory `/cfg`, for example `cfg:<file name>`, where the file name is constructed as follows:

```
bqm_yyyy_mm_dd_hhmmss-μsec.cfg
```

where:

yyyy	year represented by 4 digits, for example 2004.
mm	numerical value representing the month, for example July by 07.
dd	numerical value representing the day of the month, for example the 28th day by 28.
hh	numerical value for hour in 24 hour format, for example 1:00 pm by 13.
mm	numerical value for minutes, for example twenty minutes past the hour by 20.
ss	numerical value for seconds, for example thirty seconds by 30.
μsec	numerical value for microseconds, for example 41,234 microseconds by 41234.

Hence a configuration saved at 1:20pm, 30 seconds, and 41234 on the 28th of July 2004 would be saved in a file as follows:

`cfg: bqm_20040728132030-41234.cfg`.

To make a previous configuration the current configuration, you use the **copy** command:

```
host(config)$ copy cfg:bqm_20040728132030.cfg config
```

You can define or edit a configuration file in a text editor off the BQM, save it with the `.cfg` file extension and copy it to the BQM to become the current configuration. In the following example, the file is copied from a tftp server to the BQM:

```
host(config)$ copy tftp://192.168.2.3 cfg:bqm_20040728132030.cfg config
```

You can also copy the current configuration file to a tftp server for storage and editing off the box:

```
host(config)$ copy cfg:bqm_20040728132030.cfg tftp://192.168.2.3
```

Note You can copy configuration files to and from the BQM when logged in as either the admin or config users.

Working with Subnet Filtering

Subnet filtering applies when a site has subnets defined with the **subnet** command. To enable interface packet filtering based on either configured site subnet, or traffic source or destination address on local or remote site interfaces or peer interfaces, use the **subnet-filtering** command. This command is automatically invoked for interfaces when you define site subnets. You do not need to explicitly add it to the configuration in this case.

Subnet filtering applies as follows:

- Remote site interfaces match packets that have a source address within any of that remote site's subnets. Note that packets with both a source and destination address within the remote site will be included.
- Remote site peer-interfaces match packets that have a destination address within any of that remote site's subnets. As above, packets with both a source and destination address within the remote site's subnets will be included here also.
- Remote site interfaces connected directly to the local site match packets that have a destination address within the remote site's subnets. This also matches packets with both a source and destination address within the remote site's subnets.
- Local-site interfaces will match packets that do not have a destination address within the local-site's subnets. This means that they will exclude traffic that is internal to the local-site's subnets, but they will include transit traffic that does not involve any local-site subnets.
- Local-site peer-interfaces will match packets that do not have a source address within the local-site's subnets. This means that they will exclude traffic that is internal to the local-site's subnets, but they will include transit traffic that does not involve any local-site subnets.

Defining sites with subnets is optional in the BQM configuration. Using **no subnet-filtering** indicates that you intend to ignore site subnets when matching traffic. So this is used when you are

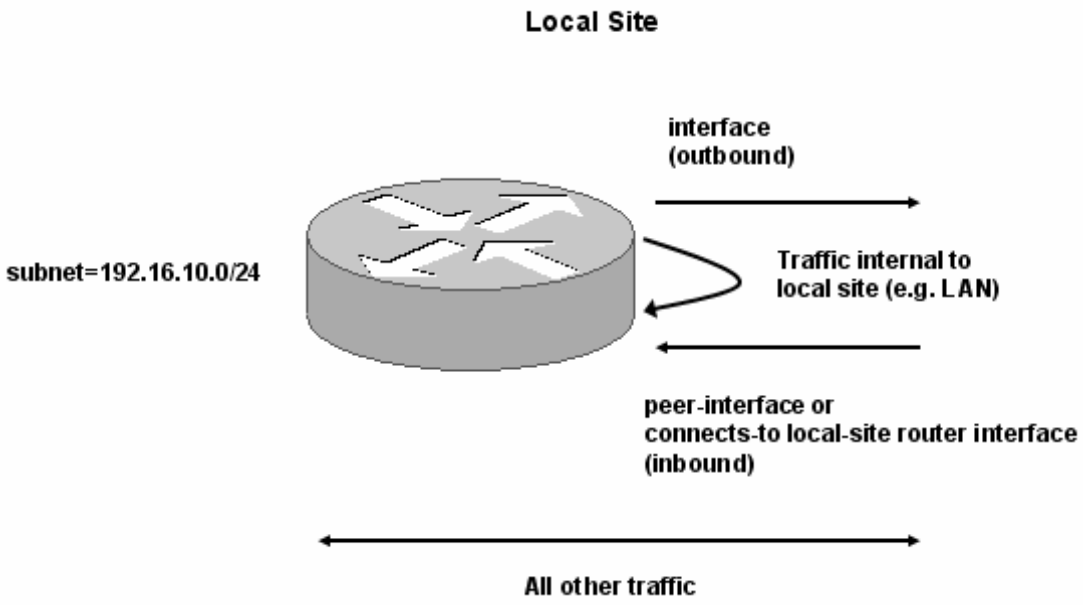
- using the **attached-ports** command to establish traffic filtering with the physical BQM ports (PortA, PortB, PortC, PortD, PortAC, PortBD)
- using the **filter-class** command or if you define a particular set of match rules using a class-map

The use of the BQM physical ports (such as PortA, PortB and so on) in the default first day of service configuration requires subnet filtering to be explicitly disabled. So the default BQM configuration includes a **no subnet-filtering** command on each relevant interface. Note that the default BQM configuration has no subnets defined for any sites. For example, from the default configuration:

```
interface PortA
          attached-port PortA
          bandwidth 1000000
          max-reserved-bandwidth 75
          no subnet-filtering
          service-policy output default
            class class-default
```

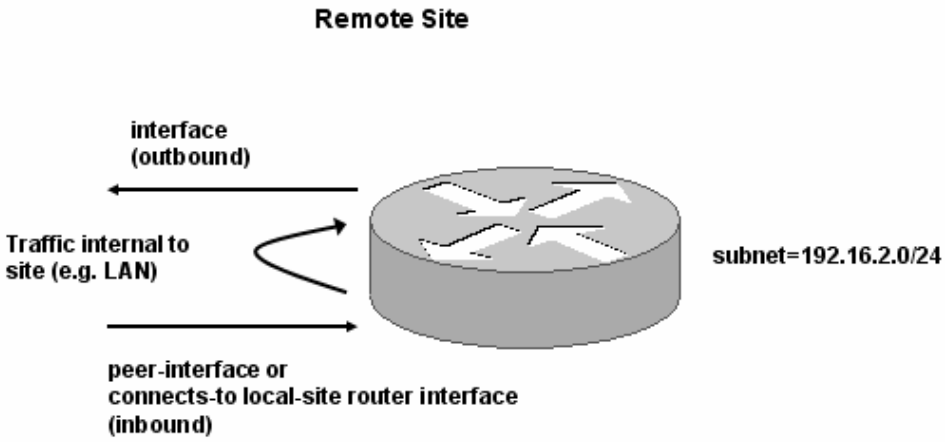
Where local site interfaces or peer interfaces are filtered using the **attached-ports** command, it may be desirable to exclude traffic that is internal to the local site's subnets (that is, both source and destination address within the site).

Figure 7-1: Subnet Filtering



Using the **subnet-filtering non-local-only** command switches to excluding only traffic where both the source and destination addresses fall inside the local site's subnets. The interface, peer-interface (or connected interface) and all other traffic seen by the BQM are included. Finally, since the default behavior effectively double-counts traffic that is internal to remote site subnets (once at the interface and once at the peer or connected interface), you can add a **subnet-filtering exclude-local** command that excludes traffic that is local to the site.

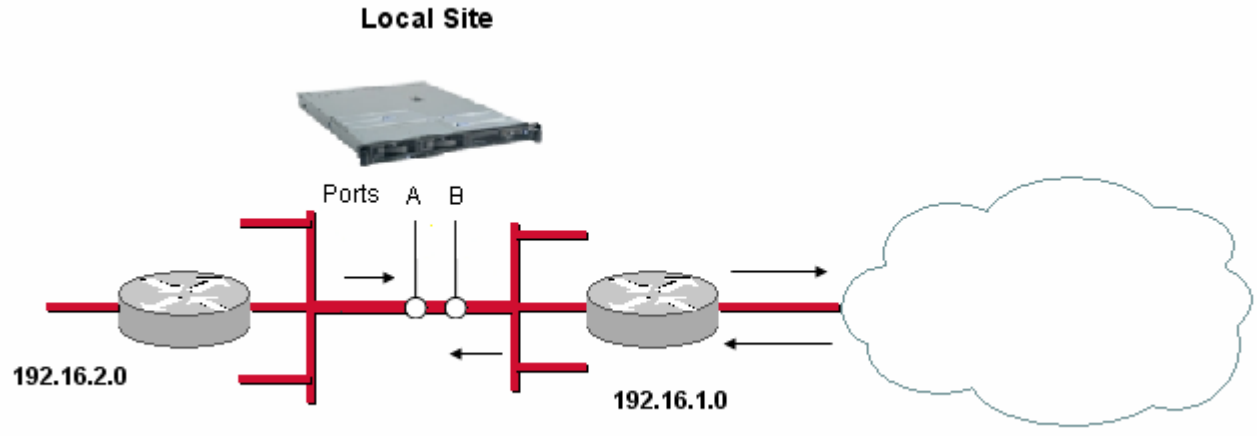
Figure 7-2: Subnet Filtering – Exclude Local Traffic



In the diagram above, using the exclude-local option excludes the traffic internal to the remote site, for example LAN traffic on the remote site subnet.

In the following example of using the **subnet-filtering non-local-only** command, the BQM sees traffic internal to the local site from two different local site subnets as well as the traffic going to and coming from the WAN. The configuration excludes the internal inter-LAN traffic while measuring only the traffic bound for or coming from the WAN. The BQM physical port PortA is used to measure outbound traffic and PortB is used to measure inbound traffic:

Figure 7-3: Subnet Filtering – Non-local Traffic Only




```
host(config-local-site)$ subnet 192.16.1.0
host(config-local-site)$ subnet 192.16.2.0
host(config-local-site)$ router default
host(config-local-site-router)$ interface default
host(config-local-site-router-if)$ attached-port portA
host(config-local-site-router-if)$ subnet-filtering non-local-only
```

```
host(config-local-site-router-if)$ peer-interface default
host(config-local-site-router-pif)$ attached-port portB
host(config-local-site-router-pif)$ subnet-filtering non-local-only
host(config-local-site-router-pif)$ show config
!
!
local-site Local-site
  subnet 192.16.1.0/32
  subnet 192.16.2.0/32
  router default
    interface default
      attached-port PortA PortB
      subnet-filtering non-local-only
    peer-interface default
      subnet-filtering non-local-only
```

Using Filter Classes

Instead of using subnets to identify traffic, you can use filter classes to model the situation where traffic coming from a site is matched by one set of rules, and traffic going to the site is matched by a completely different set of match rules. For example, traffic leaving the SPN cloud for a remote site interface might be matched by a VLAN tag, and the traffic coming from that remote site might be matched by an outer MPLS label, an inner MPLS label, and an IP source address.

In the following example, a class-map defining the MPLS match rules is defined:

```
host(config-site-router-if)$ class-map mplstags
host(config-cmap)$ match mpls label1=100
host(config-cmap)$ match mpls inner-label1=148
host(config-cmap)$ match ip src=192.168.2.3
```

Next, the class-map is applied to the interface using the **filter-class** command. Note that subnet filtering is disabled for the interface.

```
host(config-cmap)$ site newyork_branch
host(config-site)$ router nyc_br_rtr
host(config-site-router)$ interface serial0/1
host(config-site-router-if)$ bandwidth 256
host(config-site-router-if)$ no subnet-filtering
host(config-site-router-if)$ filter-class mplstags
```

Next, the class-map defining the vLAN tags is defined, and is applied to the peer-interface. Again, subnet filtering is disabled for the peer-interface:

```
host(config-site-router-if)$ class-map vlantags
host(config-cmap)$ match vlan id=4
host(config-cmap)$ site asymmetric
host(config-site)$ router rtr
host(config-site-router)$ peer-interface customer
host(config-site-router-pif)$ no subnet-filtering
host(config-site-router-pif)$ filter-class vlantags
host(config-site-router-pif)$ end
```

You can only create and edit filter classes using the CLI. If you have define a filter class for an interface, it will be indicated in the GUI, but is not editable.

Configuring Network Model Deployments with the CLI

This section describes how to take knowledge of the existing network design, which the BQM is used to monitor and troubleshoot, and configure the appropriate deployment of the product network model using the CLI. You need to decide which of the deployment models most accurately captures the network configuration you are monitoring. There are different types of network model deployment which also then vary in complexity (usually given dual homing or failover configurations).

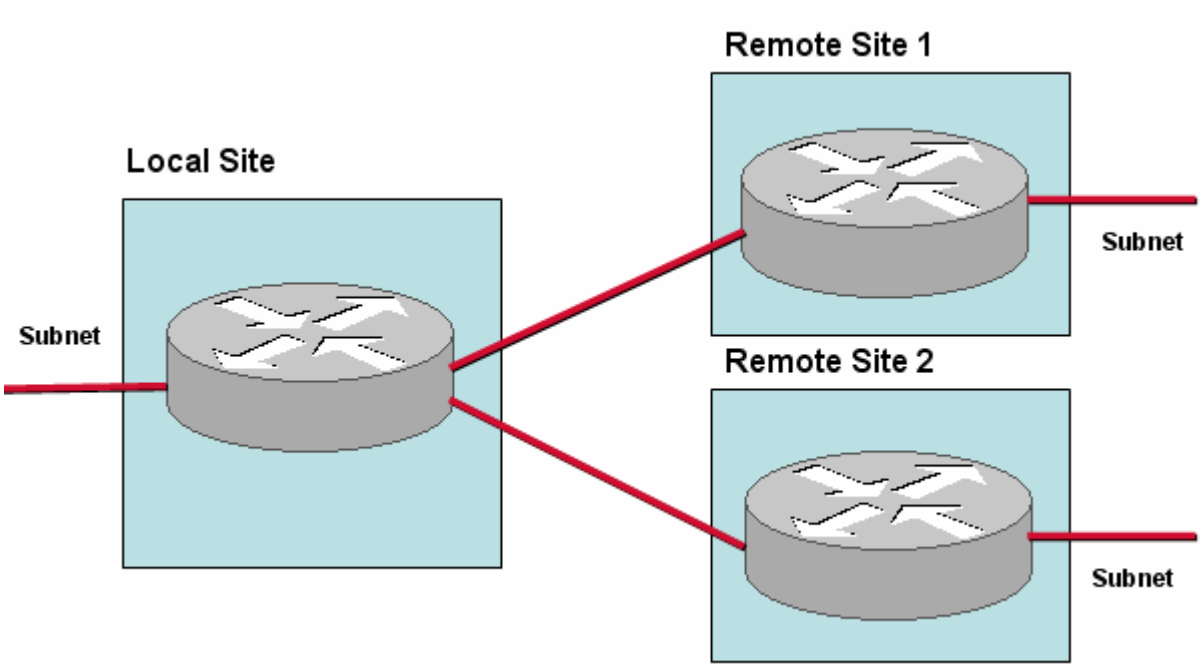
The basic network model deployments are

- ATM PVC, Frame Relay PVC, Metro Ethernet, Leased line
- MPLS VPN, Internet VPN, Private VPN

Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM.

Figure 7-4 Network Model - Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment



To configure the network model for this example deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is editable
  - Subnet
  - Router
  - Interfaces specifying bandwidth configuration and policy-maps

- Remote Sites
  - Name
  - Subnet
  - Router
  - Interface with link to local site-router-interface, bandwidth, policy-map

To configure the network model for this deployment from the CLI, you do the following:

Step 1 Define the monitor-queuing-map and monitor end2end map for the configuration. In this example monitor-queuing-map configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified:

```
host(config)$ monitor-queuing-map low_speed
host(config-mqmap)$ measure-bandwidth
host(config-mqmap)$ measure-microburst milliseconds 150
host(config-mqmap)$ queuing-targets delay-milliseconds 150
```

For more information on defining monitor-queuing-maps, see the **monitor-queuing-map**, **measure-bandwidth**, **measure-microburst**, and **queuing-targets** commands in the "Command Reference" chapter of this document.

In this example monitor end2end map, the default ping interval and ICMP packet size are retained, and event detection is enabled if packet delay exceeds 500 ms and if any packets are lost.

```
host(config-mqmap)$ monitor-end2end-map low_speed
host(config-me2emap)$ measure-ping event-thresholds delay-
milliseconds 500 loss
```

For more information on defining monitor-end2end-maps, see the **monitor-end2end-map**, and **measure-ping** commands in the "Command Reference" chapter of this document.

Step 2 Define the policy-map for the configuration. In this example, the single-class FIFO policy-map comprises only the default class, class-default, and the monitor-queuing-map values specified above are used:

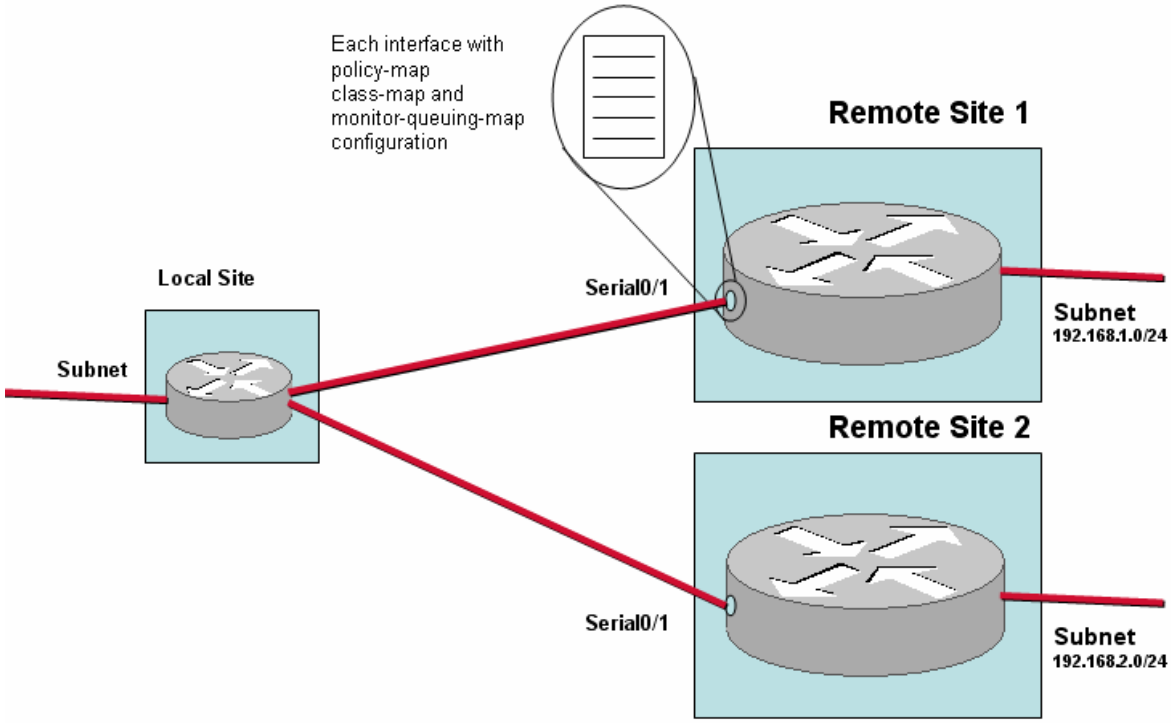
```
host(config-mqmap)$ policy-map FIFO
host(config-pmap)$ monitor-queuing low_speed
```

Step 3 Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has two interfaces, Serial0/1 and Serial0/2, with both connected to links of 512 kbps and both using the FIFO policy-map:

```
host(config)$ local-site Local-Site
host(config-local-site)$ subnet 192.168.5.0/24
host(config-local-site)$ router core1
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to Remote
Site 1"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output FIFO
```

```
host(config-local-site-router-if)$ interface Serial0/2
host(config-local-site-router-if)$ description "Link to Remote
Site 2"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output FIFO
```

Figure 7-5 Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Remote Site Configuration



Step 4 Define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet and has a well-known ping address at 192.168.1.3. Each remote site has a site router, whose interface connections back to each local site interface is made explicit in the configuration using the **connects-to** command:

```
host(config-local-site-router-if)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ ping-address 192.168.1.3
host(config-site)$ monitor-end2end low_speed
host(config-site)$ end2end-target low speed
host(config-site)$ router remote1
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to Local Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output FIFO
host(config-site-router-if)$ connects-to Local Site core1
Serial0/1
host(config-site-router-if)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
host(config-site)$ ping-address 192.168.2.3
host(config-site)$ end2end-target low-speed
host(config-site)$ router remote2
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to Local Site"
```

```
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output FIFO
host(config-site-router-if)$ connects-to Local Site core1
Serial0/2
```

Step 5 Check the configuration with the **show config** command:

```
host(config-site-router-if)$ show config
monitor-queuing-map low_speed
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
!
monitor-end2end-map low_speed
  measure-ping interval-milliseconds 10000 size-bytes 36
availability-threshold 10 event-thresholds delay-milliseconds
500
!
!
policy-map FIFO
  monitor-queuing low_speed
  class class-default
!
!
local-site Local-Site
  subnet 192.168.5.0/24
  router core1
    interface Serial0/1
      description "Link to Remote Site 1"
      bandwidth 512
      service-policy output FIFO
      link-adjust 0
    interface Serial0/2
      description "Link to Remote Site 2"
      bandwidth 512
      service-policy output FIFO


site "Remote Site 1"
  subnet 192.168.1.0/24
  ping-address 192.168.1.3
  end2end-target low_speed
  router remote1
    interface Serial0/1
      description "Link to Local Site"
      bandwidth 512
      service-policy output FIFO
      connects-to Local-Site core1 Serial0/1

site "Remote Site 2"
  subnet 192.168.2.0/24
  ping-address 192.168.2.3
  end2end-target low_speed
  router remote2
    interface Serial0/1
      description "Link to Local Site"
      bandwidth 512
      service-policy output FIFO
      connects-to Local-Site core1 Serial0/2
```

```
--More--
```

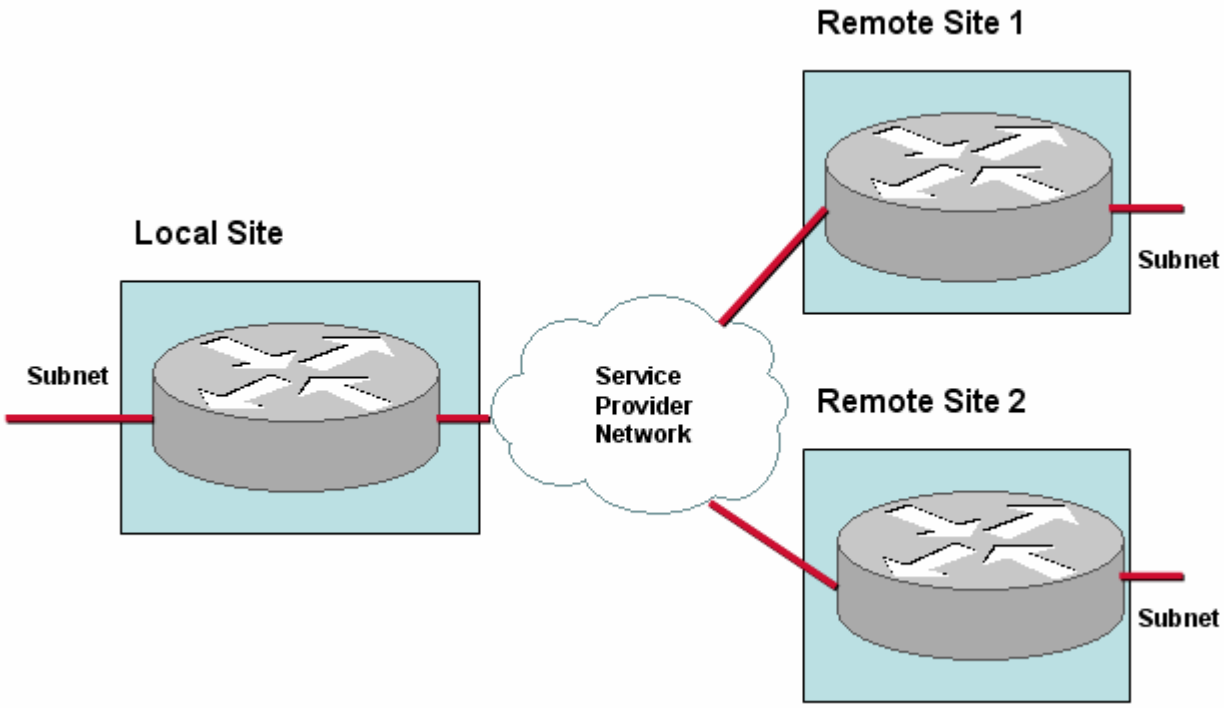
Step 6 When you have satisfied with the configuration, you save your changes. To save the new configuration, you use the copy command:

```
host(config)$ copy config
```

Basic MPLS VPN, Internet VPN, Private VPN Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM and so all measurements are made from the perspective of the local site. At least one local site WAN link must be configured with the correct aggregate link bandwidth speed. Ideally you use the Service Provider Network policy-map for the remote site QoS policies. These polices can be modeled on the Service Provider Network, or less ideally the inbound direction of the remote site interfaces.

Figure 7-6 Network Model – Basic MPLS VPN, Internet VPN, Private VPN Deployment

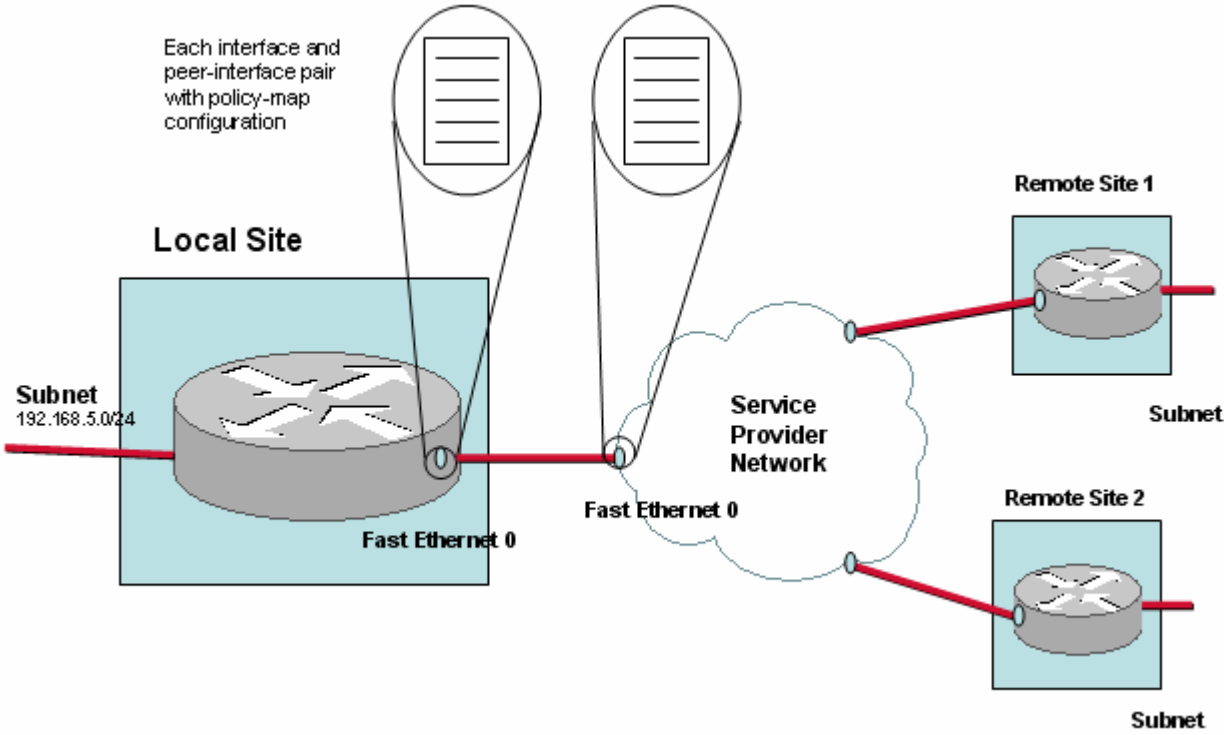


To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is editable
  - Subnet
  - Router
  - Local site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

Figure 7-7: Basic MPLS VPN, Internet VPN, Private VPN ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Local Site Configuration



To configure the network model for this deployment from the CLI, you do the following:

Step 1 Define the monitor-queuing-map and monitor-end2end-map for the configuration. In this example configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified:

```
host(config)$ monitor-queuing-map low_speed
host(config-mqmap)$ measure-bandwidth
host(config-mqmap)$ measure-microburst milliseconds 150
host(config-mqmap)$ queuing-targets delay-milliseconds 150
```

For more information on defining monitor-queuing-maps, see the **monitor-queuing-map**, **measure-bandwidth**, **measure-microburst**, and **queuing-targets** commands in the "Command Reference" chapter of this document.

In this example monitor end2end map, the default ping interval and ICMP packet size are retained, and event detection is enabled in case of delay exceeding 500 ms and if any packets are lost.

```
host(config-mqmap)$ monitor-end2end-map low_speed
host(config-me2emap)$ measure-ping event-thresholds delay-
milliseconds 500 loss
```

For more information on defining monitor-end2end-maps, see the **monitor-end2end-map**, and **measure-ping** commands in the "Command Reference" chapter of this document.

Step 2 Define the class-maps for the configuration. In this example, there are the following class-maps:

realtime
critical
video
bulk
besteffort

The class-map details are configured as follows:

```
class-map match-any besteffort
  match ip dscp=0
class-map match-any bulk
  match ip dscp=10
class-map match-any critical
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map match-any realtime
  match ip dscp=46
  match ip dscp=40
class-map match-any video
  match ip dscp=18
  match ip dscp=16
```

Step 3 Define the policy-maps for the configuration. In this example, there are three policy-maps:

mpls_policy - models the local site router policy
pe-policy - models the SPN router policy
low_speed - models the remote site router policies

In this example, the same details are configured for each policy-map.

The monitor-queuing-map values specified above are applied to each policy-map class:

```
host(config-mqmap)$ policy-map mpls_policy
host(config-pmap)$ class realtime
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 25
host(config-pmap-c)# class critical
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class video
host(config-pmap-c)$ monitor-queuing low_speed
```

```
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class bulk
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 10
host(config-pmap-c)# class besteffort
host(config-pmap-c)$ monitor-queuing low_speed
```

The other policy-maps are configured in the same way:

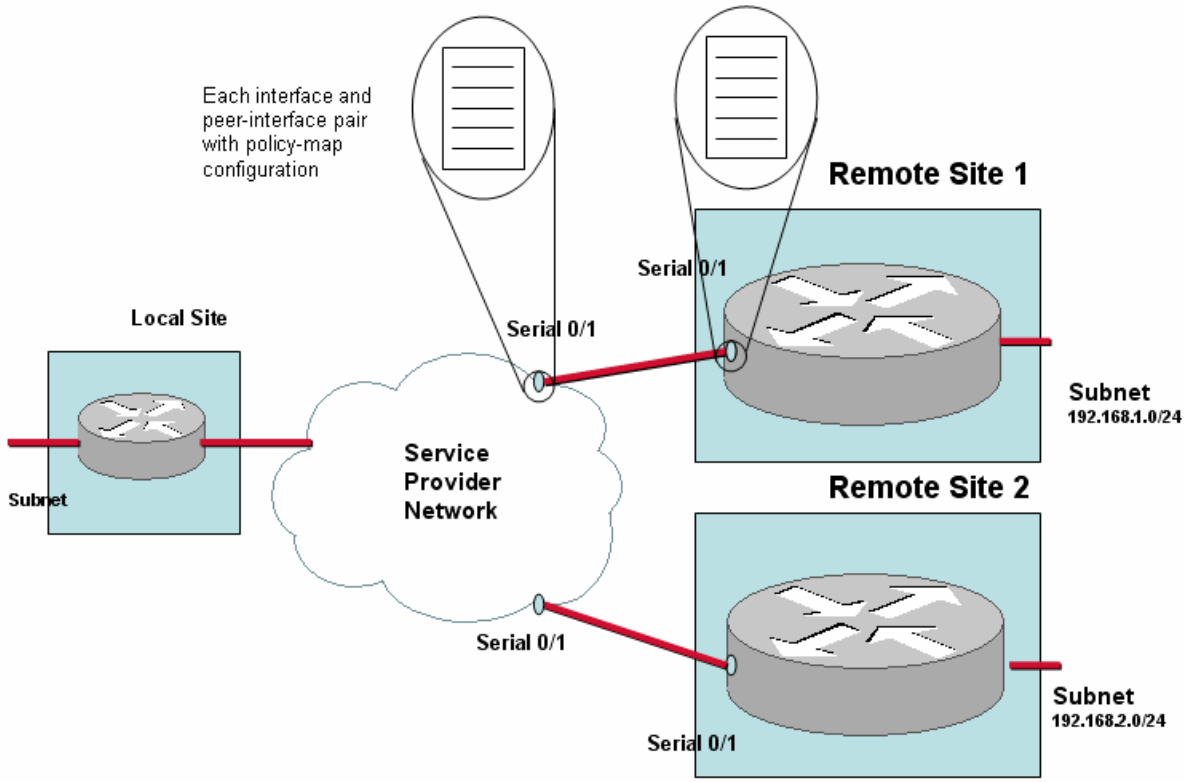
Step 4 Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has one interface, Fast Ethernet0, with an associated peer-interface, both connected to the 10000 kbps link and each using a separate policy-map:

```
host(config)$ local-site Local-Site
host(config-site)$ subnet 192.168.5.0/24
host(config-local-site)$ router core1
host(config-local-site-router)$ interface FastEthernet0
host(config-local-site-router-if)$ description "Link to SPN MPLS"
host(config-local-site-router-if)$ bandwidth 10000
host(config-local-site-router-if)$ service-policy output mpls_policy
host(config-local-site-router-if)$ peer-interface FastEthernet0
host(config-local-site-router-pif)$ description "interface on PE"
host(config-local-site-router-pif)$ bandwidth 10000
host(config-local-site-router-pif)$ service-policy output pe-policy
```

Note You configure peer-interfaces to complete the network model for MPLS VPN, Internet VPN, Private VPN deployments.

In cases where you have access to the service provider PE router configuration details, you configure the equivalent peer-interfaces in the network model accordingly. If you do not have this information, you configure each peer-interface with the same details as the site interface with which it is paired.

Figure 7-8 Basic MPLS VPN, Internet VPN, Private VPN Deployment – Remote Site Configuration



Step 5 Define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, with interface and peer-interface configurations:

```
host(config-local-site-router-pif)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ ping-address 192.168.1.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote1
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to SPN MPLS"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ peer-interface Serial0/1
host(config-site-router-pif)$ description "interface on PE"
host(config-site-router-pif)$ bandwidth 512
host(config-site-router-pif)$ service-policy output pe-policy
host(config-site-router-pif)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
host(config-site)$ ping-address 192.168.2.5
host(config-site)$ monitor-end2end low_speed
host(config-site)$ router remote2
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to SPN MPLS"
host(config-site-router-if)$ bandwidth 256
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ peer-interface Serial0/1
```

```
host(config-site-router-pif)$ description " interface on PE"
host(config-site-router-pif)$ bandwidth 256
host(config-site-router-pif)$ service-policy output pe-policy
host(config-site-router-pif)$
```

Step 6 Check the configuration with the **show config** command:

```
host(config-site-router-pif)$ show config
monitor-queuing-map low_speed
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
!
monitor-end2end-map low_speed
  measure-ping interval-milliseconds 10000 size-bytes 36
availability-threshold 10 event-thresholds delay-milliseconds
500 loss
!
!
class-map match-any besteffort
  match ip dscp=0
class-map match-any bulk
  match ip dscp=10
class-map match-any critical
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map match-any realtime
  match ip dscp=46
  match ip dscp=40
class-map match-any video
  match ip dscp=18
  match ip dscp=16
!
!
policy-map low_speed
  class realtime
    monitor-queuing low_speed
    bandwidth 25
  class critical
    monitor-queuing low_speed
    bandwidth 20
  class video
    monitor-queuing low_speed
    bandwidth 20
  class bulk
    monitor-queuing low_speed
    bandwidth 10
  class besteffort
    monitor-queuing low_speed
  class class-default

policy-map mpls_policy
  class realtime
    monitor-queuing low_speed
    bandwidth 25
  class critical
    monitor-queuing low_speed
    bandwidth 20
  class video
```

```
    monitor-queuing low_speed
    bandwidth 20
  class bulk
    monitor-queuing low_speed
    bandwidth 10
  class besteffort
    monitor-queuing low_speed
  class class-default

policy-map pe_policy
  class realtime
    monitor-queuing low_speed
    bandwidth 25
  class critical
    monitor-queuing low_speed
    bandwidth 20
  class video
    monitor-queuing low_speed
    bandwidth 20
  class bulk
    monitor-queuing low_speed
    bandwidth 10
  class besteffort
    monitor-queuing low_speed
  class class-default


local-site Local-site
  subnet 192.168.5.0/24
  router core1
    interface FastEthernet0
      description "Link to SPN MPLS"
      bandwidth 10000
      service-policy output mpls_policy
    peer-interface FastEthernet0
      description "interface on PE"
      bandwidth 10000
      service-policy output pe-policy

site "Remote Site 1"
  subnet 192.168.1.0/24
  ping-address 192.168.1.3
  end2end-target low_speed
  router remote1
    interface Serial0/1
      description "Link to SPN MPLS"
      bandwidth 512
      service-policy output low_speed
    peer-interface Serial0/1
      description "interface on PE"
      bandwidth 512
      service-policy output pe-policy

site "Remote Site 2"
  subnet 192.168.2.0/24
  ping-address 192.168.2.3
  end2end-target low_speed
  router remote2
    interface Serial0/1
      description "Link to SPN MPLS"
```

```
        bandwidth 256
        service-policy output low_speed
      peer-interface Serial0/1
        description "interface on PE"
        bandwidth 256
        service-policy output pe-policy
--More--
```

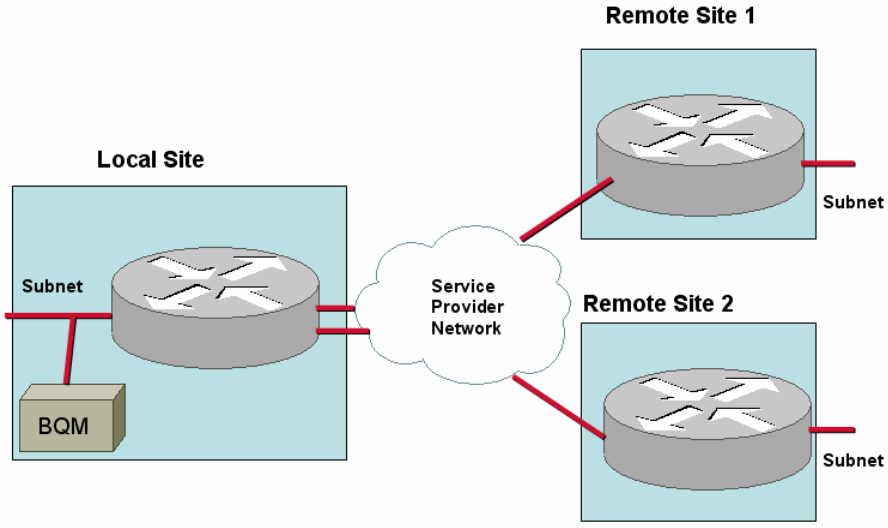
Step 7 When you have satisfied with the configuration, you save your changes. To save the new configuration, you use the copy command:

```
host(config)$ copy config
```

MPLS VPN, Internet VPN, Private VPN Deployment with Redundant Local Site Connectivity

The BQM network model can be configured to model this deployment. However, because of the potential in a load balancing situation for the same traffic to be split over both links, the BQM does not present accurate traffic statistic results for the local site interfaces in this case.

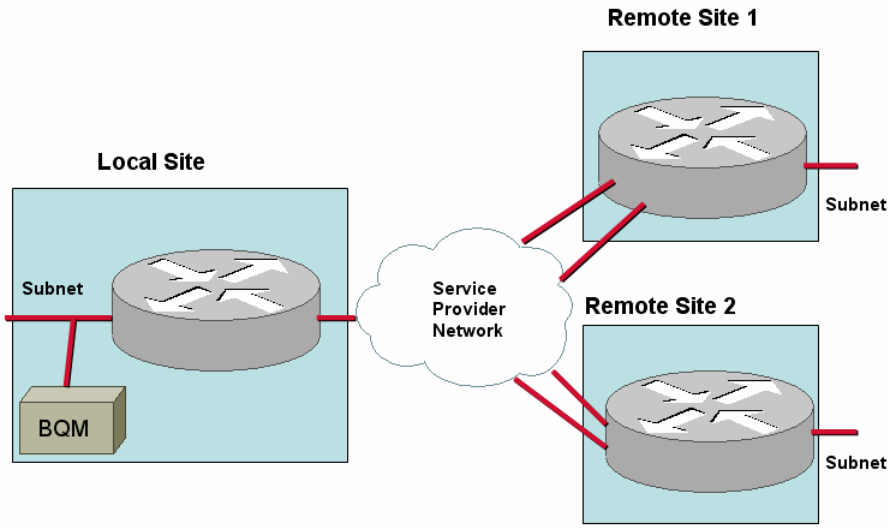
Figure 7-9 Network Model –MPLS VPN, Internet VPN, Private VPN Deployment with Redundant Remote Site Connectivity



MPLS VPN, Internet VPN, Private VPN Deployment with Redundant Remote Site Connectivity

The BQM network model can be configured to model this deployment. However, because of the potential in a load balancing situation for the same traffic to be split over both links, the BQM does not present accurate traffic statistic results for the remote site interfaces in this case.

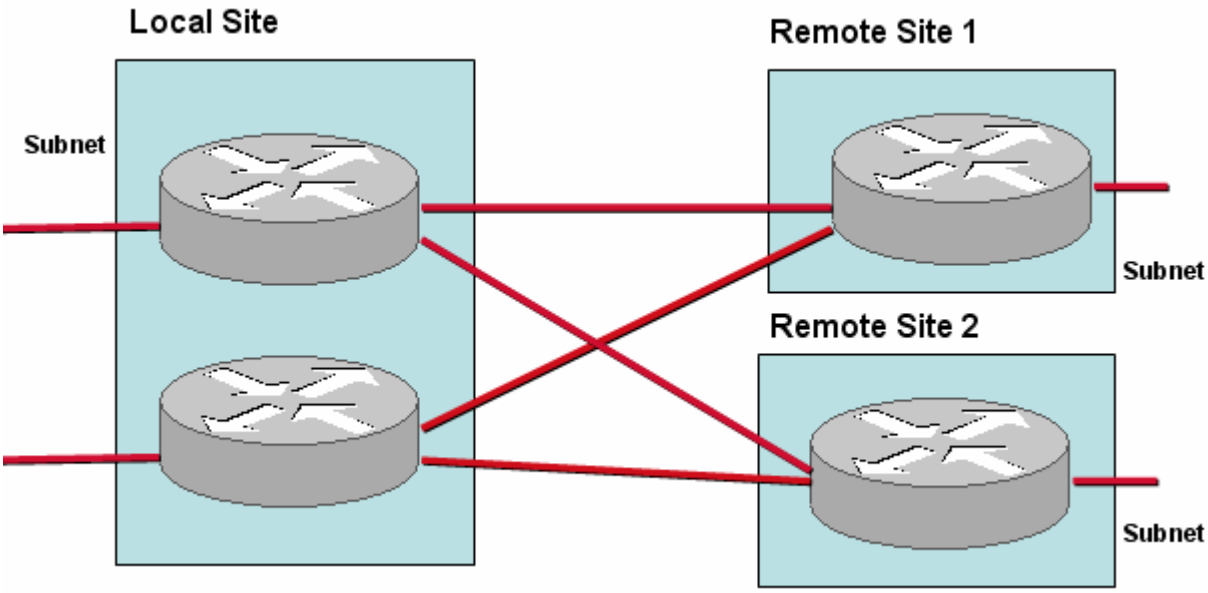
Figure 7-10 Network Model –MPLS VPN, Internet VPN, Private VPN Deployment with Redundant Remote Site Connectivity



Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local-site' site contains the BQM and so all measurements are made from the perspective of the local site. Each local site router must be bound to specific BQM physical measurement ports.

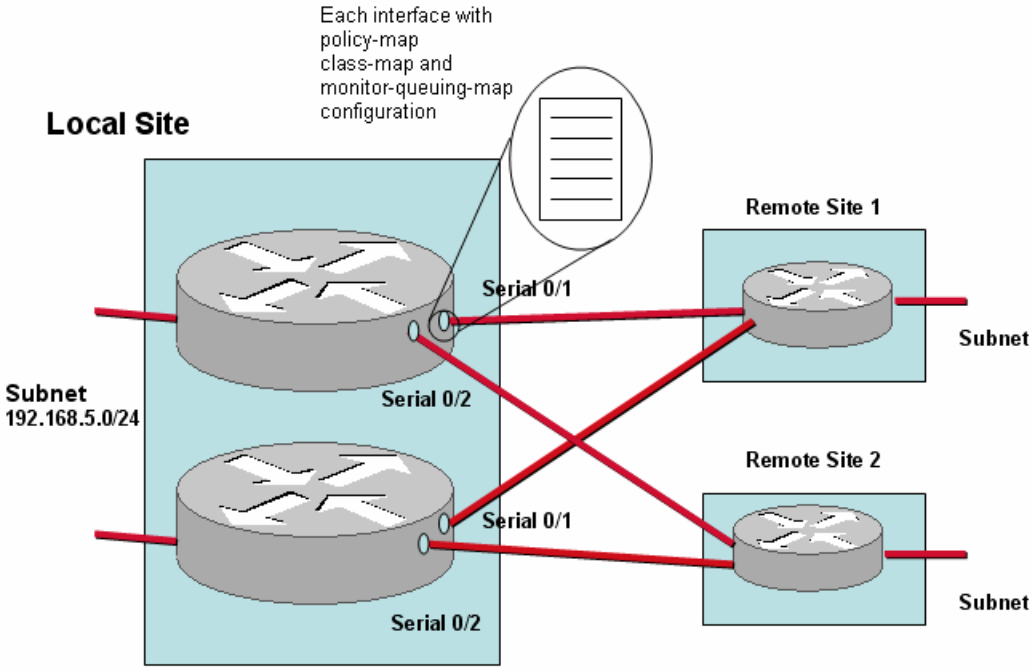
Figure 7-11 Network Model – Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment



To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is editable
  - Subnet
  - Router
  - Two interfaces specifying bandwidth configuration and policy-maps
  - Mapping of BQM physical measurement ports to routers
- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Interface with link to local site-router-interface, bandwidth, policy-map

Figure 7-12 Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Local Site Configuration



To configure the network model for this deployment from the CLI, you do the following:

Step 1 Define the monitor-queuing-map and monitor end2end map for the configuration. In this example monitor-queuing-map configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified:

```
host(config)$ monitor-queuing-map low_speed
host(config-mqmap)$ measure-bandwidth
host(config-mqmap)$ measure-microburst milliseconds 150
host(config-mqmap)$ queuing-targets delay-milliseconds 150
```

For more information on defining monitor-queuing-maps, see the **monitor-queuing-map**, **measure-bandwidth**, **measure-microburst**, and **queuing-targets** commands in the "Command Reference" chapter of this document.

In this example monitor end2end map, the default ping interval and ICMP packet size are retained, and event detection is enabled in case of delay exceeding 500 ms and if any packets are lost.

```
host(config-mqmap)$ monitor-end2end-map low_speed
host(config-me2emap)$ measure-ping event-thresholds delay-
milliseconds 500 loss
```

For more information on defining monitor-end2end-maps, see the **monitor-end2end-map**, and **measure-ping** commands in the "Command Reference" chapter of this document.

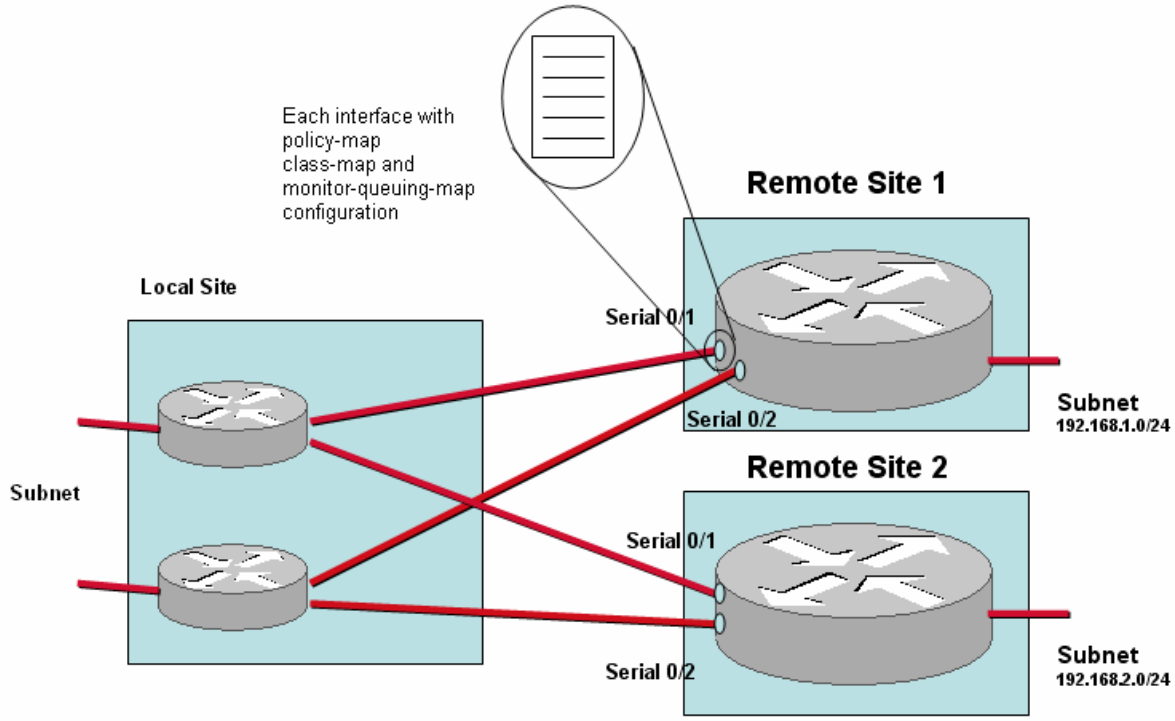
Step 2 Define the policy-map for the configuration. In this example, the single-class FIFO policy-map comprises only the default class, class-default, and the monitor-queuing-map values specified above are used:

```
host(config-mqmap)$ policy-map FIFO
host(config-pmap)$ monitor-queuing low_speed
```

Step 3 Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and two local site routers, named core1 and core2, each with two interfaces, Serial0/1 and Serial0/2, with all interfaces connected to links of 512 kbps and all using the FIFO policy-map. The physical measurement ports Port A and PortB are mapped to the core1 local site router. PortC and PortD are mapped to the core2 local site router:

```
host(config)$ local-site Local-site
host(config-local-site)$ subnet 192.168.5.0/24
host(config-local-site)$ router core1
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to Remote
Site 1"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
low_speed
host(config-local-site-router-if)$ interface Serial0/2
host(config-local-site-router-if)$ description "Link to Remote
Site 2"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
low_speed
host(config-local-site-router-if)$ attached-port PortA PortB
host(config-local-site-router-if)$ router core2
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to Remote
Site 1"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
low_speed
host(config-local-site-router-if)$ interface Serial0/2
host(config-local-site-router-if)$ description "Link to Remote
Site 2"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
low_speed
host(config-local-site-router-if)$ attached-port PortC PortD
host(config-local-site-router-if)$
```

Figure 7-13 Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Remote Site Configuration



Step 4 Define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, whose interface connections back to each local site interface is made explicit in the configuration using the **connects-to** command:

```
host(config)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ ping-address 192.168.1.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote1
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to Local Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ connects-to Local-site core1
Serial0/1
host(config-site-router-if)$ interface Serial0/2
host(config-site-router-if)$ description "Link to Local Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ connects-to Local-site core2
Serial0/1
host(config-site-router-if)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
host(config-site)$ ping-address 192.168.2.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote2
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to Local Site"
```

```
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ connects-to Local-site core1
Serial0/2
host(config-site-router-if)$ interface Serial0/2
host(config-site-router-if)$ description "Link to Local Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ connects-to Local-site core2
Serial0/2
host(config-site-router-if)$
```

Step 5 Check the configuration with the **show config** command:

```
host(config-site-router-if)$ show config
monitor-queuing-map low_speed
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
!
monitor-end2end-map low_speed
measure-ping interval-milliseconds 10000 size-bytes 36
availability-  threshold 10 event-thresholds delay-milliseconds
500 loss
!
!
policy-map low_speed
  monitor-queuing low_speed
  class class-default
local-site Local-site
  subnet 192.168.5.0/24
  router core1
    attached-port PortA PortB
    interface Serial0/1
      description "Link to Remote Site 1"
      bandwidth 512
      service-policy output low_speed
    interface Serial0/2
      description "Link to Remote Site 2"
      bandwidth 512
      service-policy output low_speed
  router core2
    attached-port PortC PortD
    interface Serial0/1
      description "Link to Remote Site 1"
      bandwidth 512
      service-policy output low_speed
    interface Serial0/2
      description "Link to Remote Site 2"
      bandwidth 512
      service-policy output low_speed
site "Remote Site 1"
  subnet 192.168.1.0/24
  ping-address 192.168.1.5
  end2end-target low_speed
  router remote1
    interface Serial0/1
      description "Link to Local Site"
      bandwidth 512
      service-policy output low_speed
```

```
      connects-to Local-site core1 Serial0/1
    interface Serial0/2
      description "Link to Local Site"
      bandwidth 512
      service-policy output low_speed
      connects-to Local-site core2 Serial0/1
site "Remote Site 2"
  subnet 192.168.2.0/24
  ping-address 192.168.2.5
  end2end-target low_speed
  router remote2
    interface Serial0/1
      description "Link to Local Site"
      bandwidth 512
      service-policy output low_speed
      connects-to Local-site core1 Serial0/2
    interface Serial0/2
      description "Link to Local Site"
      bandwidth 512
      service-policy output low_speed
      connects-to Local-site core2 Serial0/2
--More--
```

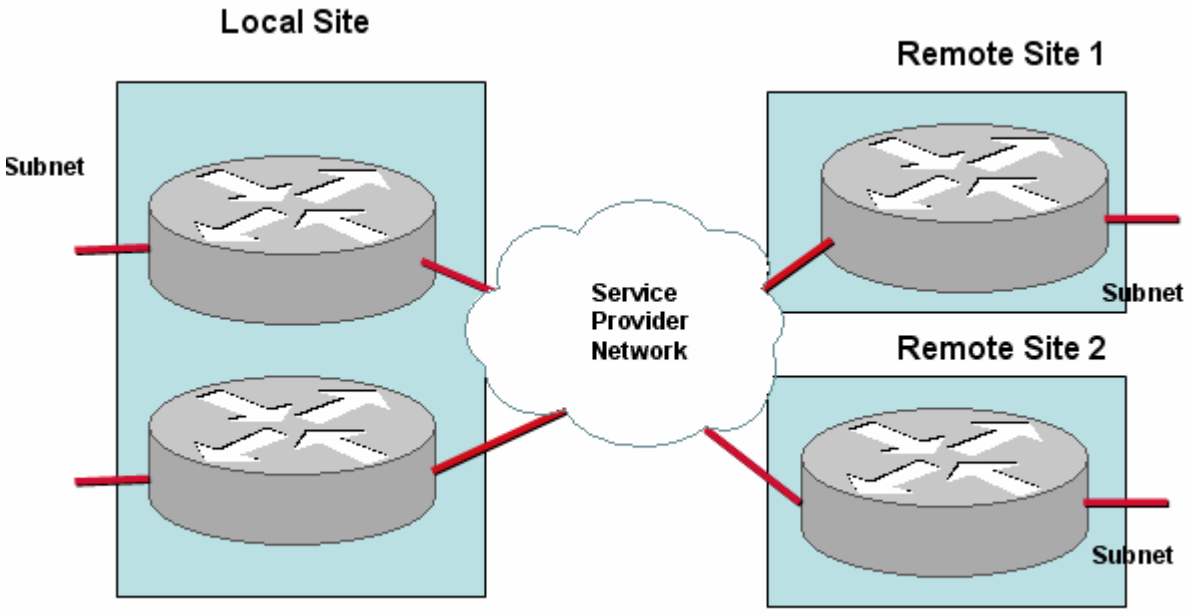
Step 6 When you have satisfied with the configuration, you save your changes. To save the new configuration, you use the copy command:

```
host(config)$ copy config
```

Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local-site' site contains the BQM and so all measurements are made from the perspective of the local site. The local site link to the SPN cannot be sized, but you can calculate a 'total' WAN bandwidth value. The remote site links can be sized.

Figure 7-14: Network Model – Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment



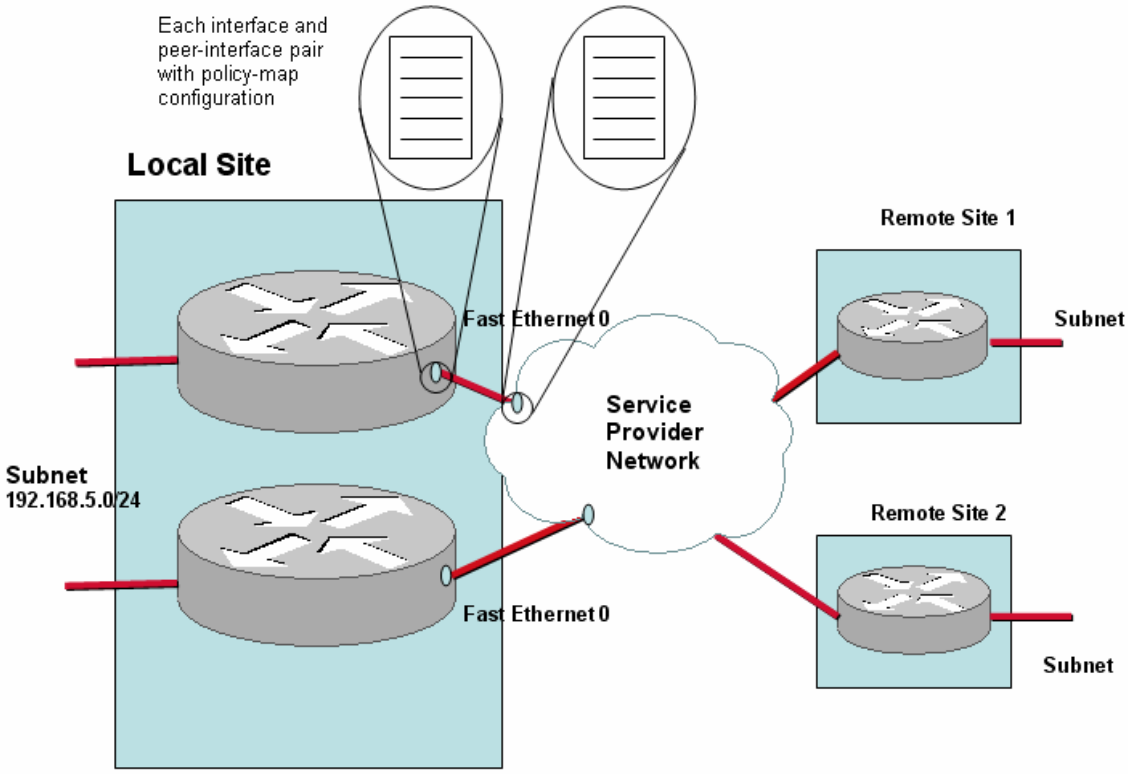
To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is editable
  - Subnet
  - Router
  - Local site interface/SPN peer-interface pair with bandwidth configuration and policy-maps
  - Mapping of BQM physical measurement ports to routers

- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

To configure the network model for this deployment from the CLI, you do the following

Figure 7-15 Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment – Local Site Configuration



To configure the network model for this deployment from the CLI, you do the following:

Step 1 Define the monitor-queuing-map and monitor end2end map for the configuration. In this example monitor-queuing-map configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified:

```
host(config)$ monitor-queuing-map low_speed
host(config-mqmap)$ measure-bandwidth
host(config-mqmap)$ measure-microburst milliseconds 150
host(config-mqmap)$ queuing-targets delay-milliseconds 150
```

For more information on defining monitor-queuing-maps, see the **monitor-queuing-map**, **measure-bandwidth**, **measure-microburst**, and **queuing-targets** commands in the "Command Reference" chapter of this document.

In this example monitor end2end map, the default ping interval and ICMP packet size are retained, and event detection is enabled in case of delay exceeding 500 ms and if any packets are lost.

```
host(config-mqmap)$ monitor-end2end-map low_speed
host(config-me2emap)$ measure-ping event-thresholds delay-
milliseconds 500 loss
```

For more information on defining monitor-end2end-maps, see the **monitor-end2end-map**, and **measure-ping** commands in the "Command Reference" chapter of this document.

Step 2 Define the class-maps for the configuration. In this example, there are the following class-maps:

realtime
critical
video
bulk
besteffort

The class-map details are configured as follows:

```
class-map match-any besteffort
  match ip dscp=0
class-map match-any bulk
  match ip dscp=10
class-map match-any critical
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map match-any realtime
  match ip dscp=46
  match ip dscp=40
class-map match-any video
  match ip dscp=18
  match ip dscp=16
```

Step 3 Define the policy-maps for the configuration. In this example, there are three policy-maps:

mpls_policy - models the local site router policy
pe-policy - models the SPN router policy
low_speed - models the remote site router policies

In this example, the same details are configured for each policy-map.

The monitor-queuing-map values specified above are applied to each policy-map class:

```
host(config-mqmap)$ policy-map mpls_policy
host(config-pmap)$ class realtime
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 25
host(config-pmap-c)# class critical
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class video
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class bulk
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 10
host(config-pmap-c)# class besteffort
host(config-pmap-c)$ monitor-queuing low_speed
```

The other policy-maps are configured in the same way:

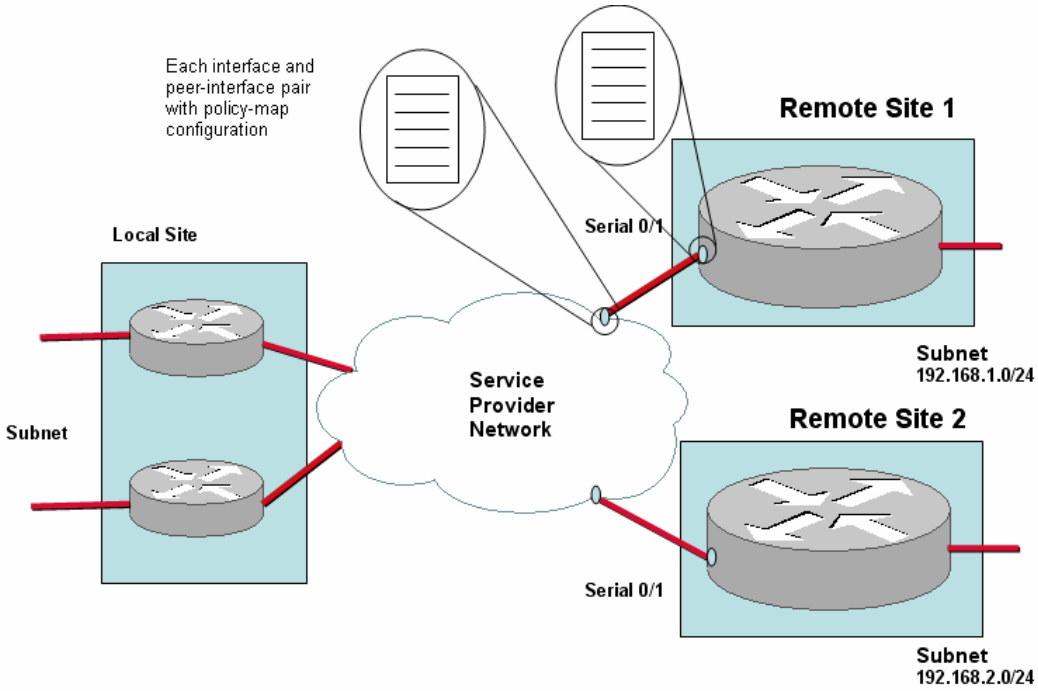
Step 4 Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has one interface, Fast Ethernet0, with an associated peer-interface, both connected to the 10000 kbps link and each using a separate policy-map. The physical measurement ports Port A and PortB are mapped to the core1 local site router. PortC and PortD are mapped to the core2 local site router:

```
host(config)$ local-site Local-site
host(config-local-site)$ subnet 192.168.5.0/24
host(config-local-site)$ router core1
host(config-local-site-router)$ interface FastEthernet0
host(config-local-site-router-if)$ description "Link to SPN
MPLS"
host(config-local-site-router-if)$ bandwidth 10000
host(config-local-site-router-if)$ service-policy output
mpls_policy
host(config-local-site-router-if)$ peer-interface FastEthernet0
host(config-local-site-router-pif)$ description "interface on
PE"
host(config-local-site-router-pif)$ bandwidth 10000
host(config-local-site-router-pif)$ service-policy output pe-
policy
host(config-local-site-router-pif)$ attached-port PortA PortB
host(config-local-site-router-pif)$ router core2
host(config-local-site-router)$ interface FastEthernet0
host(config-local-site-router-if)$ description "Link to SPN
MPLS"
host(config-local-site-router-if)$ bandwidth 10000
host(config-local-site-router-if)$ service-policy output
mpls_policy
host(config-local-site-router-if)$ peer-interface FastEthernet0
host(config-local-site-router-pif)$ description "interface on
PE"
host(config-local-site-router-pif)$ bandwidth 10000
host(config-local-site-router-pif)$ service-policy output pe-
policy
host(config-local-site-router-pif)$ attached-port PortC PortD
```

Note You configure peer-interfaces to complete the network model for MPLS VPN, Internet VPN, Private VPN deployments.

In cases where you have access to the service provider PE router configuration details, you configure the equivalent peer-interfaces in the network model accordingly. If you do not have this information, you configure each peer-interface with the same details as the site interface with which it is paired.

Figure 7-16: Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment – Remote Site Configuration



Step 5 Define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, with interface and peer-interface configurations:

```
host(config-local-site-router-pif)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ ping-address 192.168.1.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote1
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to SPN MPLS"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ peer-interface Serial0/1
host(config-site-router-pif)$ description "interface on PE"
host(config-site-router-pif)$ bandwidth 512
host(config-site-router-pif)$ service-policy output pe-policy
host(config-site-router-pif)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
host(config-site)$ ping-address 192.168.2.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote2
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to SPN MPLS"
host(config-site-router-if)$ bandwidth 256
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ peer-interface Serial0/1
host(config-site-router-pif)$ description " interface on PE"
host(config-site-router-pif)$ bandwidth 256
host(config-site-router-pif)$ service-policy output pe-policy
```

```
host(config-site-router-pif)$
```

Step 6 Check the configuration with the **show config** command:

```
host(config-site-router-pif)$ show config
monitor-queuing-map low_speed
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
!
monitor-end2end-map low_speed
  measure-ping interval-milliseconds 10000 size-bytes 36
availability-threshold 10 event-thresholds delay-milliseconds
500 loss
!

class-map match-any besteffort
  match ip dscp=0
class-map match-any bulk
  match ip dscp=10
class-map match-any critical
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map match-any realtime
  match ip dscp=46
  match ip dscp=40
class-map match-any video
  match ip dscp=18
  match ip dscp=16
!
!
policy-map low_speed
  class realtime
    monitor-queuing low_speed
    bandwidth 25
  class critical
    monitor-queuing low_speed
    bandwidth 20
  class video
    monitor-queuing low_speed
    bandwidth 20
  class bulk
    monitor-queuing low_speed
    bandwidth 10
  class besteffort
    monitor-queuing low_speed
  class class-default

policy-map mpls_policy
  class realtime
    monitor-queuing low_speed
    bandwidth 25
  class critical
    monitor-queuing low_speed
    bandwidth 20
  class video
    monitor-queuing low_speed
    bandwidth 20
```

```
    class bulk
      monitor-queuing low_speed
      bandwidth 10
    class besteffort
      monitor-queuing low_speed
    class class-default

  policy-map pe_policy
    class realtime
      monitor-queuing low_speed
      bandwidth 25
    class critical
      monitor-queuing low_speed
      bandwidth 20
    class video
      monitor-queuing low_speed
      bandwidth 20
    class bulk
      monitor-queuing low_speed
      bandwidth 10
    class besteffort
      monitor-queuing low_speed
    class class-default

  local-site Local-site
    subnet 192.168.5.0/24
    router core1
      attached-port PortA PortB
      interface FastEthernet0
        description "Link to SPN MPLS"
        bandwidth 10000
        service-policy output mpls_policy
      peer-interface FastEthernet0
        description "interface on PE"
        bandwidth 10000
        service-policy output pe-policy
    router core2
      attached-port PortC PortD
      interface FastEthernet0
        description "Link to SPN MPLS"
        bandwidth 10000
        service-policy output mpls_policy
      peer-interface FastEthernet0
        description "interface on PE"
        bandwidth 10000
        service-policy output pe-policy


  site "Remote Site 1"
    subnet 192.168.1.0/24
    ping-address 192.168.1.5
    end2end-target low_speed
    router remote1
      interface Serial0/1
        description "Link to SPN MPLS"
        bandwidth 512
        service-policy output low_speed
      peer-interface Serial0/1
        description "interface on PE"
        bandwidth 512
```

```
        service-policy output pe-policy

site "Remote Site 2"
  subnet 192.168.2.0/24
  ping-address 192.168.2.3
  end2end-target low_speed
  router remote2
    interface Serial0/1
      description "Link to SPN MPLS"
      bandwidth 256
      service-policy output low_speed
    peer-interface Serial0/1
      description "interface on PE"
      bandwidth 256
      service-policy output pe-policy
--More--
```

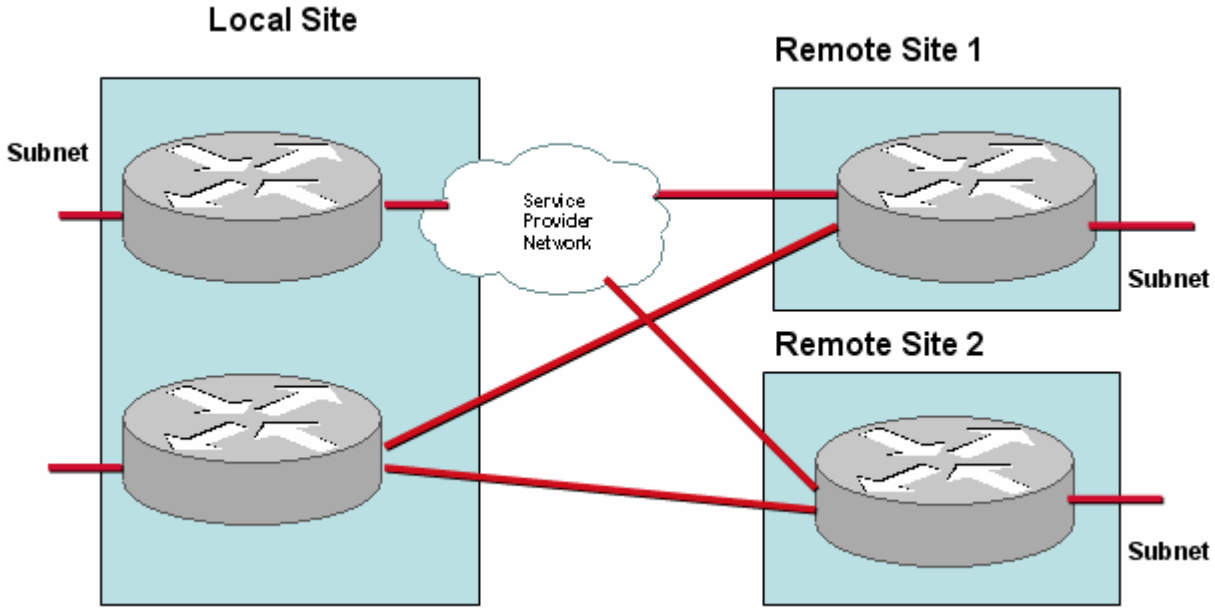
Step 7 When you have satisfied with the configuration, you save your changes. To save the new configuration, you use the copy command:

```
host(config)$ copy config
```

Hybrid Deployment

The BQM is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' site contains the BQM and so all measurements are made from the perspective of the local site. Each local site router must be bound to specific BQM physical measurement ports.

Figure 7-17 Network Model – Hybrid Deployment



To configure the network model for this deployment, you configure the following:

- Local site
  - Default site in model that contains a BQM; the name is editable
  - Subnet
  - Routers
  - Local site interface/SPN peer-interface pair for MPLS part of deployment with bandwidth configuration and policy-maps
  - Local site router with point-to-point connections to remote sites with bandwidth configuration and policy-maps
  - Mapping of BQM physical measurement ports to routers

- Remote Site 1 and Remote Site 2
  - Name
  - Subnet
  - Router
  - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps
  - Remote site interfaces in point-to-point connection with local site router with bandwidth configuration and policy-maps

To configure the network model for this deployment from the CLI, you do the following:

Step 1 Define the monitor-queuing-map and monitor end2end map for the configuration. In this example monitor-queuing-map configuration, Corvil Bandwidth is explicitly enabled, microburst measurement is enabled down to a resolution of 150 milliseconds, and a queuing delay target of 150 milliseconds is specified:

```
host(config)$ monitor-queuing-map low_speed
host(config-mqmap)$ measure-bandwidth
host(config-mqmap)$ measure-microburst milliseconds 150
host(config-mqmap)$ queuing-targets delay-milliseconds 150
```

For more information on defining monitor-queuing-maps, see the **monitor-queuing-map**, **measure-bandwidth**, **measure-microburst**, and **queuing-targets** commands in the "Command Reference" chapter of this document.

In this example monitor end2end map, the default ping interval and ICMP packet size are retained, and event detection is enabled in case of delay exceeding 500 ms and if any packets are lost.

```
host(config-mqmap)$ monitor-end2end-map low_speed
host(config-me2emap)$ measure-ping event-thresholds delay-
milliseconds 500 loss
```

For more information on defining monitor-end2end-maps, see the **monitor-end2end-map**, and **measure-ping** commands in the "Command Reference" chapter of this document.

Step 2 Define the class-maps for the configuration. In this example, there are the following class-maps:

realtime
critical
video
bulk
besteffort

The class-map details are configured as follows:

```
class-map match-any besteffort
  match ip dscp=0
class-map match-any bulk
  match ip dscp=10
class-map match-any critical
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map match-any realtime
  match ip dscp=46
  match ip dscp=40
class-map match-any video
  match ip dscp=18
  match ip dscp=16
```

Step 3 Define the policy-maps for the configuration. In this example, there are three policy-maps:

mpls_policy - models the local site router policy
pe-policy - models the SPN router policy
low_speed - models the remote site router policies

In this example, the same details are configured for each policy-map.

The monitor-queuing-map values specified above are applied to each policy-map class:

```
host(config-mqmap)$ policy-map mpls_policy
host(config-pmap)$ class realtime
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 25
host(config-pmap-c)# class critical
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class video
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class bulk
host(config-pmap-c)$ monitor-queuing low_speed
host(config-pmap-c)# bandwidth percent 10
host(config-pmap-c)# class besteffort
host(config-pmap-c)$ monitor-queuing low_speed
```

The other policy-maps are configured in the same way:

Step 4 Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has one interface, Fast Ethernet0, with an associated peer-interface, both connected to the 10000 kbps link and each using a separate policy-map. The physical measurement ports Port A and PortC are mapped to the core1 local site router. PortB and PortD are mapped to the core2 local site router:

```
host(config)$ local-site Local-site
host(config-local-site)$ subnet 192.168.5.0/24
host(config-local-site)$ router core1
host(config-local-site)$ attached-port PortA PortC
host(config-local-site-router)$ interface FastEthernet0
```

```
host(config-local-site-router-if)$ description "Link to SPN
MPLS"
host(config-local-site-router-if)$ bandwidth 10000
host(config-local-site-router-if)$ service-policy output
mpls_policy
host(config-local-site-router-if)$ peer-interface FastEthernet0
host(config-local-site-router-pif)$ description "interface on
PE"
host(config-local-site-router-pif)$ bandwidth 10000
host(config-local-site-router-pif)$ service-policy output pe-
policy
host(config-local-site-router-pif)$ router core2
host(config-local-site)$ attached-port PortB PortD
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to Remote
Site 1"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
low_speed
host(config-local-site-router-if)$ interface Serial0/2
host(config-local-site-router-if)$ description "Link to Remote
Site 2"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
low_speed
```

Note You configure peer-interfaces to complete the network model for the MPLS portion of this deployment.

In cases where you have access to the service provider PE router configuration details, you configure the equivalent peer-interfaces in the network model accordingly. If you do not have this information, you configure each peer-interface with the same details as the site interface with which it is paired.

Step 5 Define the remote site details for the configuration. In this example, there are two remote sites. Each remote site has its own subnet. Each remote site has a site router, with one interface and peer-interface pair configured to the Service Provider cloud and one interface directly connected back to a local site router interface. You need to specify an additional **attached-port** command for each interface connecting to the Service Provider cloud. This enables the BQM to distinguish between the traffic coming in via the different routes (that is, one route via the SP cloud and one route via a direct point-to-point connection):

```
host(config-local-site-router-pif)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ ping-address 192.168.1.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote1
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to SPN MPLS"
host(config-site-router-if)$ attached-port PortA PortC
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ peer-interface Serial0/1
```

```
host(config-site-router-pif)$ description "interface on PE"
host(config-site-router-pif)$ bandwidth 512
host(config-site-router-pif)$ service-policy output pe-policy
host(config-site-router-pif)$ interface Serial0/2
host(config-site-router-if)$ description "P2P Link to Local
Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ connects-to Local-site core2
Serial0/1
host(config-site-router-pif)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
host(config-site)$ ping-address 192.168.2.5
host(config-site)$ end2end-target low_speed
host(config-site)$ router remote2
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to SPN MPLS"
host(config-site-router-if)$ attached-port PortB PortD
host(config-site-router-if)$ bandwidth 256
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ peer-interface Serial0/1
host(config-site-router-pif)$ description "interface on PE"
host(config-site-router-pif)$ bandwidth 256
host(config-site-router-pif)$ service-policy output pe-policy
host(config-site-router-pif)$ interface Serial0/2
host(config-site-router-if)$ description "P2P Link to Local
Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ service-policy output low_speed
host(config-site-router-if)$ connects-to Local-site core2
Serial0/2
```

Notice that the **attached-port** commands are used only for remote site interfaces (not peer-interfaces) that are connected to the SP cloud.

Step 6 Check the configuration with the **show config** command:

```
host(config-site-router-pif)$ show config
monitor-queuing-map low_speed
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
!
monitor-end2end-map low_speed
measure-ping interval-milliseconds 10000 size-bytes 36
availability-threshold 10 event-thresholds delay-milliseconds
500 loss
!

class-map match-any besteffort
  match ip dscp=0
class-map match-any bulk
  match ip dscp=10
class-map match-any critical
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map match-any realtime
```

```
    match ip dscp=46
    match ip dscp=40
  class-map match-any video
    match ip dscp=18
    match ip dscp=16
  !
  !
  policy-map low_speed
    class realtime
      monitor-queuing low_speed
      bandwidth 25
    class critical
      monitor-queuing low_speed
      bandwidth 20
    class video
      monitor-queuing low_speed
      bandwidth 20
    class bulk
      monitor-queuing low_speed
      bandwidth 10
    class besteffort
      monitor-queuing low_speed
    class class-default

  policy-map mpls_policy
    class realtime
      monitor-queuing low_speed
      bandwidth 25
    class critical
      monitor-queuing low_speed
      bandwidth 20
    class video
      monitor-queuing low_speed
      bandwidth 20
    class bulk
      monitor-queuing low_speed
      bandwidth 10
    class besteffort
      monitor-queuing low_speed
    class class-default

  policy-map pe_policy
    class realtime
      monitor-queuing low_speed
      bandwidth 25
    class critical
      monitor-queuing low_speed
      bandwidth 20
    class video
      monitor-queuing low_speed
      bandwidth 20
    class bulk
      monitor-queuing low_speed
      bandwidth 10
    class besteffort
      monitor-queuing low_speed
    class class-default

  local-site Local-site
    subnet 192.168.5.0/24
```

```
    router core1
      attached-port PortA PortC
      interface FastEthernet0
        description "Link to SPN MPLS"
        bandwidth 10000
        service-policy output mpls_policy
      peer-interface FastEthernet0
        description "interface on PE"
        bandwidth 10000
        service-policy output pe-policy
    router core2
      attached-port PortB PortD
      interface Serial0/1
        description "Link to Remote Site 1"
        bandwidth 512
        service-policy output low_speed
      interface Serial0/2
        description "Link to Remote Site 2"
        bandwidth 512
        service-policy output low_speed


  site "Remote Site 1"
    subnet 192.168.1.0/24
    ping-address 192.168.1.5
    end2end-target low_speed
    router remote1
      interface Serial0/1
        description "Link to SPN MPLS"
        attached-port PortA PortC
        bandwidth 512
        service-policy output low_speed
      peer-interface Serial0/1
        description "interface on PE"
        bandwidth 512
        service-policy output pe-policy
      interface Serial0/2
        description "P2P Link to Local Site"
        bandwidth 512
        service-policy output low_speed
        connects-to Local-site core2 Serial0/1



  site "Remote Site 2"
    subnet 192.168.2.0/24
    ping-address 192.168.2.5
    end2end-target low_speed
    router remote2
      interface Serial0/1
        description "Link to SPN MPLS"
        attached-port PortB PortD
        bandwidth 256
        service-policy output low_speed
      peer-interface Serial0/1
        description "interface on PE"
        bandwidth 256
        service-policy output pe-policy
      interface Serial0/2
        description "P2P Link to Local Site"
```

```
        bandwidth 512
        service-policy output low_speed
        connects-to Local-site core2 Serial0/2

--More--
```

Step 7 When you have satisfied with the configuration, you save your changes. To save the new configuration, you use the copy command:

```
host(config)$ copy config
```

8 System Administration

This chapter provides information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance. Many of these tasks are performed using the BQM command line interface.

This chapter has the following major sections:

- User Administration
- Basic System Setup
- System Status and Resources
- Backup and Restore
- Diagnostics
- Configuring Fault Notification
- Performing a Manual Packet Capture

User Administration

This section contains the following topics:

- Changing User Passwords
- Password Recovery
- Viewing Current User Sessions

You can log on to the BQM CLI as one of the following users:

- admin
- config

When you have set up the BQM, both admin and config users can log on remotely via telnet or ssh. There can only be one admin user and five config users logged in to the BQM at any one time.

If you log in as a config user you have access to configuration commands and a basic set of administrative commands. Configuration mode allows you to make changes to the BQM configuration. If you log in as an admin user, you also have access to the following additional administration commands:

- allow
- backup
- license
- ntp
- reload
- setup
- shutdown

Also the following commands allow additional functionality to the admin user:

- copy
- show

Changing User Passwords

If you log on to the BQM as an admin user, you have the ability to change both the admin and config user account passwords.

Note You should change both passwords on the first day of use, as soon as you have set up the BQM. Valid passwords comprise a mixture of at least eight upper and lowercase, alphanumeric and non-alphanumeric characters.

For example, to change the config user account password, you use the **password** command:

```
host /# password config
Changing password for config
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.


Enter new password:
Re-enter new password:
password: The password for config has been changed.

host /#
```

Password Recovery

To restore the original default passwords shipped with the BQM, you do the following:

Log in at the serial console using the username restorepasswords. No password is needed.

This can only be done from the serial console, that is, a physical link to the appliance.

Viewing Current User Sessions

The Current User Sessions table is a record of the users who are logged into the application. The user session times out after 20 minutes of inactivity. After a user session times out, that row is removed from the table.

To view the current user sessions table you use the **show users** command on the BQM CLI:

```
host(config)# show users
User              Connection    From            Host
-------------------------------------------------------------
config            Terminal      Sep 7 09:30    172.18.3.126
monitor           GUI           Sep 07 09:10    -
admin             GUI           Sep 07 09:18    -
host(config)#
```

Table 8-1: Current User Sessions

Column	Description
User	Identifies the type of user logged in: GUI users – admin, monitor CLI users – admin, config
Connection	Identifies whether the user is logged in to the CLI (Terminal) or the GUI.
From	Displays the time at which the user logged in.
Host	The IP address is displayed for CLI users only. If a user is logged in via the serial port, the Host column displays `serial-line`.

System Setup

The basic system setup operations include:

- Installing a License
- Viewing and Configuring Network Settings
- Restricting SNMP Access
- Restricting IP Address Access
- System Time Settings

Installing a License

If the BQM is unlicensed, the major features of the product are disabled. You are notified when you log in to the BQM CLI or GUI if there is no valid license. You can check the licensing status using the BQM CLI **status** command. Requests for licenses must be accompanied by the system ID of the BQA. The System ID may be retrieved using the **status** command.

```
host(config)$ status

Cisco Bandwidth Quality Manager software: Version 3.0 (trunk.21883 Thu 07
Sep 20
06)
CorvilMeter software: CDK_3_0_BUILD_27 (conf Sep  7 03:43:41 2006)
Application Recognition Module: ARM (full) v3.5
System type: 20b
Logging: <off>
Access control: unrestricted
 uptime is 32 minutes, 41 seconds

License system id: 03b568de49115aaa2d
License status: ** missing **

cpu #0: "Intel(R) Xeon(TM) CPU 2.66GHz", 512 KB cache, 1%
cpu #1: "Intel(R) Xeon(TM) CPU 2.66GHz", 512 KB cache, 1%
cpu #2: "Intel(R) Xeon(TM) CPU 2.66GHz", 512 KB cache, 1%
cpu #3: "Intel(R) Xeon(TM) CPU 2.66GHz", 512 KB cache, 2%
5-minute average load (all CPUs): 1%
```

In this example, the BQM is unlicensed and the license system id is displayed.

Licenses consist of a plain text file (file extension `.lic`) that must be installed on the BQM. If there is an attempt to install an invalid license, or a license that doesn't match the BQM system ID, an error is reported and no license is installed.

To install the BQM license you use the **license** command from the BQM CLI**.** You must be logged in to the BQM CLI as an admin user to use this command.

license install tftp://[<hostname> | <A.B.C.D>]/*remote_filename*

For example, to install the specified license file from tftp host 192.16.10.1, use the following:

```
host(config)$ license install
tftp://192.16.10.1/BQM_license/BQM_0E456de6556aaa.lic
```

If the license has been installed, this command displays the text of the BQM license agreement when no arguments specified. To display the license agreement, you do the following:

```
host(config)$ license
```

Installing a License Using SSH

It is possible to install the license file directly on the BQM using SSH. To perform the license installation procedure you need an ssh client. For Windows users, we recommend the OpenSSH client. The OpenSSH client may be downloaded from: http://sshwindows.sourceforge.net/download/

The 'plink' client (part of the puTTY distribution) is not suitable for this purpose). Also, if you already have an ssh client such as cygWin installed, attempting to install OpenSSH may cause problems.

Having received the license file, save it to your desktop.

On Windows, open a command prompt (Start >Run >'cmd');

On Linux, Solaris, or other Unix system, open a terminal window.

In either case, then run the following command:

```
ssh admin@name install license < licensefile.lic
```

where you should replace *name* with the DNS name or IP address of the BQM, and replace *licensefile*.lic with the full path and filename of the license file you receive. After entering the admin user password, the license will be installed. If there are any problems, you will see an error message.

Configuring Network Settings

To reconfigure the BQM network settings, involving the setup of the BQM IP address, subnet mask, hostname, and the adjacent router's IP address and the IP address of the Domain Name Server (DNS) for DNS name resolution, you use the **setup** command. You must be logged in to the BQM CLI as an admin user to use this command. The setup is automatically run on the first admin login and on subsequent logins if you quit the first setup or you do not change the supplied default values.

This command prompts you for the following information:

Table 8-2: Setup Information

IP address	Specify an IP address for the BQM. If you specify a prefix length when entering the IP Address, you will be automatically shown the appropriate subnet mask in the next step.
Netmask	Specify a subnet mask for the BQM.
Router	Specify an IP address for the adjacent router.
Domain-name-server	Specify an IP address for the domain name server for DNS name resolution.
Hostname	Specify a hostname for the BQM.

Here is an example of using the **setup** command:

```
host(config)$ setup

IP address: 192.16.5.1/24
Netmask: 255.255.255.0
Router: 192.16.5.254
Domain-name-server: 192.16.24.1
Hostname: corphq_nyc
```

To define DNS Name Servers that can be used by the BQM for DNS name resolution, you can also use the **domain** command in addition to the **setup** command. A specific DNS Name Server can be removed by use of 'no domain name-server <A.B.C.D>' where A.B.C.D is the IP v4 dotted decimal address of the specific DNS Name Server.

In this example, the DNS server with IP address 192.16.24.2 is configured for BQM host name resolution:

```
host(config)$ domain name-server 192.16.24.2
```

Restricting SNMP Access

If you are logged in as admin user, you can restrict SNMP access to the BQM using the **snmp-server** command.

SNMPv2 uses simple community-based authentication to check if SNMP requests are allowed. For example, an SNMP MIB browser sends a plain text community string to identify itself. The SNMP agent or server checks the plain text community string to determine if it will answer the request.

The default configuration on the BQM is ‘public. This community string is not configurable.

Restricting IP Address Access

By default, all IP addresses are allowed to connect to the BQM. If you are logged in as the admin user you can allow only a single, or certain multiple appliances or subnet addresses to access the BQM. Typically you add an entry for the TFTP server IP address. You do this using the **allow** command. To configure multiple addresses, you use the **allow** command repeatedly as required. To configure access from a subnet, you supply a prefix with the command. For example, to allow an appliance with IP address 192.168.128.5 to have access to the BQM, you type the following command:

```
host(config)$ allow 192.168.128.5
host(config)$
```

To remove an allowed IP address, you use the **no allow** command. In the following example, the IP address 192.168.128.5 is no longer allowed access to the BQM:

```
host(config)$ no allow 192.168.128.5
host(config)$
```

To remove all allowed IP addresses that have been previously set, you use the **no allow** * command. This switches off access restrictions and allows all addressable appliances to connect:

```
host(config)$ no allow *
host(config)$
```

To allow access from subnet 192.168.128.0:

```
host(config)$ allow 192.168.128.0/24
host(config)$
```

In this example, you begin with an unrestricted appliance. You telnet in from the IP address 192.168.128.1 and you try to allow 192.168.128.200. Doing this alone would prevent your computer from subsequently accessing the BQM:

```
host(config)$ allow 192.168.128.200
```

```
Warning: you are accessing the appliance via the IP address
‘192.168.128.1’.
‘allow 192.168.128.200’ will prevent you accessing the appliance. Continue
(y/n)? n
host(config)$
```

You can use the **status** command to verify whether access restrictions are in place or not.

System Time Settings

You can check the current time configuration on the BQM using the **show clock** or **clock** commands.

```
host(config)$ show clock
10:42:56  7 December 2006 UTC  (UTC)
host(config)$
```

Using the **clock** command without parameters displays the current time without time zone information.

```
host(config)$ clock
10:15:56  7 December 2006
```

Setting the System Time

To manually set the system software clock, you use the **clock set** command. Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP), you need not set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command.

Setting the clock results in the BQM being rebooted to ensure consistency.

clock set *hh*:*mm*:*ss day month year*

Table 8-3: Clock Command Settings

hh:*mm*:*ss*	Specify the current time in hours (24-hour format), minutes, and seconds.
day	Specify the current day (by number) in the month.
month	Specify the current month (by full name).
year	Specify the current year (four digits, no abbreviation).

The following example manually sets the software clock to 7:29 p.m. on May 13, 2003:

```
host(config)$ clock set 19:29:00 13 May 2003
```

Setting the Time Zone

To set the time zone for display purposes, use the **clock timezone** command. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command:

clock timezone *zone*

Table 8-4: Clock Timezone Command Settings

zone	Name of the time zone. The complete list of available time zone names is available in the command reference.

The following example sets the time zone to Eastern Standard Time in the U.S., which is 5 hours behind UTC:

```
host(config)$ clock timezone US/EST
```

Configuring an NTP Time Server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, you use the **ntp server** command. You must be logged in to the BQM CLI as an admin user to use this command. To disable this capability, use the **no** form of this command.

ntp server { [*IP address* | *hostname*] [**prefer**] }

Table 8-5: NTP Server Command Settings

IP address	Specify the IP v4 dotted decimal address of the server providing the clock synchronization .
hostname	Specify the DNS host name of the server providing the clock synchronization .
prefer	Specifies that the server is referenced in this command is preferred over other configured NTP servers.

In this example, the **ntp** command is used to switch on time synchronization using the server with IP address 192.168.128.4:

```
host(config)$ ntp server 192.168.128.4
host(config)$
```

System Status and Resources

You can use the **status** command to check the status of the BQM. The **status** command returns information about the BQM, such as the software version, CPU information, and memory usage details.

```
host(config)# status
Cisco Bandwidth Quality Manager software: Version 3.0 (trunk.21883 Thu 07
Sep 20
06)
CorvilMeter software: CDK_3_0_BUILD_27 (conf Sep  7 03:43:41 2006)
Application Recognition Module: ARM (full) v3.5
System type: 11a
Logging: <off>
Access control: unrestricted
 uptime is 2 days, 22 hours, 54 minutes, 10 seconds

License system id: 0366ef7d042e4f3ece
License status: valid
License features: Sites: 100, Packet Capture: enabled
License evaluation time total: unlimited
License evaluation time remaining: unlimited

cpu #0: "Intel(R) Xeon(TM) CPU 3.40GHz", 2048 KB cache, 34%
cpu #1: "Intel(R) Xeon(TM) CPU 3.40GHz", 2048 KB cache, 20%
cpu #2: "Intel(R) Xeon(TM) CPU 3.40GHz", 2048 KB cache, 32%
cpu #3: "Intel(R) Xeon(TM) CPU 3.40GHz", 2048 KB cache, 32%
5-minute average load (all CPUs): 16%

disk #0: "IBM-ESXS ST3300007LC FN", total=287352268 KB, used=3190848 KB
(1%)
disk #1: "IBM-ESXS ST3300007LC FN", total=288370300 KB, used=28169516 KB
(10%)

11 fan component(s), 0 alert(s)
2 power supply component(s), 1 alert(s)
  Alert for #0: "IPMI sensor PSU 1 Supply [70]: Unspecified problem"
6 temperature sensor component(s), 0 alert(s)
BIOS date: 01/17/05

Memory: total=4149572 KB, cached=1695540 KB, used=3989372 KB (46%)
        5-minute average usage: 46%

System throughput: 0%

Interface        Received              Sent
---------        --------              ----
mgmt:
          bytes  480846032             1367619851
        packets  5891334               10352629
   dropped pkts  0
   frame errors  0
     CRC errors  0
protocol errors  0

PortA:
```

```
          bytes  0
        packets  0
   dropped pkts  0
   frame errors  0
     CRC errors  0
protocol errors  0

PortB:
          bytes  147241350322
        packets  526796370
   dropped pkts  0
   frame errors  0
     CRC errors  0
protocol errors  0

PortC:  *** down 2 days, 22 hours, 54 minutes, 6 seconds ***
          bytes  0
        packets  0
   dropped pkts  0
   frame errors  0
     CRC errors  0
protocol errors  0

PortD:  *** down 2 days, 22 hours, 54 minutes, 6 seconds ***
          bytes  0
        packets  0
   dropped pkts  0
   frame errors  0
     CRC errors  0
protocol errors  0

Configuration totals:
            class-maps: 51
               matches: 121
            interfaces: 27
  monitor-queuing-maps: 11
  monitor-end2end-maps: 5
       peer-interfaces: 20
           policy-maps: 15
               routers: 19
                 sites: 18
    configured classes: 93
        active classes: 239
      service policies: 47

Packets dropped during disk capture: 0

host(config)#
```

Table 8-6: System Status and Resource Information

Status Information	Description
Version Information	Displays the software component version information for the current release of the BQM software. This information is also displayed using the **show version** command.
System Type	Displays the current system platform configuration type.
Logging	Displays whether logging has been enabled or disabled. For more information see the section "Storing System Log Messages" or the **logging** command.
Access Control	Displays whether IP address access control has been enabled or disabled. For more information see the section "Restricting IP Address Access" or the **allow** command.
License Information	Displays the following license information: License system id: the unique system id number required when applying for a license License status: the current licensing status of the BQM License features: the features available with the current license (100 or more sites, packet capture enabled/disabled) License evaluation time total: the duration of the current license License evaluation time remaining: the time remaining until the current license expires
CPU Utilization	Displays CPU utilization information for each CPU, including a five-minute average utilization figure across all CPUs.
Disk Utilization	Displays disk utilization information for each disk.
Components, Alerts	Displays a list of system hardware components and any alerts raised against them.
BIOS Date	Displays the date of the BIOS.
Memory Utilization	Displays memory utilization information, including a five-minute average usage value.
System Throughput	Displays a percentage value indicating the extent to which network interface card buffers are filling up. High values (over 90%) may indicate that packet drops are possible, compromising displayed results or packet capture data.
Configuration Totals	Displays the total number of each configuration object in the current configuration file. To find out more about the configuration details, you use the **show** command.
Packets dropped during disk capture	Displays the number of packets dropped (if any) during the operation of packet capture. This gives you an indication of how reliable the packet capture data is.

Backup and Restore

This section contains the following topics:

- Restoring System Software
- Backing Up and Restoring Configuration and Packet Capture Files
- Upgrading the Application Recognition Module (ARM)

Restoring System Software

In general, the restore procedure involves the following steps:

1. Backup current configuration file and database
2. Perform restore – ftp, scp the previous system image or locally
3. Perform recovery mechanism and verify the restore

The system software restore can be done using the **copy** command from the BQM CLI, or from a remote, connected machine using ssh. During a restore operation, the current BQM IP address, login settings, and configuration information are all persisted.

As a precaution, you can backup the configuration, the database and packet capture files from the BQM to an FTP server or using scp. The following section describes the tasks involved in upgrading the system software. To copy the configuration file to a specified directory on an FTP server with the specified relative path, you use the **copy** command:

backup <data | data-with-captures> ftp://[*hostname* | A.B.C.D]/[*file path/*]*file [username] [password]*

Note If you are performing a backup using ftp, the ftp process will only create one new target directory at a time. The scp option enables you to create more than one target directory.

Alternatively, you can use scp:

backup <data|data-with-captures> scp://[*hostname*|A.B.C.D]/ [*file path/*]*file* [*username*] [*password*]

Alternatively, if you want to backup the configuration file you can ssh from a remote machine. To do so, you do the following:

ssh admin@*bqm_hostname* **retrieve config >** [*file path/*]*file*

To back up the current operational system software image file used on the BQM to a specified file in a TFTP directory on a TFTP server with the specified relative path You must be logged in as an admin user to perform this operation.

copy system-image tftp://[hostname | A.B.C.D]/[*file path/*]*file*

In this example the BQM configuration and database (but no packet capture files) are first backed up and then the current system software image is also backed up:

```
host(config)$ backup data scp://192.168.128.2/backup/1155756573_2006-08-16-192933 admin adminp4sswd
host(config)$ copy system-image tftp://192.168.128.2/image/CBQM-v3.0_trunk.21883_RELEASE.gz
```

To restore a specified system image file from the TFTP directory on a TFTP server with the specified relative path to the BQM, you use the **copy** command. The new image is initially copied in as the standby image, so the current operational system image in memory remains unaffected.

```
copy tftp://A.B.C.D/[file path/]file standby-system-image
```

The new file should first be copied into the root directory of the TFTP server before the restore is done. To perform the restore, you copy the chosen system image to the BQM. You must be logged in as an admin user to perform this operation. In the following example the new system image is copied from a tftp server with IP address 192.168.128.1:

```
copy tftp://192.168.128.1 CBQM-v3.0_trunk.21950_RELEASE.gz standby-system-image
```

The new standby image file does not become effective until the **reload standby-system-image** command is executed:

```
reload standby-system-image
```

To verify the procedure, you can log in to the BQM and use the **show version** command to check the restored software build number.

The standby image version is always the image that was installed immediately before the current operational image. You can check the current standby software version, using the **show version standby-system-image** command:

```
show version standby-system-image
```

If you just want to restore this previous system software image you use the **reload standby-system-image** command in place of the procedure described above:

```
reload standby-system-image
```

For more information on the **reload** and **show version** commands, see the chapter *BQM Commands*.

If you are using ssh from a remote machine, you do the following:

```
ssh admin@bqm_hostname install system < CBQM-v3.0_trunk.21950_RELEASE.gz
```

Backing Up and Restoring Configuration and Packet Capture Files

You can back up the BQM configuration and/or capture files to a specified target using the **backup** command. The target may be an accessible local file system , an FTP server or a host accessible via SSH/SCP. In the case of FTP or SCP backups, the host name (resolvable via DHCP, if configured) or host IP address must be given:

```
backup [data | data-with-captures] backup:path
[scp://[hostname | IP address]/[path] username password]
[ftp://[hostname | IP address]/[path] username password]
```

If a username or password is not entered and the backup is via ftp or scp, you are prompted for them.

For example, to back up the configuration file, including packet capture files to a `/home/myuser` directory on host 192.168.8.10 using scp, you do the following:

```
backup data-with-captures scp://192.168.8.10/home/myuser
```

A backup operation involving packet capture files will usually take significantly longer than one involving a backup of only the BQM configuration.

Note If a backup operation does not return a response for a long period of time and you suspect that the operation has hung, you can reboot the BQM. This will stop the backup and clear up any temporary directories and files created by the backup.

Note When you use the scp or ftp options to perform backups to remote machines, you must have the appropriate write permission for the target path on the remote machine. If you do not have the appropriate permissions, the backup operation will fail.

In the following example, the BQM configuration is backed up locally (without capture files) to a directory named 12-15-2006. The **dir** command is used to illustrate the directory structure created by the backup operation:

```
host(config)$ backup data backup:12-15-2006
Backup task successfully launched in background
host(config)$ dir backup:
backup:/
        Size  Name
        4096  12-15-2006/
host(config)$ dir backup:/12-15-2006
backup:12-15-2006/
        Size  Name
        4096  config/
        4096  database/
host(config)$ dir backup:/12-15-2006/config
backup:12-15-2006/config/
        Size  Name
        4096  section000001/
host(config)$ dir backup:/12-15-2006/config/section000001
backup:12-15-2006/config/section000001/
```

```
        Size  Name
       10805  file000001
host(config)$ dir backup:/12-15-2006/database
backup:12-15-2006/database/
        Size  Name
       37124  file000001
host(config)$
```

The backup operation creates a `/config` directory containing a numbered section directory, which in turn contains the configuration file. A `/database` directory is also created containing the database file. If you specify the backup of packet capture files, a separate `/pcap` directory is also created containing these files.

Before you perform a local backup, you can check the available disk space using the **show file-systems** command.

To restore configuration and/or capture files from a specified target you use the **restore** command. The target may be an accessible filesystem , an FTP server or a host accessible via SSH/SCP. In the case of FTP or SCP backups, the host name (resolvable via DHCP) or host IP address must be given.

Any restore action will cause the system to be halted during the restore process. So you are prompted to confirm a request to perform a restore. If you confirm the restore request, you are logged out. When you log back in again, the restore should be completed.

restore [data | data-with-captures]
[scp://[*hostname* | *IP address*]/[*path*] *username password*]
[ftp://[*hostname* | *IP address*]/[*path*] *username password*]

If a username or password is not entered and the backup is via ftp or scp, you are prompted for them.

For example, to restore the configuration file, including packet capture files from a `/home/myuser` directory on host 192.16.8.10 using scp, you do the following:

restore system-with-captures scp://192.16.8.10/home/myuser

If you are using ssh from a remote machine and you want to install a configuration, do the following:

ssh admin@*bqm_hostname* **install config <** [*file path*/]*file*

Upgrading the Application Recognition Module (ARM)

The BQM employs an Application Recognition Module (ARM) to identify applications automatically when monitoring network traffic. You can use the **show version** command to check the current operating version of the ARM. You use ssh from a remote, connected machine to update the ARM file:

ssh admin@*bqm_hostname* **install arm** < [*file path*/]*file*

In the following example, the ARM is updated from a remote machine for a BQM with host name sanfran_dc:

```
host(config)$ ssh admin@sanfran_dc install arm < arm35.arm.tar.gz
```

If you attempt to update the BQM with a new ARM file that lacks applications that exist in the previous ARM file, and those applications are being used in a class-map or custom-application, the update will not complete and you will see an error reported:

```
Initializing drdl...
Analysing new ARM module (size: 4)
The new ARM file you are attempting to install is missing the following
applications, which are in use by your configuration:

 1: HTTP, used in 1 place:
    class-map test

 2: IRC, used in 1 place:
    custom-application ims

 3: MSN messenger, used in 1 place:
    custom-application ims

4: SSL v3, used in 1 place:
    class-map test

5: Yahoo! messenger, used in 2 places:
    class-map test
    custom-application ims


References to these applications must be removed from your configuration
before you install the new ARM.
```

Diagnostics

This section contains the following topics:

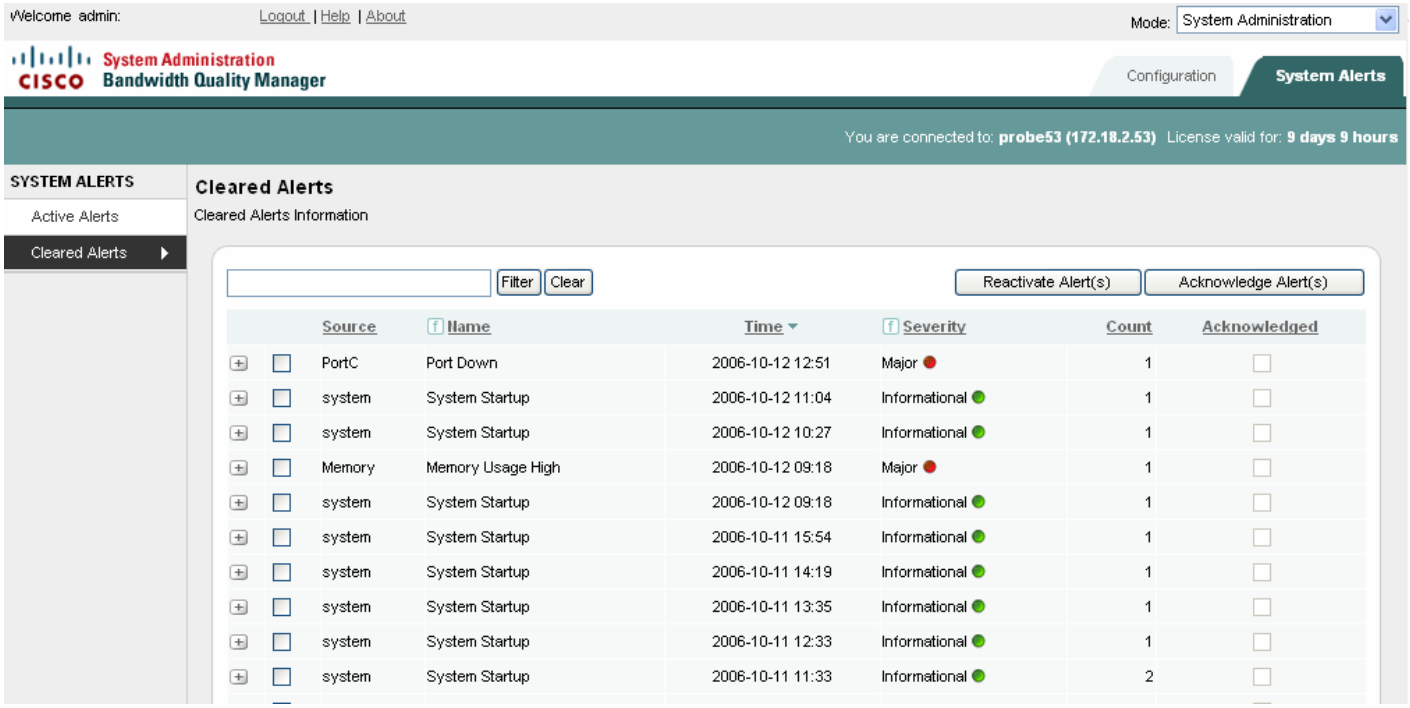
- Viewing System Alerts
- Viewing the Audit Trail
- Generating System Technical Support Diagnostic Information
- Reviewing the System Log
- Storing System Log Messages
- Watchdog Operation

Viewing System Alerts

If you are logged in to the BQM GUI as an admin user you can view active and cleared system alerts.

To open the **System Alerts** tab you go to **System Administration** mode and click the **System Alerts** tab.

Figure 8-1: System Alerts Tab



By default the **System Alerts** tab lists all active alerts triggered due to system events on the BQM itself. Click the **Cleared Alerts** link to view the list of cleared alerts during the chosen reporting period. The summary table information is sorted by the time of the alert. You can sort the active and cleared alert information by column.

System Alert Types

The following system alert types are reported by the BQM:

System Shutdown - indicates that the system is about to be shut down.
System Startup - indicates that the system has started up.
Fan Failure - indicates a problem with the system fan.
Power Supply Failure - indicates a problem with the system power supply.
Watchdog Restart - indicates that the system watchdog has restarted.
Hard Drive Failure - indicates a problem with the system hard disk.
Temperature - indicates that the system temperature is too high.
CPU Failure - indicates a problem with the system CPU.
Port Down - indicates that the named physical port is down.
CPU Usage High - indicates that the CPU utilization is running over the 90% threshold.
System Throughput - indicates that the average buffer utilization is over the 80% threshold.
License Expired - indicates that the product license has expired.
License Invalid - indicates that the product license file on the system is invalid.
License Near Expiration - indicates that the product license is within seven days of expiration.
Memory Usage High - indicates that the memory utilization is above the 90% threshold.
Soft Disk Threshold - indicates that the data storage disk is over 80% full.
Hard Disk Threshold - indicates that the data storage disk is over 95% full.

Viewing Active and Cleared Alerts Information

By default, twenty active or cleared alerts are displayed per page and if there are more than twenty alerts to display, you use the links at the bottom of the list to navigate between pages of results. If there are many active or cleared alerts, you can also click the **View 50**, **View 100**, or **View All** links to display the corresponding number of alerts on a single page. In these cases you scroll down the page to view all the presented results.

The following describes the information displayed in the System Alerts table:

Source - indicates the part of the system affected by the alert.

Name - displays the system alert type.

Time - displays the time at which the active alert triggered, or at which a cleared alert was cleared.

Severity - displays the severity of the alert. The severity levels for SNMP traps are the following:
Informational – events that require notification but do not cause failures
Warning – typically used for thresholds that warn of an impending failure
Minor – not used for defaults
Major – an event that has the potential to make BQM no longer operational
Severe – system no longer operational

Count - the system employs a 30-minute sliding window event coalescing period to avoid the system becoming flooded with alerts. This number displays the number of individual coalesced alert triggers comprising this reported alert since an alert of this type was last cleared.

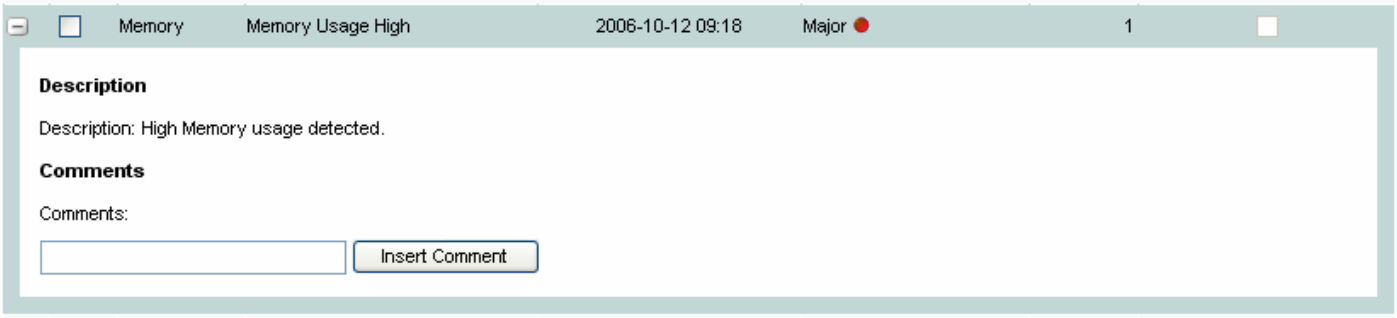
Acknowledged - identifies acknowledged alerts.

Adding a Comment to a System Alert

You can tag the alert with a comment. To add a comment, you do the following:

Step 1 Click + to expand the alert information.

Figure 8-2: Commenting a System Alert



Step 2 Enter the comment text in the **Comments** field and click **Insert Comment**.

Clearing, Reactivating and Acknowledging System Alerts

The following system alerts do not clear automatically:

- System Shutdown
- System Startup
- Watchdog Restart

The remaining system alerts clear automatically when the relevant condition clears or the measured value on which the alert is based returns below the configured threshold. To force an active alert (or group of active alerts) to clear, you check the alert check box(es) on the **Active Alerts** page and click **Clear Alert(s)**. The cleared alerts are no longer displayed on the **Active Alerts** page, but are now shown on the **Cleared Alerts** page.

To force a cleared alert (or group of cleared alerts) to reactivate, you check the alert check box(es) on the **Cleared Alerts** page and click **Reactivate Alert(s)**. The reactivated alerts are no longer displayed on the **Cleared Alerts** page, but are now shown on the **Active Alerts** page.

To acknowledge an alert (or group of alerts), you check the alert check box(es) and click **Acknowledge Alert(s)**.

Sorting the System Alerts Table

The System Alerts table is sorted by the **Time** column by default, but you can sort this table by any column. Click the heading of the column by which you want to sort. The information in the table is then arranged from highest to lowest according to that column. You can click again to reverse the order of the sort and display results from lowest to highest.

For example, to view alerts with the highest severity rating, you click the **Severity** column heading to sort. The summary is rearranged according to the severity of alerts, with the highest severities first. Click the **Severity** column heading again to sort the summary screen again, this time with the lowest severities first.

Filtering the System Alerts Table

You can use the search facility on the **System Alerts** tab to display a particular quality alarm or set of quality alarms of interest. Enter the name of the source of alerts, or part of a name to match a group of sources, and click **Filter**. To clear the filter field text and return to the default display of alerts, click **Clear**.

For example, entering 'Serial' will display all interfaces whose full names (site – router – interface – direction) contain the words 'Serial' or 'serial'.

The **System Alerts** tab also provides the option to filter results based on the type or severity of active or cleared alerts. Click beside the **Name** or **Severity** column headings and select an option from the list. The screen will refresh, displaying only the results relevant to the filtering option you selected. The filter icon changes to indicate that it is in use.

Generating a System Alerts Report

You can generate a report in .pdf format at any point when viewing active or cleared alerts.

To generate a report, click the pdf icon.

The generated report is available for download in .pdf format. Reports are not stored on the system.

The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all cleared major alerts sorted by time over the last hour. If the original results are displayed across multiple pages onscreen, then the report contains the data from all such screens in the order they were displayed at the time the report was generated.

The time displayed at the top of each report is the configured time zone of the system.

When a large report is being generated, the system issues a warning indicating that the action may take some time to complete.

Using the CLI to View Alerts

You can also view a list of recent alerts using the BQM CLI. To do this you use the **show alerts** command. The details displayed are similar to those shown in the GUI.

```
host(config)$ show alerts
Time                    Severity        Count   Ack             Name                    Source
2006-09-07 09:29:30.533 Major           1       false           License Invalid         Licence
2006-09-07 09:29:30.533 Severe          1       false           Hard Drive Failure      PacketCapturesDisk
2006-09-07 09:29:30.533 Major           1       false           Port Down               PortA
2006-09-07 09:29:30.533 Major           1       false           Port Down               PortB
2006-09-07 09:29:30.533 Major           1       false           Port Down               PortD
2006-09-07 09:30:00.043 Major           1       true            Memory Usage High       Memory
```

Viewing the Audit Trail

The audit trail displays a listing of recent critical activities that have been recorded in an internal log file. Syslog messages can also be sent to an external log. The following user activities are logged in the audit trail:

- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- Starting and stopping packet captures

Each log entry contains the following:

- Time stamp
- Object model identifier
- Object name\
- User ID
- Activity description

To view the audit trail you use the **show audit** command:

```
host(config)$ show audit
Occurred At                  Model Entity  Name           User Name  Description
Thu Sep  7 09:28:33 2006       class          class-default   System  Adding class
Thu Sep  7 09:28:33 2006       End2End mmaps  Inter-continent System  Adding end-end-map
Thu Sep  7 09:28:33 2006       End2End mmaps  Internet VPN    System  Adding end-end-map
Thu Sep  7 09:28:33 2006       End2End mmaps  Metro Area      System  Adding end-end-map
Thu Sep  7 09:28:33 2006       End2End mmaps  Short Haul WAN  System  Adding end-end-map
Thu Sep  7 09:28:33 2006       interface      default         System  Adding peer-interface
```

The internal log files are overwritten after reaching a certain size limit.

Generating System Technical Support Diagnostics Information

As well as the various status and system resource information available from the BQM CLI, the BQM records data about potentially noteworthy conditions. This feature generates a potentially extensive display of the results of various internal system troubleshooting commands and system logs.

This information is unlikely to be meaningful to the average user. It is intended to be used by the Cisco TAC for debugging purposes. You are not expected to understand this information; instead, you should copy the information to file and attach it to an email message to the Cisco TAC.

To view the tech support output, you use the **show tech-support** command. To copy the diagnostics information to a file on a tftp server, use the **copy diagnostics** command. You must be logged in as an admin user to use either of these commands:

copy diagnostics tftp://<hostname | A.B.C.D>/[*filepath*]/*filename*

Reviewing the System Log

You can use the **log** command to review the last number of messages written to the system log for diagnostic purposes. As in the case of using the **show tech-support** command, it is intended to be used by the Cisco TAC for debugging purposes.

In this example, the **log** command is used to display the end of the system log:

```
host(config)$ log
Sep  7 14:35:54 (none) local2.notice sudo:     root : TTY=unknown ;
PWD=/etc/init.d ; USER=root ; COMMAND=/bin/mkhdrw
Sep  7 14:35:54 (none) user.warn kernel: EXT2-fs warning: mounting
unchecked fs, running e2fsck is recommended
Sep  7 14:35:54 (none) local2.notice sudo:     root : TTY=unknown ;
PWD=/etc/init.d ; USER=root ; COMMAND=/bin/mkhdro
Sep  7 14:35:54 (none) user.info -probesh: 'config' entered command: show
version
Sep  7 14:36:54 (none) auth.info sshd(pam_unix)[27344]: session closed for
user config
Sep  7 14:39:51 (none) user.info -probesh: 'admin' entered command: show
tech-support
Sep  7 14:39:51 (none) local2.notice sudo:     root : TTY=unknown ;
PWD=/etc/init.d ; USER=root ; COMMAND=/bin/showipmi
Sep  7 14:42:36 (none) user.info -probesh: 'admin' entered command: end
Sep  7 14:42:37 (none) user.info -probesh: 'admin' entered command: log
Sep  7 14:42:37 (none) local2.notice sudo:    admin : TTY=pts/0 ; PWD=/ ;
USER=root ; COMMAND=/bin/logread
```

Storing System Log Messages

The BQM uses a circular log on the local system to store log messages. The size of the circular log is 200 Kb. The BQM can use a remote syslog server to store all system log messages. To copy the system log messages to a remote syslog server, you use the **logging** command. To stop copying the system log messages to a remote syslog server, you use the **no logging** command.

In this example, the **logging** command is used to switch on logging to the syslog server with IP address 192.168.128.4:

```
host(config)# logging 192.168.128.4
host(config)#
```

You can use the **status** command to verify whether remote logging is enabled or disabled.

Watchdog Operation

The BQM comes equipped with a watchdog timer that reboots the system and restarts all services if processing comes to a standstill for whatever reason. This feature ensures system reliability in industrial standalone, or unmanned, environments, for example if performing a remote upgrade.

In practice, the watchdog checks the current status of the BQM every 10 seconds. If the watchdog determines that the BQM is unresponsive, or that it is no longer running then the watchdog will generate an alarm and cause the system to reboot. The BQM reboots, and returns to its last known good state.

Configuring Fault Notification

The BQM provides an integrated faults and alerts management platform for both system and network QoS events. The events of interest that are signaled to the user are divided into two categories:

- Quality Alarms - associated with a configured quality object that is in violation of a specified quality target.
- System Alerts – associated with the infrastructure of the BQM platform. This includes communications and resource faults which occur where the BQM resources have degraded availability or capacity to provide the essential data.

Overview

The BQM supports the logging of system events to a fault management system using SNMP traps and to a remote syslog host.

The severity level for SNMP traps and emails are the following:

- Informational – events that need communicating but do not cause failures
- Warning – typically used for thresholds that warn of an impending failure
- Minor – not used for defaults
- Major – an event that has the potential to make BQM no longer operational
- Severe – BQM no longer operational

The syslog severity levels are defined as follows:

0 – emergency - System is unusable
1 – alert - Immediate action required
2 – critical - Critical condition
3 – error - Error condition
4 – warning - Warning condition
5 – notification - Normal but significant condition
6 – informational - Informational message only
7 – debugging - Message that appears during debugging only

Each fault can be reported at a set frequency, which you can configure. The BQM supports the following frequencies for alerts:

- Every
- Daily
- Hourly
- None

The following table lists the supported network quality faults along with their default syslog and SNMP severities and frequencies:

Table 8-7: Quality Faults

Fault	Description	Syslog Severity	SNMP Severity	Frequency	Clear
Congestion Indicated	The Congestion Indicator crossed the configured threshold.	Alert	Major	Every	Yes
Corvil Bandwidth Threshold Exceeded	The Corvil Bandwidth measurement indicates the class bandwidth threshold has been exceeded.	Alert	Major	Every	Yes
End-to-End Loss Detected	The measured end-to-end loss crossed the configured threshold.	Alert	Major	Every	Yes
Expected Policing Threshold Exceeded	The Expected Policing crossed the configured threshold.	Alert	Major	Every	Yes
Expected Queuing Delay Threshold Exceeded	The Expected Queuing Delay crossed the configured threshold.	Alert	Major	Every	Yes
Expected Queuing Loss Threshold Exceeded	The Expected Queuing Loss crossed the configured threshold.	Alert	Major	Every	Yes
Microburst Detected	Microbursts exceeding the configured bandwidth threshold have been detected.	Alert	Major	Every	Yes

Note Names containing spaces must be delimited by quotes, for example: “Microburst Detected”

The following table lists the supported system faults along with their default syslog and SNMP severities and frequencies:

Table 8-8: System Faults

Fault	Description	Syslog Severity	SNMP Severity	Frequency	Clear
System shutdown	BQM has shutdown.	Informational	Informational	Every	No
System startup	BQM has started up.	Informational	Informational	Every	No
CPU Failure	Problem with a system CPU	Alert	Major	Hourly	Yes
FanFailure	Fan failure detected.	Critical	Major	Daily	Yes
HardDiskThresholdViolation	Hard disk threshold violation detected.	Emergency	Severe	Hourly	Yes
HardDriveFailure	Hard drive failure detected.	Emergency	Severe	Daily	Yes
PortDown	BQM physical interface down detected.	Alert	Major	Hourly	Yes
LicenseExpired	License expired detected.	Critical	Major	Daily	Yes
LicenseInvalid	License invalid detected.	Critical	Major	Daily	Yes
LicenseNearExpiration	License is near expiration.	Warning	Warning	Daily	Yes
MemoryUtilization	High Memory usage detected.	Critical	Major	Every	Yes
System Throughput	Average buffer utilization over 80% for a period of time.	Alert	Major	Every	Yes
Temperature	System temperature is too high.	Emergency	Severe	Hourly	Yes
PowerSupplyFailure	Power supply failure detected.	Critical	Major	Daily	Yes
SoftDiskThresholdViolation	Soft disk threshold violation detected.	Warning	Warning	Daily	Yes
WatchdogRestart	Watchdog has restarted.	Notification	Warning	Every	No

You can configure different settings for any given fault using the appropriate commands. For more information, see the section “Configuring Alert Settings.”

The BQM default configuration. Use the **show snmp-server** command to view the initial configuration:

```
host(config)$ show snmp-server
no snmp-server enable traps email
no snmp-server enable traps syslog
no snmp-server enable traps
no snmp-server fault "E2E Delay Threshold Exceeded" report-email
no snmp-server fault "E2E Loss Detected" report-email
no snmp-server fault "E2E Availability Issue" report-email
no snmp-server fault "Congestion Threshold Exceeded" report-email
no snmp-server fault "Micro-Burst Detected" report-email
no snmp-server fault "Corvil Bandwidth Threshold Exceeded" report-email
no snmp-server fault "Expected Queuing Loss Threshold Exceeded" report-
email
no snmp-server fault "Expected Queuing Delay Threshold Exceeded" report-
email
no snmp-server fault "Expected Policing Threshold Exceeded" report-email

host(config)$
```

Use the **snmp-server enable traps** command to enable state change SNMP traps or notifications. To disable notification, use the **no** form of the command.

snmp-server enable traps [*notification-type*]

The available notification types are e-mail and syslog. If you enter the command with a particular notification keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option. In the following example, separate commands are issued to enable both email and syslog notification:

```
host(config)$ snmp-server enable traps email
host(config)$ snmp-server enable traps syslog
```

Note Standard system fault logging is disabled by default. If logging has been disabled on your system (using the **no snmp-server enable traps syslog** command), logging must be re-enabled using the command **snmp-server enable traps syslog**.

You can use the **show snmp-server** command to check your changes. Having enabled notification, you can use the following commands to set e-mail or syslog destinations:

snmp-server enable traps email {destination <*to-address*> | server <*hostname*|*ip address*> from <*from-address*>}

snmp-server enable traps syslog [destination <*hostname*|*ip address*> [port <*port*>]]

In the following example, e-mail notification is enabled to the specified e-mail destination address:

```
host(config)$ snmp-server enable traps email destination reporter@acme.com
host(config)$
```

The following example shows how to send all traps to the syslog host 192.168.10.1:

```
host(config)$ snmp-server enable traps syslog destination 192.168.10.1
```

Note We recommend that you use IP addresses when specifying destination servers. You can enter a hostname when using the **snmp-server** command to define a server destination, but you have to use the server IP address when using the **no snmp-server command** to remove a destination server.

If you configure e-mail notification, an e-mail is sent to the configured destination address when an alarm is raised, up to a limit of ten per hour. The following is an example of notification e-mail sent:

```
From: noreply@acme.com
Sent: Thursday, September 28, 2006 11:00 AM
To: reporter@acme.com
Subject: Email Alert - Micro-Burst Detected. Severity 'Major'. Source 'rt-
class/Walkinstown/default/Walkinstown.i/peer-output/class-default'.
WARNING: Last email this hour.


Email Alert - Micro-Burst Detected

  severity[Major]

source[rt-class/Walkinstown/default/Walkinstown.i/peer-output/class-
default]
  description[Micro-Bursts exceeding the configured bandwidth threshold
have been detected.]
  details[400ms]
  reason[EventSet]
  time[2006/09/28 10:00:03.0 UTC]
  count[13]
  value[199.0]

WARNING: No more email alerts will be sent this hour,
         the hourly limit of 10 email alerts per hour has been reached.
         Please go to the Alarms tab in the GUI to see all alerts.
```

This is an example of the final e-mail to be sent in a given hour. The message indicates that you may now need to go to the GUI to see all active alarms.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host(s) receive notifications. To send notifications, you must configure at least one **snmp-server host** command.

snmp-server host <*hostname*|*ip address*> [traps] <*community-string*>
[udp-port *port*]

The following example shows how to send all traps to the host with IP address 192.168.11.2, using the community string `public`:

```
host(config)$ snmp-server enable traps
host(config)$ snmp-server host 192.168.11.2 public
```

Note We recommend that you use IP addresses when specifying destination servers. You can enter a hostname when using the **snmp-server** command to define a server destination, but you have to use the server IP address when using the **no snmp-server command** to remove a destination server.

Configuring Alarm Severity and Frequency Settings

You can use the BQM CLI to configure severity and frequency settings for both quality and system alarms.

snmp-server fault <*name*> [traps *traps-severity*] [report-traps]
[syslog *syslog-severity*] [report-syslog]
[report-email] [freq <*frequency*>]

The following example shows how to configure the SNMP and syslog severity levels and frequency for the fault named Microburst Detected:

```
host(config)$ snmp-server fault “Microburst Detected” traps major syslog
alert freq every
```

Note Remember to use the CLI tab completion feature when entering these commands.

In this case the fault name contains a space, so it must be delimited by quotes.

The following example shows how to configure the SNMP and syslog severity levels and frequency for the fault named FanFailure:

```
host(config)$ snmp-server fault FanFailure traps major syslog alert freq
every
```

Checking Fault Configuration Status

As you use the snmp-server fault command to configure the various faults, you can use the **show-faults** command to check your configuration. The output of show faults is a list of all available fault types and each fault's current SNMP, syslog and e-mail configuration status:

```
host(config)$ show faults-info
Name                  Snmp Enabled      Syslog Enabled    Email Enabled
Default fault type    True              True              False
System Startup        True              True              True
Fan Failure           True              True              True
Fan Failure Clear     True              True              True
Power Supply Failure  True              True              True
--More--
```

If you enter a string it will show all faults matching that string

```
host(config)$ show faults-info CPU
Name                  Snmp Enabled      Syslog Enabled    Email Enabled
CPU Utilization High  True              True              True
CPU Utilization Clear True              True              True
CPU Failure           True              True              True
CPU Failure Clear     True              True              True
host(config)$
```

For more information on the full syntax and parameters of the **snmp-server** commands, see the "Command Reference" chapter.

9 CLI Command Reference

This chapter provides information on each of the CLI commands available on the BQM.

Configuration Mode

The following table lists the commands available in global configuration mode when you log in to the device initially. Typically commands that are available in any one mode are also available in the mode's children, so the commands listed here are also available in all other modes.

Command	Description
?	Shows all possible completions of a character string in the current configuration mode. Use this command to list the available commands at any given time.
allow	Specifies certain IP addresses or subnets to access the BQM and restrict all others. Only available if you are logged in as an admin user.
backup	Creates a system configuration backup (with or without capture files) on a target disk or host. Only available if you are logged in as an admin user
capture-settings	Configures global packet capture parameters: disk space quota and capture file password
clear	Clears all configuration changes from memory, or clears counters for interface statistics.
clock	Configures the system clock.
copy	Copies a file from a source to a destination.
dir	Lists the files and directories on the file system.
domain	Configures a DNS name server for domain name resolution.
end	Returns to global configuration mode.
help	Lists valid commands that can be run from the current directory.
license	Displays the BQM license agreement. Only available if you are logged in as an admin user

log	Displays the end of the system log file.
logging	Switches on logging of the system log messages to a remote syslog server.
logout	Logs you out of the system.
no	Deletes an object or entry. An object that is being used by another object cannot be deleted.
ntp	Configures Network Time Protocol services. Only available if you are logged in as an admin user
password	Sets your login password.
ping	Uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.
port	Specifies the Ethernet operation of the selected BQM port (mgmt, PortA, PortB, PortC, PortD). You configure the operation to be auto negotiated, or you force either half-duplex or full duplex operation at 10 Mbps, 100 Mbps, or 1 Gbps.
reload	Reboots the appliance. Only available if you are logged in as an admin user.
rename	Allows renaming of class-maps, policy-maps, interfaces, local-site, routers, sites, custom-applications and monitor-queuing-maps.
restore	Restores the system configuration (with or without capture files) from a target disk or host. Only available if you are logged in as an admin user.
service	Allows network services on the device to be enabled/disabled.
setup	Sets basic appliance configuration details. Only available if you are logged in as an admin user.
show	Lists the contents of each available configuration mode. It is a recursive listing by default. Also used to display the current running and startup configurations.
shutdown	Shuts down this device. Only available if you are logged in as an admin user.
snmp-server	Specifies the SNMP community strings (passwords) for SNMP set and g commands to restrict SNMP access to the BQM. Supports configuration of BQM fault notification.
status	Reports the current status of the BQM.
terminal	Sets the number of lines of output displayed in the terminal window.
traceroute	Traces the route to a destination address on networks.

You can perform basic BQM configuration by creating class-maps, policy-maps, and interfaces in this mode.

Valid identifiers for configuration objects (class-maps, policy-maps, interfaces) are as follows: US ASCII characters from 32 – 126, with certain defined exceptions (see below). The full list of supported characters is as follows:

32 Space
33 !
35 #

36 $
37 %
38 &
40 (
41)
42 *
43 +
44 ,
45 -
46 .
47 /
48 0
49 1
50 2
51 3
52 4
53 5
54 6
55 7
56 8
57 9
58 :
59 ;
60 <
61 =
62 >
64 @
65 A
66 B
67 C
68 D
69 E
70 F
71 G
72 H
73 I
74 J
75 K
76 L
77 M
78 N
79 O
80 P
81 Q
82 R
83 S
84 T
85 U
86 V
87 W
88 X
89 Y
90 Z
91 [
93]

94 ^
95 _
96 `
97 a
98 b
99 c
100 d
101 e
102 f
103 g
104 h
105 i
106 j
107 k
108 l
109 m
110 n
111 o
112 p
113 q
114 r
115 s
116 t
117 u
118 v
119 w
120 x
121 y
122 z
123 {
124 |
125 }
126 ~

The following characters from the list above are excluded from being used in object names:

34 "
39 '
63 ? (Primarily used as a completion character in the CLI. You can enter Ctrl-V ?, for example to add a question mark to an object description.)
92 \

The following are also unsupported configuration object names on the BQM:

Names with leading and trailing spaces
Names with no characters (empty string)
Name comprising the minus sign on its own (-)
Names comprising a single period on its own (.)
Names comprising two periods on their own (..)

In addition to the above system administration commands, the following lists the configuration commands available in configuration mode:

Command	Description
class-map	Creates a class-map. This will automatically move you into class-map configuration mode.
custom-application	Configures a custom application.
local-site	Configures a representation of the local site.
monitor-end2-end-map	Creates a monitor end2end map. This will automatically move you into monitor end2end map configuration mode.
monitor-queuing-map	Creates a monitor-queuing-map. This will automatically move you into monitor-queuing-map configuration mode.
policy-map	Creates a policy-map. This will automatically move you into Policy-map Configuration mode.
site	Creates a representation of a remote site, defined at a minimum by specifying network subnets. Interfaces are then defined under sites.

The following lists the packet capture and file system commands available in configuration mode:

Command	Description
capture	Creates a packet capture instance. This will automatically move you into capture configuration mode.
delete	Deletes packet capture files from the file system.
dir	Lists the packet capture files on the file system.
more	Lists the contents of a file.
start capture	Starts packet capture for a named instance or for all configured packet capture instances if no name is specified. Use the global **no start capture** command to stop packet capture for a named instance or all packet captures if no name is specified.

Class-map Configuration Mode

You use Class-map configuration mode to enter match rules for class-maps. The following lists the commands available when working with specific instances of class-maps.

Command	Description
`description`	Adds a text description to a class-map.
`match`	Adds a match rule to a class-map The **match** command is the most important in the BQM command set, because it identifies the set of IP packets that are used to classify traffic. The match-rule is flexible and enables traffic matching that represents any realistic IP classification.

Policy-map Configuration Mode

You use Policy-map configuration mode to create a class entry in a policy-map for each previously configured class-map. The following lists the commands available when working with specific instances of policy-maps:

Command	Description
`class`	Creates a policy-map entry that matches a previously configured class-map.
`description`	Adds a text description to a policy-map.
`down`	Moves a class down in the list of policy-map classes.
`monitor-queuing`	Creates a policy-map entry that matches a previously configured monitor-queuing-map.
`trace-events`	Enables rolling event detection packet capture for a policy-map.
`up`	Moves a class up in the list of policy-map classes.

Policy-map Class Configuration Mode

When you create a class entry in a policy-map using the **class** command, you are brought directly into this mode. Using this mode, you can

- Configure class entries for previously configured class-maps

Command	Description
`bandwidth`	Specifies or modifies bandwidth allocated for a policy-map class.
`monitor-queuing`	Creates a class entry that matches a previously configured monitor-queuing-map.
`priority`	Specifies guaranteed allowed bandwidth for the class.
`priority-level`	Specifies the strict priority level of a class in a policy-map:

	high, medium, normal, or low.
`queue-limit`	Specifies the maximum number of packets that a queue for a class can accumulate before dropping packets during periods of congestion.

Monitor End2End Map Configuration Mode

When you create a monitor-queuing-map using the **monitor-end2end-map** command, you are brought directly into this mode.

Command	Description
`description`	Adds a text description for a monitor-end2end-map.
`measure-ping`	Enables monitoring of end-to-end connections between the local site and remote sites.

Monitor-Queuing-Map Configuration Mode

When you create a monitor-queuing-map using the **monitor-queuing-map** command, you are brought directly into this mode.

Command	Description
`description`	Adds a text description for a monitor-queuing-map.
`estimate-service-level`	Enables Congestion Indicator calculations and estimation of the achieved loss or delay for a class or interface. The optional keywords enable detection of events using the configured queuing-target as the thresholds.
`measure-bandwidth`	Enables Corvil Bandwidth measurement for bandwidth sizing and sets an optional threshold in kbps or as a percentage of the link rate for triggering an event if the calculated Corvil Bandwidth value exceeds the threshold.
`measure-microburst`	Enables millisecond-level peak rate measurement and sets an optional threshold in kbps or as a percentage of the link rate for triggering an event if the calculated millisecond peak rate value exceeds the threshold.
`queuing-targets`	Specifies the delay queuing targets for Corvil Bandwidth, expected service level and bandwidth sizing.

Local Site Configuration Mode

You use local site configuration mode to edit the properties of the default local site. The following lists the commands available when working with the default local site.

Command	Description
`description`	Adds a text description to the default local site.

ping-address	Specifies an always-available ICMP Responder host address on the local site subnet; utilized by end-to-end round trip measurements.
router	Creates a router for the default local site.
subnet	Edit the subnet address for the default local site.

Site Configuration Mode

You use site configuration mode to define the properties of remote sites. The following lists the commands available when working with specific instances of remote sites.

Command	Description
description	Adds a text description to a class-map.
end2end-target	Specifies end-to-end delay and loss targets for site round-trip measurements.
ping-address	Specifies an always-available ICMP Responder host address on the site subnet; utilized by end-to-end round trip measurements.
router	Creates a router for a given site.
subnet	Specifies a subnet for a given site.

Site Router Configuration Mode

You use site router configuration mode to define the properties of site routers. The following lists the commands available when working with specific instances of routers.

Command	Description
`attached-port`	Specifies which physical ports (PortA, PortB, PortC, PortD) to use for traffic measurement for a local site only.
`description`	Adds a text description to a router.
`interface`	Creates a model interface for a router. An interface is used to measure traffic outbound from the perspective of a given site.
`peer-interface`	Specifies a model peer interface for a router when configuring MPLS VPN, Internet VPN, Private VPN deployments. to measure traffic output from a local site to a remote site (that is, the inbound traffic to a remote site, but from the local site's outbound perspective. This is because Cisco routers queue traffic on an outbound basis).

Interface Configuration Mode

You use Interface configuration mode to enter interface configuration details when configuring sites. The following lists the commands available when working with specific instances of model interfaces.

There are predefined BQM interfaces: PortA, PortB, PortC, and PortD. These interfaces cannot be renamed or deleted.

Command	Description
`bandwidth`	Specifies a bandwidth allocation for the interface.
`connects-to`	Specifies the local site interface to which the chosen remote site interface is connected in a point-to-point deployment.
`description`	Adds a text description to an interface.
`filter-class`	Specifies a class-map on which to base interface traffic filtering.
`link-adjust`	Specifies a packet size adjustment value for an interface.
`max-reserved-bandwidth`	Specifies the maximum reserved bandwidth value for an interface.
`ppp`	Specifies that link fragmentation and interleaving is enabled for an interface.
`service-policy`	Adds an input service-policy for the output direction of an interface.
`subnet-filtering`	Specifies that interface packet filtering is based on the associated site subnet(s).

Peer-interface Configuration Mode

You use Peer-interface configuration mode to enter peer interface configuration details when configuring sites in MPLS VPN, Internet VPN, Private VPN deployments. The following lists the commands available when working with specific instances of model peer interfaces.

There are predefined BQM interfaces: PortA, PortB, PortC, and PortD. These interfaces cannot be renamed or deleted.

Command	Description
`bandwidth`	Specifies a bandwidth allocation for the peer interface.
`description`	Adds a text description to a peer interface.
`filter-class`	Specifies a class-map on which to base interface traffic filtering.
`link-adjust`	Specifies a packet size adjustment value for an interface.
`max-reserved-bandwidth`	Specifies the maximum reserved bandwidth value for an interface.
`ppp`	Specifies that link fragmentation and interleaving is enabled for an interface.
`service-policy`	Adds an input service-policy for the output direction of a peer interface.
`subnet-filtering`	Specifies that interface packet filtering is based on the associated site subnet(s).

Packet Capture Configuration Mode

You can use the global capture command to create a new packet capture instance. When you use the capture command, you are automatically moved into packet capture configuration mode, from which you configure the packet capture details. In addition to the above system administration commands, the following lists the configuration commands available in configuration mode:

Command	Description
`attach interface`	Attaches the relevant packet capture instance to a specific, named interface.
`duration`	Sets the maximum duration for the packet capture. When the configured time is reached, packet capture is stopped automatically.
`start`	Starts packet capture. Use the **no start** command to stop packet capture.
`size`	Sets the maximum file size for the packet capture. When the configured file size is reached, packet capture is stopped automatically.
`snaplength`	Sets the snapshot length for the packet capture instance.

Command Reference

?

Mode

All

Usage Guidelines

To show all possible completions of a character string in the current CLI mode, type the character or string and then the ? command. You do not need to press Enter, just type ? on its own or straight after the character(s). CLI modes are not listed by the ? command. If the ? is pressed without any initial string (no text to complete)t, the help menu is displayed.

[<*initial letter(s) of a partial command*>]**?**

Syntax Description

<*initial letter(s) of a partial command*>	Specify an initial string to complete using the ? command.

Example

In this example, from the root context, typing **?** on its own displays the following:

```
host(config)# ?

  allow                Restricts network access to the device.
  backup               Backup configuration and database, [capture files] to a target
destination.
  capture              Configures a packet capture instance
  capture-settings     Configures global packet capture parameters
  class-map            Configure a class-map
  clear                Reset functions
  clock                Configure time-of-day clock.
  copy                 Copy from a source to a destination
  custom-application   Configure a custom-application
  delete               Delete files from a filesystem
  dir                  List files on a filesystem
  domain               Configures DNS Name Servers.
  end                  Return to base context
  exit                 Exit configuration mode or EXEC
  help                 List commands that can be run
  license              Install and/or displays the license file
  local-site           Configure the local site
  log                  Display the end of the local system log file.
  logging              Configures parameters of the remote logging system.
  logout               Logs out a user
```

```
  monitor-end2end-map  Configure a monitor-end2end-map
  monitor-queuing-map  Configure a monitor-queuing-map
  more                 List contents of file
  no                   Reverses next command, such as creation of a class-map.
  ntp                  Configure Network Time Protocol Services.
  password             Sets login password or passowrd used to protect capture files
  ping                 Sends ICMP ECHO_REQUEST to network hosts
  policy-map           Configure a policy-map
-- More --host(config)#
```

In this example, from the root context, typing c? displays the following:

```
host(config)# c?
  capture             Configures a packet capture instance
  capture-settings    Configures global packet capture parameters
  class-map           Configure a class-map
  clear               Reset functions
  clock               Configure time-of-day clock.
  copy                Copy from a source to a destination
  custom-application  Configure a custom-application
```

allow

Mode

Configuration
`host(config)$`

Usage Guidelines

To allow only certain IP addresses to access the BQM and restrict all others, use the **allow** command. You must be logged in as an admin user to use this command. To remove allowed IP addresses, use the **no allow** command. To remove all allowed IP addresses, use the **no allow *** command. The system issues a warning if you try to allow a certain IP address, on a previously unrestricted machine, that is different from the appliance IP address you are currently using to access the BQM.

The appliance IP address you are currently using to access the BQM might be different from the machine from which you are logged in to the BQM. This is usual in the case where you are logged in via a proxy machine.

allow <*IP address*>**[**/<*prefix*>**]**
no allow <*IP address*>**[**/<*prefix*>**]**

Syntax Description

<*IP address*>	Specify the IP address of the appliance permitted to connect to the BQM.
<*prefix*>	Specify a prefix value to identify a subnet.

Examples

In this example, an appliance with IP address 192.168.128.5 is being used to telnet to the BQM. The **allow** command is used to allow appliances with IP addresses 192.168.128.5, 192.168.128.6, and subnet 192.168.129.0:

```
host(config)$ allow 192.168.128.5
host(config)$ allow 192.168.128.6
host(config)$ allow 192.168.129.0/24
```

In this example, you begin with an unrestricted appliance. You telnet in from the IP address 192.168.128.1 and you try to allow 192.168.128.200. Doing this alone would prevent your computer from subsequently accessing the BQM:

```
host(config)$ allow 192.168.128.200
Warning: you are accessing the appliance via the IP address ‘192.168.128.1’.
‘allow 192.168.128.200’ will prevent you accessing the appliance. Continue (y/n)? n
host(config)$
```

attach

Mode

Configuration
`host(config-capture)`

Usage Guidelines

To add an interface to the selected packet capture instance, use the **attach** command. If the interface has been already assigned to a different instance the previous assignment will be removed. Only one interface or peer interface may be assigned to a given capture instance. So if you want to capture traffic for both an interface and peer-interface, then both require separate use of the **attach** command. To remove an interface from the selected capture instance, you use the no form of the command. If no interface is specified all interfaces are removed. An error is displayed if these commands are run while the capture is active.

attach {<interface> | <peer-interface>}{<*site name*><*router name*><*interface name*>}
no attach {<interface> | <peer-interface>}{<*site name*><*router name*><*interface name*>}

Syntax Description

site name	Specify the name of the site in which the interface is configured.
router name	Specify the name of the router for which the interface is configured.
interface-name	Specify the name of the interface to which to attach the packet capture.

Example

In this example, the packet capture instance named AllSerial1 is defined, attached to a site router interface, where the site is named nyc_dc, the router is named core1, and the interface is named serial1, and the capture instance has a file size and time limit applied:

```
host(config)# capture AllSerial1
host(config-capture)# attach interface nyc_dc core1 serial1
host(config-capture)# size 10000
host(config-capture)# duration 60
```

attached-ports

Mode

Configuration
`host(config-site-router)`

Usage Guidelines

To specify which physical ports to use to measure traffic in both directions for a local site, use the **attached-port** command. If attached-port is not used with a local site, then all measurement ports are assumed to be used.

attached-port <*port* > [<*port* > …]
no attached-port [<*port* > …]

Syntax Description

port	Specifies the name of the measurement port: Port A, PortB, PortC, PortD.
inbound	Specifies inbound traffic to the local site.
outbound	Specifies outbound traffic to the local site.

Example

In this example, default local site is edited to configure traffic measurement from physical ports PortA and PortB:

```
host(config)#local-site "BQM site"
host(config-local-site)# attached-ports PortA PortB
```

backup

Mode

Configuration
`host(config)`

Usage Guidelines

To back up the BQM configuration and database to a specified target destination, use the **backup** command. You can also choose to back up capture files. The target for the backup may be an accessible filesystem , an ftp server or a host accessible via ssh or scp. If the backup is via ftp or scp, you are prompted for a username and password.

If you are using the ftp or scp options you must be sure that you have the relevant permissions to create the new backup directory and copy the backup files to it. For example, if you do the following:

backup data scp://192.168.2.3/backup_dir admin adminuS3r

you may find that the operation fails because you do not have permission to create the new backup_dir directory.

In the case of FTP or SCP backups, the host name (resolvable via DHCP) or host IP address must be given.

For information on how to restore previously backed up files, see the **restore** command.

backup {**status** | [**data**] | [**data-with-captures**]} {backup: *directory* |
[ftp://[*hostname* | *IP address*]/*path*] [*user*] [*password*]] |
[scp://[*hostname* | *IP address*]/*path*}[*user*] [*password*]]}

Syntax Description

status	Displays the status of the backup.
backup:*directory*	Selects backup to an accessible file system.
ftp://*hostname/path*	Selects backup to an FTP server. You need the appropriate permissions to write the new directory and files to the target path.
scp://*hostname/path*	Selects backup to a remote machine via ssh or scp. You need the appropriate permissions to write the new directory and files to the target path.
user	Specifies the login username (ftp and scp.)
password	Specifies the login password (ftp and scp).

Example

In this example, the BQM configuration is backed up (without capture files) to a server with IP address 192.168.7.2 using scp:

```
host(config)#backup data scp://192.168.7.2/home/mydir/cfg_bck_090606 admin adminP4sswd
host(config)#
```

In the following example, the BQM configuration is backed up locally (without capture files) to a directory named 12-15-2006. The dir command is used to illustrate the directory structure created by the backup operation:

```
host(config)$ backup data backup:12-15-2006
Backup task successfully launched in background
host(config)$ dir backup:
backup:/
        Size  Name
        4096  12-15-2006/
host(config)$ dir backup:/12-15-2006
backup:12-15-2006/
        Size  Name
        4096  config/
        4096  database/
host(config)$ dir backup:/12-15-2006/config
backup:12-15-2006/config/
        Size  Name
        4096  section000001/
host(config)$ dir backup:/12-15-2006/config/section000001
backup:12-15-2006/config/section000001/
        Size  Name
       10805  file000001
host(config)$ dir backup:/12-15-2006/database
backup:12-15-2006/database/
        Size  Name
       37124  file000001
host(config)$
```

bandwidth

Mode

Policy-map Class configuration
`host(config-cmap)#`

Usage Guidelines

To specify or modify the bandwidth allocated for a class belonging to a policy-map, use the bandwidth command in policy-map class configuration mode. The **bandwidth** command specifies the bandwidth for traffic in that class. The Weighted fair queuing (WFQ) scheduling system derives the weight for packets belonging to the class from the bandwidth allocated to the class. The WFQ scheduler then uses the weight to ensure that the queue for the class is serviced fairly. To remove the bandwidth specified for a class, use the no form of this command.

You can specify bandwidth in kbps, or as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages.

The following restrictions apply when working with the **bandwidth** command:

- A given policy-map can have all the class bandwidths specified in the same format, that is they must all be kbps, percent, or remaining percent, but not a mix of different formats.
- The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.
- When the policy-map containing class configurations is attached to an interface to define the service policy for that interface, available bandwidth is assessed. If there is insufficient interface bandwidth, and the policy-map cannot be attached to a particular interface, then the policy is removed from all interfaces to which it was successfully attached.
- The bandwidth command uses a default queue limit for the chosen class. You can modify the default queue limit value using the queue-limit command.
- If an outer policy-map class contains the bandwidth remaining percent command, then there must be available bandwidth on the associated interface, that is, you cannot have 0% available on the link for use by the command.
- A regular policy-map class containing a priority command cannot contain a bandwidth command.

bandwidth {*bandwidth-kbps* | remaining percent *percentage* | percent *percentage*}
no bandwidth {*bandwidth-kbps* | remaining percent *percentage* | percent *percentage*}

Syntax Description

bandwidth-kbps	Specifies the amount of bandwidth, in kilobits per second (kbps), to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use. If the link bandwidth is unknown or variable, class bandwidth settings in kbps should not be used. Range: 8 – 2000000 kbps
remaining percent *percentage*	Specifies the amount of guaranteed bandwidth for the class, based on a relative percentage of available bandwidth. You use the bandwidth remaining percent command in cases where the link bandwidth is unknown or variable or to specify the available bandwidth remaining after use of a priority class. In this case, the class bandwidths are always proportional to the specified percentages of the interface bandwidth. If the link bandwidth is

	fixed, class bandwidth guarantees are in proportion to the configured percentages. Range: 1 to 100%
percent *percentage*	Specifies the amount of guaranteed bandwidth set aside for a bandwidth class, based on an absolute percentage of available bandwidth. Range: 1 to 100%.

Example

In this example, having previously created a class-map called class_map1, a policy-map entry for class_map1 is created along with the bandwidth assignment of 1500 kbps:

```
policy-map policy1
 description "This is policy1"
  class class_map1
  bandwidth 1500
```

In this example, having previously created a class-map called class_map2, a policy-map entry for class_map2 is created along with the assignment of 25% of the available bandwidth:

```
policy-map policy2
 description "This is policy2"
  class class_map2
  bandwidth percent 25
```

To specify or modify the bandwidth of a model interface, use the **bandwidth** command in interface configuration mode. To remove a bandwidth value, use the **no bandwidth** command. A default interface bandwidth value is applied to each interface you create.

bandwidth {*bandwidth-kbps*}
no bandwidth {*bandwidth-kbps*}

Syntax Description

bandwidth-kbps	Specifies the bandwidth of the model interface, in kilobits per second (kbps). Range: 1 – 10000000 kbps

Example

In this example, an interface called Serial1_0 is created with a capacity of 2000 kbps:

```
interface Serial1_0
bandwidth 2000
```

capture

Mode

Configuration
`host(config)#`

Usage Guidelines

To create a packet capture instance, use the **capture** command. Using the **capture** command automatically moves you into capture configuration mode. To delete a packet capture instance, use the no form of this command. Even if the packet capture instance is currently operating, the packet capture is stopped and the capture instance deleted.

capture <*name*>
no capture <*name*>

Syntax Description

name	Specify the name of the packet capture instance.

Example

In this example, packet capture instance called serial1 is created, attached to a site router interface and has a file size and time limit applied:

```
host(config)# capture serial1
host(config-capture)# attach interface nyc_dc core1 serial1
host(config-capture)# size 10000
host(config-capture)# duration 60
```

capture-settings

Mode

All configuration modes

Usage Guidelines

The BQM employs a separate hard disk for storing packet capture files. Packet capture files generated automatically by BQM event analysis in response to event triggers and those generated by manual packet capture share the same disk. This command allows for the percentage of the disk allocated to capture files generated by event analysis to be adjusted between one and 100 percent. Normally the disk is split equally between event analysis and manual capture files, that is, the default value for disk allocation for event analysis capture files is 50%. The remaining disk space is used by manual capture files. Management of these files is performed automatically. You must be logged in to the BQM CLI as an admin user to use this command.

.

capture-settings event-trace-quota percent <1-100 | **default**>

Syntax Description

percent <1 – 100>	Specifies an event capture disk quota between one and 100 percent.
percent default	Specifies the default event capture disk quota, namely 50 percent.

Examples

In the following example, the percentage of disk space allocated to packet capture files generated automatically by BQM event analysis is 70 percent:

```
host(config)$ capture-settings event-trace-quota percent 70
host(config)$
```

capture-settings password

Usage Guidelines

Change or disable password used to encrypt manual capture files. Valid passwords comprise a mixture of between five and eight upper and lowercase, alphanumeric and non alphanumeric characters. Specifies or resets a password for use with the **copy capture** command, when copying packet capture files to a remote server.

Example

Use the following to change the config user password:

```
host(config)# capture-settings password
Changing capture password
new password:
Re-enter new password:
Password changed
host(config)#
```

class

Mode

Policy-map Class configuration
`host(config-pmap)#`

Usage Guidelines

To create a policy-map entry for a class that matches a previously configured class-map, use the **class** command. To remove a policy-map entry for a class, use the no form of this command.

The policy-map class class-default is determined to be a special case where the following rules override previously defined semantic rules:

- The class-default class is deemed to be a queue-generating class even though it does not contain a **priority-level**, **priority** or **bandwidth** command. This is because it can generate a FIFO queue.
-
- The **bandwidth** command is not allowed in a class-default class.
- The **priority** command is not allowed in a class-default class.
- The class-default class is assumed to have a default **priority-level** of 'normal', unless specified differently by using a **priority-level** command, if the policy-map is using strict priority-levels.
- The **queue-limit** command is only allowed with the **bandwidth** and **priority-level** commands.

class {*class-map name* | class-default}
no class {*class-map name* | class-default}

Syntax Description

class-map name	Specify the name of the previously configured class-map (case-sensitive) to be referenced in the policy-map.
class-default	Specify the default class in order to configure or modify it. The class ‘class-default’ is always created automatically, even if not specified in the configuration. If specified in the configuration it is possible to override certain parameters. This ‘automatic’ modeling of the default class is implemented as a weighted queue with weight zero or a strict priority-level 'normal'.

Example

In this example, having created a class-map called class_map1 and a policy-map called pmap_1, a policy-map entry for class_map1 is created:

```
class-map class_map1
 description "This is class_map1"
 match any
```

```
policy-map p_map1
 description "This is policy_map1"
  class class_map1
```

class-adjust

Mode

Policy-map class configuration
`host(config-pmap-c)#`

Usage Guidelines

To specify how much (in bytes) to adjust the size of a packet that matches the current class, use the **class-adjust** command. The command is primarily used to correctly measure compressed RTP. This traffic is seen by the device as uncompressed but it subsequently gets compressed inside the router before being queued on an output interface. To remove an adjustment value, use the **no** form of this command.

This allows for increased accuracy when calculating class measurements.

class-adjust {<-2000 - 2000>|<*adjust identifier*> [<*modifier*>]}
no class-adjust {<-2000 - 2000>|<*adjust identifier*> [<*modifier*>]}

Syntax Description

adjust identifier	Specifies an identifier to use. Currently the only identifier supported is cRTP, which maps to a class-adjust value of -36.
modifier	The cRTP identifier can have two modifiers: udp-checksum - the default, corresponds to a value of -36. or no-udp-checksum - corresponds to a value of -38.

Example

In this example an integer value is specified directly:

```
policy-map FIFO
  class class-default
    class-adjust 10
```

In this example an identifier is used:

```
policy-map FIFO
  class class-default
    class-adjust cRTP
```

In this example an identifier is specified with a modifier:

```
policy-map FIFO
  class class-default
```

```
      class-adjust cRTP no-udp-checksum
```

If you specify an identifier and/or modifier then the actual numeric value to which it corresponds is shown when you use the **show** command but not of course when you show the configuration:

```
host(config)# policy-map FIFO
host(config-pmap)# class class-default
host(config-pmap-c)# class-adjust cRTP no-udp-checksum
host(config-pmap-c)# show
  class-adjust cRTP no-udp-checksum (-38)
host(config-pmap-c)# show config policy-map FIFO
  class class-default
    class-adjust cRTP no-udp-checksum
```

class-map

Mode

Configuration
`host(config)#`

Usage Guidelines

To create a class-map, use the **class-map** command. This automatically moves you into class-map configuration mode.

A class-map defines an ordered list of matching rules that is hierarchical in nature. A class-map creates one or more rows in a conceptual table, where

- A packet may match all rows in the table (match all – logical AND operator)
- A packet must match at least one row in the table (match-any – logical OR operator) – this is the default

Each row has one or more expressions and for a valid match, a packet must conform to all expressions in that row. You can also embed class-maps within class-maps. To delete an existing class-map, use the no form of this command. To delete all class-maps, use the **no class-map *** command.

class-map [match-any|match-all] <*class-map name*>
no class-map [match-any|match-all] <*class-map name*>

Syntax Description

match-any	Requires that only one of the rules in the class-map needs to be matched. This is the default.
match-all	Requires that all rules in the class-map be checked against the packet.
class-map name	Specify a unique name (case-sensitive) for the new class-map. The name can be a maximum of 255 alphanumeric characters.

Examples

To create a new class-map, where only one of the defined class-map match rules needs to be matched, use the following:

```
class-map match-any class_map1
```

In the case where all the class-map match rules must be matched, use the following:

```
class-map match-all class_map2
```

clear

Mode

Configuration
`host(config)#`

Usage Guidelines

To clear all configuration object changes from memory, or to clear statistics or counters for specified interfaces, use the **clear** command. When you use the **clear** command you are prompted to confirm your choice. You then type 'y' to continue with deleting the entire BQM configuration, or you type 'n' to cancel the operation.

clear <config | counters [<*interface-name*>][*]]

Syntax Description

config	Use the keyword **config** to clear all defined objects in the configuration context, except for the fixed interfaces (PortA, PortB, PortC, PortD).
counters <*interface-name*>	Use the keyword **counters** to clear counters for the specified interface or peer interface. Use the wildcard symbol (*) to clear counters for all configured interfaces.

Examples

From the global configuration context, use the following to clear the BQM configuration:

```
host(config)# clear config
Are you sure you want to clear the current configuration (y/n)? y
host(config)#
```

From the global configuration context, use the following to clear counters for the specified BQM interface:

```
host(config)# clear counters Serial0/1
Are you sure you want to clear the current configuration (y/n)? y
host(config)#
```

clock

Mode

Configuration
`host(config)#`

Usage Guidelines

To manually set the system software clock, use one of the following formats of the **clock set** command. Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP), you need not set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the timezone specified by the configuration of the **clock timezon**e command.

Setting the clock results in the BQM being rebooted to ensure consistency.

clock set *hh***:***mm***:***ss day month year*
no clock set *hh***:***mm***:***ss day month year*

Syntax Description

*hh***:***mm***:***ss*	Specify the current time in hours (24-hour format), minutes, and seconds.
day	Specify the current day (by number) in the month.
month	Specify the current month (by full name).
year	Specify the current year (four digits, no abbreviation).

Example

The following example manually sets the software clock to 7:29 p.m. on May 13, 2003:

`host(config)# clock set 19:29:00 13 May 2003`

To set the time zone for display purposes, use the **clock timezone** command. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command. Cisco has a similar command which is more UNIX like, but to maintain consistency with the GUI, a JAVA style timezone is used.

clock timezone *zone*
no **clock timezone**

Syntax Description

zone	Name of the time zone, as per Java. The complete list of available Java time zone names is as follows:

	IDLW (GMT-12:00) IDLW (International Date Line West) Pacific/SST (GMT-11:00) Midway Island, Samoa US/Hawaii (GMT-10:00) Hawaii US/Alaska (GMT-08:00) Alaska US/Pacific (GMT-07:00) Pacific Time (US & Canada); Tijuana US/Arizona (GMT-07:00) Arizona US/Mountain (GMT-06:00) Mountain Time (US & Canada) America/Chihuahua (GMT-06:00) Chihuahua, Mazatlan Canada/Saskatchewan (GMT-06:00) Saskatchewan US/Central (GMT-05:00) Central Time (US & Canada) America/Mexico_City (GMT-05:00) Mexico City America/Central (GMT-05:00) Central America America/Bogota (GMT-05:00) Bogota, Lima, Quito US/EST (GMT-05:00) Eastern Standard Time America/Indiana (GMT-04:00) Indiana (East) US/EST_EDT (GMT-04:00) Eastern Time (US & Canada) America/CLT_CLST (GMT-04:00) Santiago America/VET (GMT-04:00) Caracas Canada/AST_ADT (GMT-03:00) Atlantic Time (Canada) America/ART (GMT-03:00) Buenos Aires Brasil/BRT_BRST (GMT-03:00) Brasilia Greenland (GMT-02:00) Greenland Atlantic/FNT (GMT-02:00) Mid-Atlantic Atlantic/CVT (GMT-01:00) Cape Verde Is. Atlantic/AZOT_AZOST (GMT+00:00) Azores UTC (GMT+00:00) Coordinated Universal Time GMT (GMT+00:00) Greenwich Mean Time Africa/WET (GMT+00:00) Casablanca, Monrovia Europe/UK (GMT+01:00) London, Edinburgh Europe/WET_WEST (GMT+01:00) Lisbon Europe/Ireland (GMT+01:00) Dublin Europe/CET_CEST_Ams (GMT+02:00) Amsterdam, Berlin, Bern, Rome, Stockholm... Europe/CET_CEST_Bel (GMT+02:00) Belgrade, Bratislava, Budapest, Ljubljan... Europe/CET_CEST_Bru (GMT+02:00) Brussels, Copenhagen, Madrid, Paris Europe/CET_CEST_Sar (GMT+02:00) Sarajevo, Skopje, Warsaw, Zagreb Africa/CET_CEST (GMT+02:00) West Central Africa Africa/CAT (GMT+02:00) Harare, Pretoria Europe/EET_EEST_Ath (GMT+03:00) Athens, Istanbul, Minsk Europe/EET_EEST_Buc (GMT+03:00) Bucharest Africa/EET_EEST (GMT+03:00) Cairo Europe/EET_EEST_Hel (GMT+03:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vi... Asia/Jerusalem (GMT+03:00) Jerusalem Asia/AST (GMT+03:00) Kuwait, Riyadh Africa/EAT (GMT+03:00) Nairobi Asia/AST_ADT (GMT+04:00) Baghdad Europe/MSK_MSD (GMT+04:00) Moscow, St. Petersburg, Volgograd Asia/GST (GMT+04:00) Muscat, Abu Dhabi Asia/AZT_AZST (GMT+05:00) Baku, Tbilisi, Yerevan Asia/PKT (GMT+05:00) Karachi, Islamabad, Tashkent Asia/YEKT_YEKST (GMT+06:00) Ekaterinburg Asia/BDT (GMT+06:00) Dhaka, Astana

	Asia/ALMT_ALMST (GMT+06:00) Almaty, Novosibirsk Asia/ICT (GMT+07:00) Bangkok, Hanoi, Jakarta Asia/KRAT_KRAST (GMT+08:00) Krasnoyarsk Asia/Hongkong (GMT+08:00) Hong Kong, Beijing, Chongqing, Urumqi Asia/SGT (GMT+08:00) Singapore, Kuala Lumpur Australia/Perth (GMT+08:00) Perth Asia/Taipei (GMT+08:00) Taipei Asia/IRKT_IRKST (GMT+09:00) Irkutsk, Ulaan Bataar Asia/JST (GMT+09:00) Tokyo, Osaka, Sapporo Asia/KST (GMT+09:00) Seoul Asia/YAKT_YAKST (GMT+10:00) Yakutsk Australia/Brisbane (GMT+10:00) Brisbane Australia/Canberra (GMT+10:00) Canberra, Melbourne, Sydney Pacific/ChST (GMT+10:00) Guam, Port Moresby Australia/Hobart (GMT+10:00) Hobart Asia/Vladivostok (GMT+11:00) Vladivostok Asia/MAGT_MAGST (GMT+12:00) Magadan, Solomon Is., New Caledonia Pacific/NZST_NZDT (GMT+12:00) Auckland, Wellington Pacific/FJT (GMT+12:00) Fiji, Kamchatka, Marshall Is. Pacific/Nukualofa (GMT+13:00) Nuku'alofa

Example

The following example sets the time zone to Eastern Standard Time in the U.S., which is 5 hours behind UTC:

```
clock timezone US/Eastern
```

Using the **clock** command without parameters displays the current time, abbreviated timezone and the timezone used information such that the resulting initial part of the output can be used as input to the **clock set** command. The time values input for the clock are automatically adjusted for the system time zone, such that the time active within the system is always in the appropriate UTC time values: For example:

```
clock
10:15:56  4 August 2006 EDT (US/Eastern)
clock set 10:15:56  4 August 2006
```

Also, the **show clock** command displays the abbreviated timezone and the timezone used when setting the timezone, for example:

```
show clock
10:15:56  4 August 2006 EDT  (US/Eastern)
```

connects-to

Mode

Router Interface Configuration
`host(config-site-router-if)#`

Usage Guidelines

When you are constructing the network model to reflect point-to-point deployments, you need to define the local site router interface to which each defined remote site interface is connected. To specify the local site interface to which a remote site interface is connected in a point-to-point deployment, use the **connects-to** command in the context of the chosen site interface. To remove an association between the chosen site interface and the data center interface, use the **no** form of this command.

connects-to *<local-site><router><interface>*
no connects-to *<local-site><router><interface>*

Syntax Description

local-site	Specify the name of the local site to which the chosen remote site interface is connected.
router	Specify the name of the local site router to which the chosen remote site interface is connected.
interface	Specify the name of the local site interface to which the chosen remote site interface is connected.

Example

In this example, the remote site interface Serial0/1 is connected to the local site core router interface Serial0/1:

```
host(config-site-router)# interface Serial0/1
host(config-site-router-if)# description “Link to Data Center”
host(config-site-router-if)# bandwidth 512
host(config-site-router-if)# service policy output low-speed
host(config-site-router-if)# connects-to DataCenter core1 Serial0/1
```

copy

Mode

Configuration
`host(config)#`

Usage Guidelines

To copy any file from a source to a destination, use the **copy** command. You must be logged in as an admin user to have all **copy** command options available. The fundamental function of the copy command is to allow you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file is specified using a URL. This allows you to specify any supported local or remote file location. The file system being used (such as a local memory source or a remote server) dictates the syntax used in the command.

The filename/pathname limit for the **copy** command when used to back up or restore files to/from a TFTP server is determined by the host operating system of the TFTP server. For example, in the case of RedHat 9 Linux, the limits are 255 characters for filenames and 4096 for pathnames.

Packet Capture Files
When you select a capture file to be copied, the file is converted internally to pcap format. It is then compressed to ZIP format and password protected using the capture password. If no capture password is present in the system, then the file copied will not be password protected. See the **capture-settings password** command for more information. You must be logged in as an admin user to copy capture files off the BQM.

Configuration Files
The BQM file system contains a time stamped copy of each BQM configuration file at user login or the last time the current active configuration was saved. The configurations due to login are automatically generated, current active configuration changes are saved using the following command:

```
copy config
```

You use the **dir cfg:** command to view the current list of configuration files. The file names include date/time stamping, and are located in the directory `/cfg`, for example `cfg:<file name>`, where the file name is constructed as follows:

```
bqm_yyyy-mm-dd-hhmmss-μsec.cfg
```

where:

yyyy	year represented by 4 digits, for example 2004.
mm	numerical value representing the month, for example July by 07.
dd	numerical value representing the day of the month, for example the 28th day by 28.
hh	numerical value for hour in 24 hour format, for example 1:00 pm by 13.
mm	numerical value for minutes, for example twenty minutes past the hour by 20.
ss	numerical value for seconds, for example thirty seconds by 30.
μsec	numerical value for microseconds, for example 41,234 microseconds by 41234.

Hence a configuration saved at 1:20pm, 30 seconds, and 41,234 microseconds on the 28th of July 2007 would be saved in a file as follows:

`cfg: bqm_2007-07-28-13-2030-41234.cfg`.

copy *source-URL destination-URL*

copy config [cfg:<*file-name*>]

copy cfg:<*file-name*> {config | tftp://[*hostname*|A.B.C.D]/<*file-name*>}

copy capture:<*file-name*>[tftp://[*hostname*|A.B.C.D]/<*file-name*>] | scp://*username@hostname*:*filename* | ftp://*username@hostname*:*filename*]
The **copy capture** command is only available to the admin user.

copy diagnostics tftp://<hostname | A.B.C.D>/[*filepath*]/*filename*
The **copy diagnostics** command is only available to the admin user.

copy {standby-system-image| system-image} tftp://[*hostname*|A.B.C.D]/<*file-name*>
This option of the **copy** command is only available to the admin user.

copy tftp://[*hostname*|A.B.C.D]/<*file-name*> {standby-system-image | config | arm}

Syntax Description

source-url	The location URL or alias of the copied file or directory. The destination can be local or remote, depending on whether the file is being downloaded or uploaded.
destination-url	Destination-URL or alias of the copied file or directory. The destination can be local or remote, depending on whether the file is being downloaded or uploaded.
config	Specifies the current configuration that is active in memory.
standby-system-image	Specifies the standby system image in the BQM image area.
system-image	Specifies the current operational system image in the BQM image area.
tftp://hostname |ip address/<*filename*>	Specifies the parameters used to save or retrieve configurations. The file is specified by [file path/]<file name>, relative to the directory determined for TFTP access at a TFTP server specified by the DNS hostname or ip address parameter. The current timeout value for inactivity is approximately 20 minutes.
ftp://*username@hostname:filename*	Specifies the DNS host name or IPv4 address of a target FTP server. The user account must be specified using the <username> parameter. The <filename> can be a relative or absolute path on the remote target server. A password prompt will appear once a connection with the server has been established.
scp://*user@hostname:filename*	Specifies the DNS host name or IPv4 address of a target SCP/SSH server. The user account must be specified using the <username> parameter. The <filename> can be a relative or absolute path on the remote target server. A password prompt will appear once a connection with the server has been established.

cfg:<*filename*>	Specifies a file from the BQM file system. The file is identified by [*file path*/]<*filename*>.
arm	Specifies that the file being copied by tftp to the BQM replaces the current Application Recognition Module (ARM) file.

Examples

To copy the current configuration to the file system:

```
copy config
```

To copy a specified configuration file from the TFTP directory on a TFTP server with the specified relative path to become the current BQM configuration.

```
copy tftp://hostname|A.B.C.D/[file path/]<filename> config
```

Note: that the new configuration becomes operational, that is, it becomes the configuration running in memory.

To copy the flat file used for initialization to a specified configuration file in the TFTP directory on a TFTP server with the specified relative path. The current running configuration in memory remains unaffected.

```
copy config tftp://hostname|A.B.C.D/[file path/]<filename>
```

To copy a specified system image file from the TFTP directory on a TFTP server with the specified relative path to the BQM image area. The current operational system image in memory remains unaffected, and the saved image file does not become effective until the `reload standby` command is executed.

```
copy tftp://hostname|A.B.C.D/[file path/]<filename> standby-system-image
```

To copy the current operational system image file used on the BQM to a specified configuration file in the TFTP directory on a TFTP server with the specified relative path. The current running configuration in memory and the startup configuration file remain unaffected.

```
copy system-image tftp://hostname|A.B.C.D/[<file path>/]<filename>
```

To copy capture files to a tftp server:

```
copy capture:serial1cap tftp://192.168.30.10/serial1cap
```

To update the Application Recognition Module (ARM) with a new version located on a tftp server:

```
copy tftp://hostname|A.B.C.D/[file path/]<filename> arm
```

custom-application

Mode

Configuration
`host(config)#`

Usage Guidelines

To define a custom application, you use the **custom-application** command. Using this command brings you directly into custom-application configuration mode, where you define match rules for the custom application and define precedence to specify which custom-application applies when a given network flow matches more than one set of rules. See the command reference information for the **match** and **precedence** commands for more information. To remove a custom application you use the **no** form of the command.

You can use all class-map match rules with the **custom-application** command except for ‘match class-map’. Note that a custom-application is similar to a class-map and supports both 'match-any' and 'match-all' syntax.

When a named custom application is created which corresponds to any traffic displayed, then following a refresh of any display containing that traffic, the named custom application will appear as appropriate for representing the traffic. Custom applications will be globally visible throughout the configuration of the system.

Named custom applications can be utilized within a class-map for use in classification. Note that a class-map and custom application may have the same name and any custom application must be defined prior to its use. The custom application name will be used to identify any traffic that corresponds to its own specific match rules.

The statistics for predefined applications, and applications discovered by the system (for example, *kazaa, eMule, fasttrack* and *eDonkey*), can be reported separately and can be reported in aggregate, or grouped, using a custom application definition. This includes Top N reporting. However, since a packet can only ever match one application, you must use class-maps, and not custom applications, to group applications together and not lose the granular application level information and statistics.

NOTE: See Appendix C for a full list of supported protocols.

custom-application <*name* >
no custom-application <*name*>

Syntax Description

name	Specify a unique name for the custom application. If there is a name clash with a predefined application name (see list above), then the user-defined custom application takes precedence.

Example

For example, you can create an application called "market-data" matching TCP port 1234, and it appears as:

```
custom-application market-data
 match tcp port=1234
```

In this example, a policy-map called "low-speed" is created containing a "market-data" class that matches the market-data application with 20% weight and has a "low-latency" monitor-queuing-map. In the CLI you see:

```
 class-map market-data
   match application market-data


 policy-map low-speed
   class market-data
     bandwidth percent 20
     monitor-queuing low-latency
```

In this example, the custom application named p-t-p is used to group peer-to-peer custom application traffic that has been previously identified by the system, in this case peer to peer traffic kazaa, eMule and eDonkey.

```
custom-application fasttrack
  match tcp port=1214


custom-application p-t-p
  match application kazaa
  match application eMule
  match application fasttrack
  match application eDonkey
```

delete

Mode

Configuration
`host(config)#`

Usage Guidelines

To delete files from the file system, use the **delete** command. You must be logged in as an admin user to be able to use all the **delete** command options. You can delete files from the `capture:`, `log:`, `cfg:`, `license:`, or `arm:` directories of the file system. Directory deletion is not supported in this release. All files deleted should be confirmed individually before deletion. Alternatively, you can use the */force* option to delete files without prompting for confirmation.

When performing packet capture, you use this command to remove packet capture files from the BQM after you have successfully copied them to a separate machine for further processing. It is not possible to delete a file belonging to an active packet capture.

Deleting the license file will leave the machine in an unlicensed state. Deleting the Application Recognition Module (ARM) file will remove the ability of the system to automatically discover application traffic.

delete [/force**] {capture: | log: | cfg: | license: | arm:}**< *file-url*>

If you are logged in as the config user you can only delete files from the capture: and cfg: file systems.

Syntax Description

<*file-url*>	Specifies the name of the file to delete. Can contain a wild card (*) or question mark (?) to match more than one file.

Example

In this example, packet capture files are deleted from the `capture:` file system:

```
host (config)# delete capture:*
Delete filename [serial1cap.pcap] (y/n) ? y
Delete filename [serial1cap.info] (y/n) ? y
host(config)#
```

In this example, packet capture files are deleted but individual confirmation is suppressed using the */force* option:

```
host(config)# delete /force capture:*
host(config)#
```

description

Mode

Class-map configuration
`host(config-cmap)`
Custom application configuration
`host(config-custom-app)`
Policy-map configuration
`host(config-pmap)`
Interface configuration
`host(config-site-router-if)`
Local-site configuration
`host(config-local-site)`
Monitor queuing map configuration
`host(config-mqmap)`
Monitor end-to-end map configuration
`host(config-me2emap)`
Router configuration
`host(config-local-site-router)`
`host(config-site-router)`
Site configuration
`host(config-site)`

Usage Guidelines

To add a text description to a class-map, custom application, policy-map, monitor queuing map, monitor-end-to-end-map, interface, local-site, router or site, use the **description** command. To delete a description, use the **no description** command. You do not have to specify the text to be deleted when removing a description.

description *text*
no description *text*

Syntax Description

text	A single word, without double quotes, describing the class-map, custom application, policy-map, monitor queuing map, monitor-end-to-end-map, interface, local-site, router or site. Use double quotes to include a description containing more than one word.

Example

Having created a new class-map, to add a description, use the following:

```
class-map match-any class_map1
description “First example class-map”
```

Having created a new interface, to add a description, use the following:

```
interface Serial1-0
description “First example logical interface”
```

dir

Mode

Configuration
`host(config)`

Usage Guidelines

To display a list of files on the BQM file system, use the **dir** command. If you are logged in as an admin user you can list backup files and files from the following file-systems: `capture:` , `log:` , `cfg:` , `license:` and `arm:`. The config user can only list the contents of the cfg: file system.

dir {[backup | capture: | cfg: | log: | license | arm]}[<*file-url*>**]**

Syntax Description

file-url	Specifies the name of the file, or directory. Can contain a wild card (*) or question mark (?) to match more than one file. Default is to display all files.

Example

In this example, all the configuration files in the cfg: directory on the file system are listed:

```
host(config)$ dir cfg:
cfg:/
        Size  Name
        1164  bqm_2006-09-13-131852.cfg
        1164  bqm_2006-09-13-131853.cfg
        1164  bqm_2006-09-13-131856.cfg
        1164  bqm_2006-09-13-131900.cfg
        1164  bqm_2006-09-13-131922.cfg
```

In this example, all the packet capture files in the capture file system are listed:

```
host(config)$ dir capture:
capture:
        Size  Name
    66060316  eth1.pcap
    66060316  eth2.pcap
          24  serial1.pcap
host(config)$
```

domain

Mode

Configuration
`host(config)`

Usage Guidelines

To define DNS Name Servers that can be used by the BQM for DNS name resolution, use the **domain** command. A specific DNS Name Server can be removed by use of 'no domain name-server <A.B.C.D>' where A.B.C.D is the IP v4 dotted decimal address of the specific DNS Name Server. . If all DNS Name Server IP addresses are deleted, then DNS name resolution is disabled.

The DNS server address values are preserved in the system configuration file and are treated as other system configuration values and saved to and read from the system configuration file upon change or power-up. Note that a DNS Name Server can also specified during **setup**. All DNS Name Servers specified or removed through either the **domain** or **setup** commands are synchronized.

domain name-server *ip-address*
no domain name-server *ip-address*

Syntax Description

ip-address	Specifies the IPv4 dotted decimal address of a DNS Name Server. No default.

Example

In this example, the DNS server with IP address 192.16.24.2 is configured for BQM host name resolution:

```
host(config)$ domain name-server 192.16.24.2
```

duration

Mode

Configuration
`host(config-capture)`

Usage Guidelines

To set the time limit for a selected packet capture instance, use the **duration** command in capture configuration mode. To remove a time limit for a selected packet capture instance, use the no form of the command. There is no time limit applied to the packet capture if you do not specify a time limit using the **duration** command.

duration <*time*> **{**seconds | minutes | hours | days**}**
no duration <*time*> **{**seconds | minutes | hours | days**}**

Syntax Description

time	Specifies the time limit. You specify the time limit in seconds, minutes, hours or days using the relevant keywords. The maximum duration is 10000 seconds/7 days.

Example

In this example, the packet capture instance is defined, attached to an interface and has file size and a time limit of 60 minutes applied:

```
host(config)# capture serial1
host(config-capture)# attach interface serial1 output
host(config-capture)# size 10000
host(config-capture)# duration 60 minutes
```

In the following example, the capture file size limit is increased to 10GB and limit duration to 2 days:

```
probe(config)# capture serial1
probe(config-capture)# size 10000
probe(config-capture)# duration 2 days
```

end2end-target

Mode

Local-site configuration
`host(config-local-site)#`

Usage Guidelines

To attach a previously configured monitor-end2end-map to the local site, use the **end2end-target** command. To remove a site entry for a monitor-end2end-map, use the **no** form of this command.

end2end-target *name*
no end2end-target *name*

Syntax Description

name	Specify the name of the previously configured monitor-end2end-map (case-sensitive) to be attached to the local site.

Example

In this example, a monitor-end2end-map named intercontinental is attached to the local site:

```
monitor-end2end-map intercontinental
  measure-ping interval-milliseconds 10000 size-bytes 36 availability-threshold
50 event-thresholds delay-milliseconds 500
```

```
host(config)$ local-site Local-site
host(config-local-site)$ end2end-target intercontinental
```

estimate-service-level

Mode

Port configuration
`host(config-mqmap)#`

Usage Guidelines

To enable Congestion Indicator calculations and estimation of the achieved loss or delay for a class or interface, use the **estimate-service-level** command when defining a monitor-queuing-map. The optional keywords enable detection of events using the configured delay queuing-target as the threshold on delay. An event is triggered if any packets are delayed, or lost due to queue tail-drop. If no queuing-target is configured in the monitor-queuing-map, then event detection will not be triggered. Check the monitor-queuing-map configuration so that you know that queuing-targets are present and what their values are.

Use the no form of the command to disable expected service level calculations. Disabling the expected service level parameter in the monitor-queuing-map means that the Expected Delay and Expected Loss graphs in the GUI will not be available.

estimate-service-level [event-thresholds [delay] [loss]]
no estimate-service-level

Syntax Description

delay	Specifies that event detection is triggered if the delay exceeds the configured queuing-targets delay value. Default: Enabled
loss	Specifies that event detection is triggered if any packets are lost due to queue tail drops. Default: Enabled

Example

In this example, the estimate-service-level command is used to enable Congestion Indicator calculations and expected delay and loss. If the delay value configured in the queuing targets for the monitor-queuing-map is exceeded, or if loss due to queue buffer overflow is detected, then the BQM will trigger alerts in each case:

```
host(config-mqm)# estimate-service-level event-thresholds delay loss
host(config-mqm)#
```

ethernet

Mode

Port configuration
`host(config-port)#`

Usage Guidelines

To configure the Ethernet operation fort physical measurement or management interface (PortA, PortB, PortC, PortD, mgmt), use the **ethernet** command. Changes take a couple of seconds to take effect. During this time, the Ethernet settings are reported as 'unknown'. If the change fails, then the interface status is reported as 'unknown'.

ethernet {auto|<duplex> <speed>}

Syntax Description

auto	Duplex and speed will be auto-negotiated.
<duplex>	Forces the duplex value. Can be one of two values: `full` - Forces full duplex operation `half` - Forces half duplex operation
<speed>	Forces the speed value. Can be one of three values: `10` - Forces 10 Mb/s speed `100` - Forces 100 Mb/s speed `1000` - Forces 1 Gb/s speed

Example

In this example, the **ethernet** command is used to change the PortA interface operation from autonegotiation to half-duplex operation at a speed of 10 Mbps:

```
host(config)# port PortA
host(config-port)# show
ethernet auto
host(config-port)# ethernet half 10
host(config-port)# show
ethernet half 10
host(config-port)#
```

exit

Mode

All configuration modes

Usage Guidelines

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode . Note that using the **exit** command in global configuration mode is equivalent to **logout**.

exit

Syntax Description

This command has no arguments or keywords.

Examples

From policy-map configuration mode, use the **exit** command to change to configuration mode:

```
host(config-pmap)# exit
host(config)#
```

filter-class

Mode

Site router interface configuration
`host(config-site-router-if)#`

Usage Guidelines

To add specific traffic filtering match rule information for an interface (or peer interface) you can define a class-map and apply this class-map to an interface with the **filter-class** command.

filter-class <*class-map-name*>
no filter-class <*class-map-name*>

Syntax Description

class-map name	Specify the name of the configured class-map representing the routing table information on the adjacent router.

Example

In the following example, the interface named Serial1/0 is defined as all packets passing through interface *alpha_if* that conform to the match rules defined in the class-map named ip-wanted:

```
class-map ip-wanted
      match ip src=192.168.1.1

site branch1
  router alpha_rtr
      interface Serial1/0
        bandwidth 512
        max_reserved_bandwidth 80
        filter-class ip-wanted
```

In the following example, a class-map defining the MPLS match rules is defined:

```
host(config-site-router-if)$ class-map mplstags
host(config-cmap)$ match mpls label1=100
host(config-cmap)$ match mpls inner-label1=148
host(config-cmap)$ match ip src=192.168.2.3
```

Next, the class-map is applied to the interface using the **filter-class** command. Note that subnet filtering is disabled for the interface.

```
host(config-cmap)$ site newyork_branch
host(config-site)$ router nyc_br_rtr
host(config-site-router)$ interface serial0/1
```

```
host(config-site-router-if)$ bandwidth 256
host(config-site-router-if)$ no subnet-filtering
host(config-site-router-if)$ filter-class mplstags
```

Next, the class-map defining the vLAN tags is defined, and is applied to the peer-interface. Again, subnet filtering is disabled for the peer-interface:

```
host(config-site-router-if)$ class-map vlantags
host(config-cmap)$ match vlan id=4
host(config-cmap)$ site asymmetric
host(config-site)$ router rtr
host(config-site-router)$ peer-interface customer
host(config-site-router-pif)$ no subnet-filtering
host(config-site-router-pif)$ filter-class vlantags
host(config-site-router-pif)$ end
```

help

Mode

All

Usage Guidelines

To list valid commands that can be run from the current configuration mode, use the **help** command. Commands that are valid for each configuration mode in the current hierarchy are listed, starting with the current configuration mode. More detailed help on a particular command can be displayed by entering a specific command name.

help [<*command name*>]

Syntax Description

command name	Specify the command for which more detailed help information is required.

Examples

From the current configuration context, use the help command to list brief details of the commands available:

```
host(config-pmap-c)# help

(config-pmap-c)#
  bandwidth        Specify or modify bandwidth allocated for a policy-maps class
  class-adjust     Sets the packet size class adjustment
  monitor-queuing  Add monitor-queuing to a policy-map's
  priority         Specify guaranteed allowed bandwidth in Kbps or %.
  priority-level   Specify the priority level of this class.
  queue-limit      Max number of packets that queue for class can accumulate
  report           Set threshold for reporting in Kilo bits or as a percentage

(config-pmap)#
  class         Adds a class to a policy-map
  description   Set the description field of a policy-map
  down          Move a class down in the list of policy-map classes
  trace-events  Enable rolling packet capture for a policy-map
  up            Move a class up in the list of policy-map classes

(config)#
  allow               Restricts network access to the device.
```

Following from the example above, use the **help** command to list help information for the **bandwidth** command:

```
host(config-pmap-c)# help bandwidth
bandwidth:
```

```
usage:           bandwidth { bandwidth-kbps | remaining percent percentage | percent
percentage }

bandwidth-kbps
Amount of bandwidth, in number of kbps, to be assigned to the class. The amount of
bandwidth varies according to the interface and platform in use

remaining percent percentage
Amount of guaranteed bandwidth, based on a relative percent of available bandwidth.

percent percentage
percentage of the total available bandwidth to be set aside for the priority class,
range <1-100>.

host(config-pmap-c)#
```

From the config directory, use the **help** command to list the commands available:

```
host(config)$ help
(config)
  allow                Restricts network access to the device.
  backup               Backup configuration and database, [capture files] to a target
destination.
  capture              Configures a packet capture instance
  capture-settings     Configures global packet capture parameters
  class-map            Configure a class-map
  clear                Reset functions
  clock                Configure time-of-day clock.
  copy                 Copy from a source to a destination
  custom-application   Configure a custom-application
  delete               Delete files from a filesystem
  dir                  List files on a filesystem
  domain               Configures DNS Name Servers.
  end                  Return to base context
  exit                 Exit configuration mode or EXEC
  help                 List commands that can be run
  license              Install and/or displays the license file
  local-site           Configure the local site
  log                  Display the end of the local system log file.
  logging              Configures parameters of the remote logging system.
  logout               Logs out a user
  monitor-end2end-map  Configure a monitor-end2end-map
  monitor-queuing-map  Configure a monitor-queuing-map
  more                 List contents of file
  no                   Reverses next command, such as creation of a class-map.
  ntp                  Configure Network Time Protocol Services.
  password             Sets login password or passowrd used to protect capture files
  ping                 Sends ICMP ECHO_REQUEST to network hosts
  policy-map           Configure a policy-map
-- More --
```

interface

Mode

Router Configuration

```
host(config-local-site-router)#
host(config-site-router)#
```

Usage Guidelines

To create a model interface, use the **interface** command. Interfaces can be used to model interfaces on an adjacent router. You use the **service-policy** command to attach a traffic policy to a model interface. See the **service-policy** command for more information.

The BQM measurement interface names PortA, PortB, PortC, and PortD are fixed and cannot be deleted.

interface <*interface name*>
no interface <*interface name*>

Syntax Description

interface name	Specifies a name for the model interface.

Examples

To create an interface called Serial1-0:

```
interface Serial1-0
```

In this example, interfaces (Serial1-0A, Serial1-0B, Serial1-1A, Serial1-1B) are defined to monitor traffic for the interfaces of interest on an adjacent router. Class-maps (Serial1-0, Serial1-1) have previously been defined to represent the topology/routing information on the router. A QoS policy, mirroring that on the router, is then defined and applied to each WAN interface:

```
policy-map QoS
  class Apps
    bandwidth 30
  class Other
    bandwidth 10

interface Serial1-0A
  service-policy output QoS
interface Serial1-0B
  service-policy output QoS
interface Serial1-1A
  service-policy output QoS
interface Serial1-1B
  service-policy output QoS
```

license

Mode

All

Usage Guidelines

To install the BQM license, use the **license** command**.** If the license has been installed, this command displays the text of the BQM license agreement when no arguments specified.

license install tftp://[<hostname> | <A.B.C.D>]/*remote_filename*

Syntax Description

install	Installs a license file.
remote filename	Installs a license from a remote filesystem (tftp://Host|A.B.C.D/<filename>).

Example

To display the license agreement, use the following:

```
host(config)$ license
```

To install the specified license file from tftp host 192.16.10.1, use the following:

```
host(config)$ license install tftp://192.16.10.1/BQM_license/BQM_0E456de6556aaa.lic
```

link-adjust

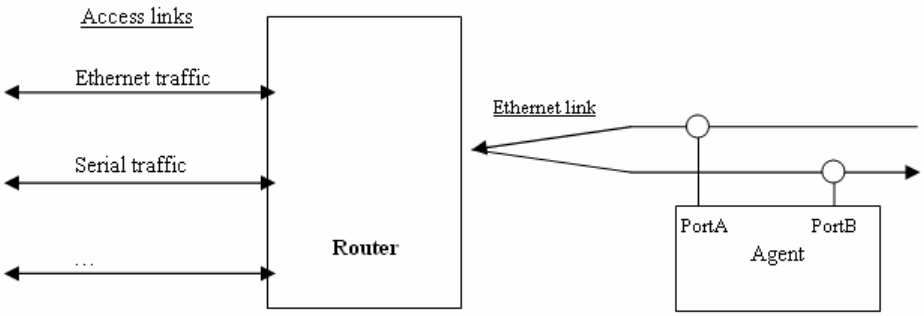
Mode

Site router interface configuration
`host(config-site-router-if)#`

Usage Guidelines

To configure a value for an interface that takes into account overhead adjustments when determining the correct number of bytes in a packet, use the **link-adjust** command. To remove an adjustment value, use the **no** form of this command. Note that if the link-adjust value is set in the interface context, then any value set in an associated policy-map is overridden.

The BQM by default uses layer 3 packet sizes only, that is only the IP packet size is counted. This behavior can however be changed using the **link-adjust** command. This allows for increased accuracy when calculating results. For example, on a HDLC Serial line, the adjustment can be made when calculating the correct number of bytes to allow for the layer 2 HDLC link layer headers when totaling the number of bytes in the packet versus the number of bytes due to an IP payload.



For example, in the diagram above, the BQM is monitoring an Ethernet link on the far side of a router that has both Ethernet and Serial interfaces. To compensate for the difference between the actual layer 2 frame size and the layer 3 packet size counted by the device, you use the **link-adjust** command.

link-adjust *adjustment-value*
no link-adjust *adjustment-value*

Syntax Description

adjustment value	Specifies a value to allow for link overhead adjustments when determining the correct number of bytes in a packet. The *adjustment-value* can be positive or negative, for example, wanting to include an MPLS Label in bandwidth calculations which has already been allowed for by the code, requires an *adjustment-value* of minus four (- 4). Range: -2000 to +2000. Default: 0 (zero)

Example

In this example, the **link-adjust** command is used to take account of Ethernet packet overhead when monitoring an Ethernet interface. To calculate the appropriate measurements using a BQM, you use the **link-adjust** command to account for the additional Ethernet packet (14 byte) overhead. In this example the link-adjust value is configured in the interface context:

```
interface Ethernet4/0
  bandwidth 200000
  service-policy output test-pol
  link-adjust 14
```

local-site

Mode

Configuration
`host(config)#`

Usage Guidelines

A default local site is configured on the system as part of the default network model. To configure local site properties, you use the **local-site** command. To remove a local site you use the **no** form of the command.

local-site <*name* >
no local-site <*name*>

Syntax Description

name	Identify the name of the configured local site to be edited.

Example

In the following example, 'Local-site' is configured:

```
local-site Local-site
      subnet 192.168.1.0/24

      router core1

            interface Serial0/1
                  description Link to remote site1
                  bandwidth 512
                  service policy output low-speed

            interface Serial0/2
                  description Link to remote site2
                  bandwidth 512
                  service policy output low-speed
```

log

Mode

All

Usage Guidelines

To display the end of the system log file, use the **log** command. You must be logged in as an admin user to use this command.

System log messages can be copied to a remote syslog server using the **logging** command.

log [internal][-<*number of lines*>]

Syntax Description

internal	Displays the contents of the internal system log.
-<*number of lines*>	Specify how many lines of the end of the log to display; defaults to 10.

Example

In this example, the **log** command is used to display the end of the system log:

```
host(config)$ log

Jan 20 16:58:33 (none) user.crit -probesh: 'admin' entered command: show
Jan 20 16:59:18 (none) user.crit -probesh: 'admin' entered command: interface
simpleScen
Jan 20 16:59:22 (none) user.crit -probesh: 'admin' entered command: show
Jan 20 17:00:35 (none) user.crit -probesh: 'config' entered command: exit
Jan 20 17:00:38 (none) user.crit -probesh: 'config' entered command: no interface if
Jan 20 17:00:45 (none) user.crit -probesh: 'config' entered command: show
Jan 20 17:01:12 (none) user.crit -probesh: 'config' entered command: help log
Jan 20 17:01:20 (none) user.crit -probesh: 'config' entered command: exit
Jan 20 17:01:23 (none) user.crit -probesh: 'config' entered command: help log
Jan 20 17:02:07 (none) user.crit -probesh: 'config' entered command: log
host(config)$
```

logging

Mode

Configuration

Usage Guidelines

To log system messages and debug output to a remote host, use the **logging** command. To remove a specified logging host from the configuration, use the **no** form of this command.

Standard system logging is enabled by default. If logging has been disabled on your system (using the **no logging** command), logging can be re-enabled using the **logging** command. The **logging** command identifies a remote host (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of hosts that receive logging messages.To specify the severity level for logging to all hosts, use the **logging trap** command. Use the **alarm** keyword and *severity* argument to limit the number of syslog messages generated.

Remote logging does not cause any changes to the information displayed in the local log, as reported in the **log** command.

logging {[*hostname* **|** *IP address***]} | [host {[***hostname* **|** *IP address***]} [transport udp [port** *port***]] >**
no logging {[*hostname* **|** *IP address***]} | [***hostname* **|** *IP address***] [transport udp [port** *port***]] >**

Syntax Description

hostname	Specifies the DNS host name of the syslog server to which you want to copy the system log messages. The remote syslog server must be set up to allow receipt of messages from the network.
IP address	Specify the IP v4 dotted decimal address of the syslog server to which you want to copy the system log messages. The remote syslog server must be set up to allow receipt of messages from the network.
transport udp	Keywords utilized to specify udp transport. Default: udp transport.
port *port*	Keyword utilized to specify udp transport port and the port number for the syslog server to which syslog notifications are to be sent. Default: udp port 514.

Example

In this example, the **logging** command is used to switch on logging to the syslog server with IP address 192.168.128.4:

```
host(config)# logging 192.168.128.4
host(config)#
```

match

Mode

Class-map configuration
`host(config-cmap)#`
Custom application configuration
`host(config-custom-app)#`

Usage Guidelines

The **match** command is the most important in the BQM command set, because it identifies the set of IP packets that are used to classify traffic. To add a match rule to a class-map or to a custom application definition, use the **match** command.

match [not] <type> <expr> [<type> <expr>]

match [not] class-map=<class-map name>

match any
no match any

<type> := class-map | application | ethertype | ip | mpls | tcp | udp | vlan | any

<expr> := any | <attr-value-list>

<attr-value-list> := [<parameter> = <value>]

<parameter> := application name | destination-port | dscp | dst | dstport |exp<N> | inner-exp<N> | inner-label<N> | label<N> |port | precedence | protocol | source-port | src | srcport | stack-size | tos

<value> := [A-Za-z0-9,.:-_][A-Za-z0-9.,:-_]

The BQM has a set of rules the syntax must obey:

- <expr>'s are logically ANDed together if they are in a single match statement
- the not keyword inverts the meaning of the match and, when used, must be the first token in the match
- the <type> keyword, apart from dictating what "type" of traffic is matched also determines which valid commands may follow
- a <type> must be entered
- a second <type> may be entered in order to match encapsulated packet information
- circular references are strictly forbidden, that is, match rules that refer to class-maps that in some way refer back to the current class-map are not allowed
- in general, position in an expression list is not important
- in general, a parameter can only appear once in an expression

In general, if you break any of these rules, an appropriate warning is issued when you attempt to verify the configuration file.

Examples

In this example, a rule to match all packets is created:

```
match any
```

In this example, a rule to match all IP traffic is created:

```
match ip any
```

However, in this example, the match not command is used. Here, the class-map criteria will be successful for any traffic other than IP traffic:

```
match not ip any
```

In this example, a rule to match MPLS traffic encapsulating IP traffic is created:

```
match mpls ip any
```

The following pages give details of the use of various match command types.

match any

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

To configure the match criteria for a class-map to accept all packets, use the **match any** command.

The **match not any** command is not allowed. To remove the match any rule, use the no form of the command.

match any
no match any

Syntax Description

This command has no arguments or keywords.

Example

In this example, the class_map1 match criterion is configured to be successful for all packets:

```
match any
```

match application

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

To enable classification based on custom applications defined using the **custom-application** command, or predefined applications, and non-UDP and TCP protocols (specifically defined in a custom-application), use the **match application** command.
To exclude the match criteria contained in one class-map from another class-map, use the **match not class-map** command.

Other non UDP and TCP protocols such as AppleTalk and IPX can be matched using the **match ethertype** or **match ip protocol** commands. The following table lists these non UDP or TCP protocols:

Protocol Name	Match Rule
AppleTalk ARP	match ethertype=0x80F3
AppleTalk	match ethertype=0x809B
IP ARP	match ethertype=0x0806
Exterior Gateway Protocol	match ip protocol=8
Enhanced Interior Gateway Routing Protocol	match ip protocol=88
Generic Routing Encapsulation	match ip protocol=47
Internet Control Message	match ip protocol=1
IP	match ethertype=0x0800
IP in IP (encapsulation)	match ip protocol=4
IP Security Protocol (ESP/AH)	match ip protocol=50 match ip protocol=51
IPV6	match ethertype=0x86DD
Novell IPX	match ethertype=0x8137

NOTE: See Appendix C for a full list of supported applications based on TCP/UDP protocols.

match application <*name*> [<*property-key*>=<*property-value*>]
no **match application** <*name*>

Syntax Description

name	Specify a configured custom application or a predefined application, for example, appletalk, ipx, eigrp, icmp.
property-key	Specifies an application property specific to the predefined well known application (that is, this is not available for custom applications). For example, the following properties are available for HTTP: File length, URL, Content-Type, Filename. No default.
property-value	Specifies an expression to match the value of the property key. For example, match application HTTP URL=http://www.cisco.com/* would match all HTTP requests where the requested URL matches the expression 'http://www.cisco.com/*'. No default.

Examples

In this example, a previously configured custom application named peer2peer is used to classify traffic:

```
match application peer2peer
```

In this example, a well-known application, in this case appletalk, is used to classify traffic:

```
match application appletalk
```

match class-map

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

To nest traffic classes within one another, use the **match class-map** command. This saves the effort of re-creating a new class-map when most of the information exists in a previously configured class-map.

To exclude the match criteria contained in one class-map from another class-map, use the **match not class-map** command.

match [not] **class-map**=<*class-map name*>
no match [not] **class-map**=<*class-map name*>

Syntax Description

class-map name	Specify the name of the class-map.

Examples

In this example, class_map1 is nested within class_map2:

```
match class-map=class_map1
```

In this example, class_map1 has the same characteristics as class_map2, except that class_map2 has added a source address as a match criterion. Rather than configuring class_map2 line by line all over again, you can use the match class-map command:

```
class-map class_map1
      match ip protocol=udp
      match ip protocol=icmp

class-map class_map2
      match class-map=class_map1
      match ip src=192.168.11.1
```

match ethertype

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

The Ethertype value appears following the Source Address field in a Version 2 Ethernet frame. The Ethertype value provides an identifier enabling the communications software to differentiate between various types of protocols. A different protocol handler is used for different function, and the Ethertype identifies the frame as belonging to one or another protocol family.

To match traffic based on Ethernet MAC Header length/type field, use the **match ethertype** command. To exclude the matching traffic, use the **match not ethertype** command. To remove this match rule, use the **no** form of the command.

This command can also be used to match/not match against 802.3/802.2 LLC traffic where the match is made against the DSAP/SSAP LLC fields.

The following table lists the major non-UDP or TCP protocols that can be matched using the **match ethertype** command:

Protocol	Match Rule
AppleTalk Address Resolution Protocol (AARP)	match ethertype=0x80F3
AppleTalk (EtherTalk)	match ethertype=0x809B
Address Resolution Protocol (ARP)	match ethertype=0x0806
IEEE 802.1Q-tagged frame	match ethertype=0x8100
IPv4	match ethertype=0x0800
IPv6	match ethertype=0x86DD
Novell IPX Reverse Address Resolution Protocol (RARP)	match ethertype=0x8137 match ethertype=0x8035

See Appendix D for a more detailed list of Ethertype identifiers.

match [not] ethertype=<*ethertype value*>
no match [not] ethertype=<*ethertype value*>

Syntax Description

ethertype value	Specify traffic with a specific Ethernet type (MAC Header length/type value for Ethernet traffic or DSAP/SSAP LLC pair for 802.3/802.2 traffic.)

Examples

In this example, the **match ethertype** command is used to match : Ethernet frame type of Appletalk:

```
match ethertype=0x809B
```

In this example, the **match ethertype** command is used to match an 802.3/802.2 DSAP/SSAP LLC using Novell's IPX:

```
match ethertype=0xE0E0
```

match ip

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

To configure the match criteria for a class-map to be successful for IP packets, subject to certain specified conditions, use the **match ip** command. At least one of the attributes listed below between the braces ({}) must be specified – either 'any' on its own, or some valid combination of the other options. To configure the match criteria for a class-map to be successful for all traffic except IP packets subject to the given criteria, use the **match not ip** command.

match [not] **ip** {[any] |
[protocol=<*protocol*>]
[src=<*ip address*>[/<*prefix length*>]]
[dst=<*ip address*>[/<*prefix length*>]]
[[precedence=<*prec-spec*>] [tos=<*tos-value*>]|[dscp=<*dscp-value*>]]}

no match [not] **ip** {[any] |
[protocol=<*protocol*>]
[src=<*ip address*>[/<*prefix length*>]]
[dst=<*ip address*>[/<*prefix length*>]]
[[precedence=<*prec-spec*>] [tos=<*tos-value*>]|[dscp=<*dscp-value*>]]}

Syntax Description

Any	Matches any type of IP traffic on any (both) measurement interfaces. No other expressions are allowed in a match if this command is used.
dscp=<dscp-value>	Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match. The current release supports only the numerical specification. Here are the keywords: <0-63> Differentiated services codepoint value af11 Match packets with AF11 dscp (001010) == 10 af12 Match packets with AF12 dscp (001100) == 12 af13 Match packets with AF13 dscp (001110) == 14 af21 Match packets with AF21 dscp (010010) == 18 af22 Match packets with AF22 dscp (010100) == 20 af23 Match packets with AF23 dscp (010110) == 22 af31 Match packets with AF31 dscp (011010) == 26 af32 Match packets with AF32 dscp (011100) == 28 af33 Match packets with AF33 dscp (011110) == 30 af41 Match packets with AF41 dscp (100010) == 34 af42 Match packets with AF42 dscp (100100) == 36

	af43 Match packets with AF43 dscp (100110) == 38 cs1 Match packets with CS1(precedence 1) dscp (001000) == 8 cs2 Match packets with CS2(precedence 2) dscp (010000) == 16 cs3 Match packets with CS3(precedence 3) dscp (011000) == 24 cs4 Match packets with CS4(precedence 4) dscp (100000) == 32 cs5 Match packets with CS5(precedence 5) dscp (101000) == 40 cs6 Match packets with CS6(precedence 6) dscp (110000) == 48 cs7 Match packets with CS7(precedence 7) dscp (111000) == 56 default Match packets with default dscp (000000) == 0 ef Match packets with EF dscp (101110) == 46
dst=<ip address>[/<prefix length>]	Matches the packets with destinations from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X/M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32.
precedence=<prec-value>	Matches a precedence value from 0 to 7. They can be specified by name too. Cannot be used with dscp command in a single match. <prec-value> can be a number from 0 to 7 or one of the following names: critical, flash, flash-override, immediate, internet, network, priority, routine.
protocol=<protocol>	Matches traffic of a particular protocol specified in the IP header. <protocol> is a number between 0 and 255 or a well known protocol name such as tcp, icmp or igmp.
src=<ip address>[/<prefix length>]	Matches the packets with source addresses from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32.
tos=<tos-value>	Matches a TOS value, from 0 to 15. Can be specified as a name too. Cannot be used with dscp command in a single match. <tos-value> can be a number from 0 to 15 or one of the following names: max-reliability, max-throughput, min-delay, min-monetary-cost, normal. tos=<tos-value><tos-value> := <number> | max-reliability | max-throughput | min-delay | min-monetary-cost | normal

Examples

The following examples show how you can use the match ip command, creating individual match criteria or concatenating several criteria in a single entry. In this example, the class_map1 match criteria is configured to be successful for all IP packets. As noted above, using any excludes the use of all other expressions:

```
match ip any
```

In this example, the class_map1 match criteria is configured to be successful for all ICMP traffic:

```
match ip protocol=icmp
```

The following table lists non UDP or TCP protocols that can be matched using the **match ip protocol** command:

Protocol Name	Match Rule
Exterior Gateway Protocol	match ip protocol=8
Enhanced Interior Gateway Routing Protocol	match ip protocol=88
Generic Routing Encapsulation	match ip protocol=47
Internet Control Message	match ip protocol=1
IP in IP (encapsulation)	match ip protocol=4
IP Security Protocol (ESP/AH)	match ip protocol=50 match ip protocol=51

In this example, the class_map1 match criterion is configured to be successful for IP packets with source address 192.168.1.10:

```
match ip src=192.168.1.10
```

In this example, the class_map1 match criterion is configured to be successful for IP packets with source network address 192.168.0.0 and destination network address 172.21.0.0:

```
match ip src=192.168.0.0/16 dst=172.21.0.0/16
```

In this example, the class_map1 match criterion is configured to be successful for IP packets with an IP precedence value of 5:

```
match ip precedence=5
```

In this example, the class_map1 match criterion is configured to be successful for IP packets with the DSCP value 5:

```
match ip dscp=5
```

In this example, the class_map1 match criterion is configured to be successful for IP packets with the DSCP value 5:

```
match ip src=192.168.0.0/16 dst=172.21.0.0/16 dscp=5
```

match mpls

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines
To configure the match criteria for a class-map to be successful for MPLS packets, subject to certain specified conditions, use the **match mpls** command. At least one of the attributes listed below between the braces ({}) must be specified – either 'any' on its own, or some valid combination of the other options. To configure the match criteria for a class-map to be successful for all traffic except MPLS packets subject to the given criteria, use the **match not mpls** command.

match [not] **mpls** {[any] | exp <*num*> | inner-exp<*num*> | inner-label<*num*> | [label<*num*>=<*label*>[:<*label*>]] | [stack-size=<*stack size*>]} [{ip | tcp | udp} ...]

no match [not] **mpls** {[any] | exp <*num*> | inner-exp<*num*> | inner-label<*num*> | [label<*num*>=<*label*>[:<*label*>]] | [stack-size=<*stack size*>]} [{ip | tcp | udp} ...]

Syntax Description

Any	Matches any type of MPLS traffic on any (both) measurement interfaces. No other expressions are allowed in a match if this command is used.
exp<num>=<exp value>	Matches MPLS traffic with the specified experimental value. <num> specifies a position on the MPLS label stack, 1 is the top of the stack (that is, the most recently pushed label). <exp value> must be a 3-bit number from 0 to 7.
inner-exp<num>=<label value>[:<label value>]	Matches MPLS traffic with the specified experimental value. <num> specifies a position on the MPLS label stack, 1 is the bottom of the stack (that is, the first pushed label). <exp value> must be a 3-bit number from 0 to 7
inner-label<num>=<label value>[:<label value>]	Matches MPLS traffic with the specified label or label range. <num> specifies a position on the MPLS label stack, 1 is the bottom of the stack (that is, the first pushed label). <label value> must be a 20-bit number from 0 to 1048575.
label<num>=<label>[:<label>]	Matches a single MPLS label or range of labels (up to and including a maximum of six labels). <num> specifies a position on the MPLS label stack, with 1 indicating the top of the stack (that is, the most recently pushed label). <label> must be a 20-bit value from 0 to 1048575.
stack-size=<stack size >	Matches MPLS traffic with a stack size equal to the specified value. This number must be from 1 to 255.
ip	Specifies that the MPLS packet encapsulates an IP packet. If this is specified then it can be followed by any expression that is valid for the match ip command (see above).
tcp	Specifies that the MPLS packet encapsulates a TCP packet. If this is specified then it can be followed by any expression that

	is valid for the match tcp command (see below).
udp	Specifies that the MPLS packet encapsulates a UDP packet. If this is specified then it can be followed by any expression that is valid for the match udp command (see below).

Examples

The following examples show how you can use the match mpls command, creating individual match criteria or concatenating several criteria in a single entry. In this example, the class_map1 match criterion is configured to be successful for all MPLS packets. As noted above, using any excludes the use of all other expressions:

```
match mpls any
```

In this example, the class_map1 match criterion is configured to be successful for all MPLS traffic with an MPLS stack of 2 labels in size:

```
match mpls stack-size=2
```

In this example, the class_map1 match criterion is configured to be successful for MPLS packets with a label of 24 on top of the stack:

```
match mpls label1=24
```

In this example, the class_map1 match criteria is configured to be successful for MPLS packets with a label between 10 and 20 on top of the stack, a second label of 40 and a stack size of 2:

```
match mpls label1=10:20 label2=40 stack-size=2
```

In this example, the class_map1 match criterion is configured to be successful for MPLS packets with an embedded IP packet:

```
match mpls ip any
```

In this example, the class_map1 match criterion is configured to be successful for MPLS packets with one label in the stack and encapsulating TCP web traffic:

```
match mpls stack-size=1 tcp port=www
```

match tcp

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines
To configure the match criteria for a class-map to be successful for TCP traffic, subject to certain specified conditions, use the **match tcp** command. At least one of the attributes listed below between the braces ({}) must be specified – either 'any' on its own, or some valid combination of the other options. To configure the match criteria for a class-map to be successful for all traffic except TCP traffic subject to the given criteria, use the **match not tcp** command.

match [not] **tcp** {[any] |
[src=<*ip address*>[/<*address mask*>]]
[dst=<*ip address*>[/<*address mask*>]]
[port=<*port*>[:<*port*>]|[source-port|srcport=<*port*>[:<*port*>]][destination-port|dstport=<*port*>[:<*port*>]][[precedence=<*prec-value*>][tos=<*tos-value*>]|[dscp=<*dscp-value*>]]}

no match [not] **tcp** {[any] |
[src=<*ip address*>[/<*address mask*>]]
[dst=<*ip address*>[/<*address mask*>]]
[port=<*port*>[:<*port*>]|[source-port|srcport=<*port*>[:<*port*>]][destination-port|dstport=<*port*>[:<*port*>]][[precedence=<*prec-value*>][tos=<*tos-value*>]|[dscp=<*dscp-value*>]]}

Syntax Description

any	Matches any type of TCP traffic on any (both) measurement interfaces. No other expressions are allowed in a match if this command is used.
destination-port=<port>[:<port>]	Matches a single port or range of destination ports. The port can be specified as a name from the well-recognized list of port names, for example, smtp, ftp, ssh.
dscp=<dscp-value>	Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match. The current release supports only the numerical specification. Here are the keywords: <0-63> Differentiated services codepoint value af11 Match packets with AF11 dscp (001010) == 10 af12 Match packets with AF12 dscp (001100) == 12 af13 Match packets with AF13 dscp (001110) == 14 af21 Match packets with AF21 dscp (010010) == 18 af22 Match packets with AF22 dscp (010100) == 20 af23 Match packets with AF23 dscp (010110) == 22 af31 Match packets with AF31 dscp (011010) == 26 af32 Match packets with AF32 dscp (011100) == 28 af33 Match packets with AF33 dscp (011110) == 30 af41 Match packets with AF41 dscp (100010) == 34

	af42 Match packets with AF42 dscp (100100) == 36 af43 Match packets with AF43 dscp (100110) == 38 cs1 Match packets with CS1(precedence 1) dscp (001000) == 8 cs2 Match packets with CS2(precedence 2) dscp (010000) == 16 cs3 Match packets with CS3(precedence 3) dscp (011000) == 24 cs4 Match packets with CS4(precedence 4) dscp (100000) == 32 cs5 Match packets with CS5(precedence 5) dscp (101000) == 40 cs6 Match packets with CS6(precedence 6) dscp (110000) == 48 cs7 Match packets with CS7(precedence 7) dscp (111000) == 56 default Match packets with default dscp (000000) == 0 ef Match packets with EF dscp (101110) == 46
dst-port=<port>[:<port>]	An alias for the destination-port command.
dst=<ip address>[/<prefix length>]	Matches the packets with destinations from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32.
port=<port>[:<port>]	Matches a single port or range of ports (source or destination). The port can be expressed as a single port or as a range. <port> can be a number or a well known port name, for example, smtp, ftp, ssh.
precedence=<prec-value>	Matches a precedence value from 0 to 7. It can be specified by name too. Cannot be used with dscp command in a single match. <prec-value> can be a number from 0 to 7 or one of the following names: critical, flash, flash-override, immediate, internet, network, priority, routine.
source-port=<port>[:<port>]	Matches a single port or range of source ports. The port can be specified as a name from the well-recognized list of port names, for example, smtp, ftp, ssh
src=<ip address>[/<prefix length>]	Matches the packets with source addresses from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32.
srcport=<port>[:<port>]	An alias for the source-port command.
tos=<tos-value>	Matches a TOS value, from 0 to 15. Can be specified as a name too. Cannot be used with dscp command in a single match. <tos-value> can be a number from 0 to 15 or one of the following names: max-reliability, max-throughput, min-delay, min-monetary-cost, normal. tos=<tos-value><tos-value> := <number> | max-reliability | max-throughput | min-delay | min-monetary-cost | normal

Examples

In this example, the class_map1 match criterion is configured to be successful for all TCP traffic:

```
match tcp any
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic telnet and ftp source ports:

```
match tcp source-port=telnet:ftp
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic with source network address 192.168.0.0 and with destination network 172.21.0.0:

```
match tcp src=192.168.0.0/16 dst=172.21.0.0/16
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic going from the source network 192.168.0.0 within the given source port range to the destination network 172.21.0.0 within the given destination port range:

```
match tcp src=192.168.11.1 dst=192.168.11.3 source-port=161:162 destination-
port=1057:1158
```

In this example, the class_map1 match criterion is configured to be successful for all packets from the source network 192.168.0.0 to the specified destination port range:

```
match tcp src=192.168.0.0/16 destination-port=80:443
```

In this example, the class_map1 match criterion is configured to be successful for all TCP traffic from/to the specified ports:

```
match tcp port=20:25
```

This example is equivalent to the one above:

```
match tcp port=ftp-data:smtp
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic with the DSCP value 6:

```
match tcp dscp=6
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic with TOS value 8:

```
match tcp tos=8
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic with precedence value 2:

```
match tcp precedence=2
```

In this example, the class_map1 match criterion is configured to be successful for TCP traffic from the source network 192.168.0.0 to the specified destination port range with a precedence value of 2:

```
match tcp src=192.168.0.0/16 destination-port=161:162 precedence=2
```

match udp

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

To configure the match criteria for a class-map to be successful for UDP traffic, subject to certain specified conditions, use the **match udp** command. At least one of the attributes listed below between the braces ({}) must be specified – either 'any' on its own, or some valid combination of the other options. To configure the match criteria for a class-map to be successful for all traffic except UDP traffic subject to the given criteria, use the **match not udp** command.

match [not] **udp** {[any] |
[src=<*ip address*>[/<*address mask*>]]
[dst=<*ip address*>[/<*address mask*>]]
[port=<*port*>[:<*port*>]|[source-port|srcport=<*port*>[:<*port*>]][destination-port|dstport=<*port*>[:<*port*>]][[precedence=<*prec-value*>][tos=<*tos-value*>]|[dscp=<*dscp-value*>]]}

no match [not] **udp** {[any] |
[src=<*ip address*>[/<*address mask*>]]
[dst=<*ip address*>[/<*address mask*>]]
[port=<*port*>[:<*port*>]|[source-port|srcport=<*port*>[:<*port*>]][destination-port|dstport=<*port*>[:<*port*>]][[precedence=<*prec-value*>][tos=<*tos-value*>]|[dscp=<*dscp-value*>]]}

Syntax Description

Any	Matches any type of UDP traffic on any (both) measurement interfaces. No other expressions are allowed in a match if this command is used.
destination-port=<port>[:<port>]	Matches a single port or range of destination ports. The port can be specified as a name from the well-recognized list of port names, for example, smtp, ftp, ssh.
dscp=<dscp-value>	Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match. The current release supports only the numerical specification. Here are the keywords: <0-63> Differentiated services codepoint value af11 Match packets with AF11 dscp (001010) == 10 af12 Match packets with AF12 dscp (001100) == 12 af13 Match packets with AF13 dscp (001110) == 14 af21 Match packets with AF21 dscp (010010) == 18 af22 Match packets with AF22 dscp (010100) == 20 af23 Match packets with AF23 dscp (010110) == 22 af31 Match packets with AF31 dscp (011010) == 26 af32 Match packets with AF32 dscp (011100) == 28 af33 Match packets with AF33 dscp (011110) == 30

	af41 Match packets with AF41 dscp (100010) == 34 af42 Match packets with AF42 dscp (100100) == 36 af43 Match packets with AF43 dscp (100110) == 38 cs1 Match packets with CS1(precedence 1) dscp (001000) == 8 cs2 Match packets with CS2(precedence 2) dscp (010000) == 16 cs3 Match packets with CS3(precedence 3) dscp (011000) == 24 cs4 Match packets with CS4(precedence 4) dscp (100000) == 32 cs5 Match packets with CS5(precedence 5) dscp (101000) == 40 cs6 Match packets with CS6(precedence 6) dscp (110000) == 48 cs7 Match packets with CS7(precedence 7) dscp (111000) == 56 default Match packets with default dscp (000000) == 0 ef Match packets with EF dscp (101110) == 46
dst=<ip address>[/<prefix length>]	Matches the packets with destinations from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32
dstport=<port>[:<port>]	An alias for the destination-port command.
port=<port>[:<port>]	Matches a single port or series of ports (source or destination). The port can be expressed as a single port or as a range. <port> can be a number or a well known port name, for example, smtp, ftp, ssh.
precedence=<prec-value>	Matches a precedence value from 0 to 7. They can be specified by name too. Cannot be used with dscp command in a single match. <prec-value> can be a number from 0 to 7 or one of the following names: critical, flash, flash-override, immediate, internet, network, priority, routine.
source-port=<port>[:<port>]	Matches a single port or range of source ports. The port can be specified as a name from the well-recognized list of port names, for example, ssh.
src=<ip address>[/<prefix length>]	Matches the packets with source addresses from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32
srcport=<port>[:<port>]	An alias for the source-port command.
tos=<tos-value>	Matches a TOS value, from 0 to 15. Can be specified as a name too. Cannot be used with dscp command in a single match. <tos-value> can be a number from0 to 15 or one of the following names: max-reliability, max-throughput, min-delay, min-monetary-cost, normal. tos=<tos-value><tos-value> := <number> | max-reliability | max-throughput | min-delay | min-monetary-cost | normal

Examples

In this example, the class_map1 match criteria is configured to be successful for all UDP traffic:

```
match udp any
```

In this example, the class_map1 match criterion is configured to be successful for UDP traffic from telnet and ftp source ports:

```
match udp source-port=telnet:ftp
```

In this example, the class_map1 match criterion is configured to be successful for UDP traffic with source network address 192.168.0.0 and destination network address 172.21.0.0:

```
match udp src=192.168.0.0/16 dst=172.21.0.0/16
```

In this example, the class_map1 match criteria is configured to be successful for UDP traffic with source network address 192.168.0.0, destination network address 172.21.0.0, and within the given source and destination port ranges:

```
match udp src=192.168.11.1 dst=192.168.11.3 source-port=1698:1699 destination-
port=1698:1699
```

In this example, the class_map1 match criterion is configured to be successful for UDP traffic with source network address 192.168.0.0 and within the specified destination port range:

```
match udp src=192.168.0.0/16 destination-port=67:68
```

In this example, the class_map1 match criterion is configured to be successful for all UDP traffic from/to the specified ports:

```
match udp port=20:25
```

This example is equivalent to the one above:

```
match udp port=ftp-data:smtp
```

In this example, the class_map1 match criterion is configured to be successful for UDP traffic with the DSCP value 3:

```
match udp dscp=3
```

In this example, the class_map1 match rule is configured to be successful for UDP traffic with TOS value 2:

```
match udp tos=2
```

In this example, the class_map1 match criterion is configured to be successful for UDP traffic with precedence value 4:

```
match udp precedence=4
```

In this example, the class_map1 match criterion is configured to be successful for UDP traffic from the source port 7070 to the specified destination port range with a precedence value of 4:

```
match udp source-port=7070 destination-port=67:68 precedence=4
```

match vlan

Mode

Class-map configuration
`host(config-cmap)#`

Usage Guidelines

To match traffic encapsulated by VLAN, use the **match vlan** command. To exclude the matching traffic, use the **match not vlan** command. To remove this match rule, use the **no** form of the command.

match [not] {vlan id**=<***vlan id***>** [src=<*ip address*>[/<*address mask*>]]
[dst=<*ip address*>[/<*address mask*>]]
[port=<*port*>[:<*port*>]|[source-port|srcport=<*port*>[:<*port*>]][destination-port|dstport=<*port*>[:<*port*>]][[precedence=<*prec-value*>][priority=<vlan user priority>][tos=<*tos-value*>]|[dscp=<*dscp-value*>]]} [{ip | tcp | udp…}]
no match [not] {vlan id**=<***vlan id***>** [src=<*ip address*>[/<*address mask*>]]
[dst=<*ip address*>[/<*address mask*>]]
[port=<*port*>[:<*port*>]|[source-port|srcport=<*port*>[:<*port*>]][destination-port|dstport=<*port*>[:<*port*>]][[precedence=<*prec-value*>][priority=<vlan user priority>][tos=<*tos-value*>]|[dscp=<*dscp-value*>]]} [{ip | tcp | udp}…]

Syntax Description

vlan id	Specify the VLAN id value for matching traffic. The vlan id number range is 0 to 4095.
destination-port=<port>[:<port>]	Matches a single port or range of destination ports. The port can be specified as a name from the well-recognized list of port names, for example, ssh.
dscp=<dscp-value>	Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match. The current release supports only the numerical specification. Here are the keywords: <0-63> Differentiated services codepoint value af11 Match packets with AF11 dscp (001010) == 10 af12 Match packets with AF12 dscp (001100) == 12 af13 Match packets with AF13 dscp (001110) == 14 af21 Match packets with AF21 dscp (010010) == 18 af22 Match packets with AF22 dscp (010100) == 20 af23 Match packets with AF23 dscp (010110) == 22 af31 Match packets with AF31 dscp (011010) == 26 af32 Match packets with AF32 dscp (011100) == 28 af33 Match packets with AF33 dscp (011110) == 30 af41 Match packets with AF41 dscp (100010) == 34 af42 Match packets with AF42 dscp (100100) == 36 af43 Match packets with AF43 dscp (100110) == 38

	cs1 Match packets with CS1(precedence 1) dscp (001000) == 8 cs2 Match packets with CS2(precedence 2) dscp (010000) == 16 cs3 Match packets with CS3(precedence 3) dscp (011000) == 24 cs4 Match packets with CS4(precedence 4) dscp (100000) == 32 cs5 Match packets with CS5(precedence 5) dscp (101000) == 40 cs6 Match packets with CS6(precedence 6) dscp (110000) == 48 cs7 Match packets with CS7(precedence 7) dscp (111000) == 56 default Match packets with default dscp (000000) == 0 ef Match packets with EF dscp (101110) == 46
dst=<ip address>[/<prefix length>]	Matches the packets with destinations from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32
dstport=<port>[:<port>]	An alias for the destination-port command.
port=<port>[:<port>]	Matches a single port or series of ports (source or destination). The port can be expressed as a single port or as a range. <port> can be a number or a well known port name, for example, ssh.
precedence=<prec-value>	Matches a precedence value from 0 to 7. They can be specified by name too. Cannot be used with dscp command in a single match. <prec-value> can be a number from 0 to 7 or one of the following names: critical, flash, flash-override, immediate, internet, network, priority, routine.
priority=<vlan user priority>	Matches VLAN traffic with a VLAN user priority equal to the specified value. This number must be from 0 to 7.
source-port=<port>[:<port>]	Matches a single port or range of source ports. The port can be specified as a name from the well-recognized list of port names, for example, ssh.
src=<ip address>[/<prefix length>]	Matches the packets with source addresses from the specified list of ip addresses. An ip address can have an optional mask. <ip-address>[/<prefix length>] := X.X.X.X /M, where X is a decimal number from 0 to 255 and M is a decimal number from 0 to 32
srcport=<port>[:<port>]	An alias for the source-port command.
tos=<tos-value>	Matches a TOS value, from 0 to 15. Can be specified as a name too. Cannot be used with dscp command in a single match. <tos-value> can be a number from 0 to 15 or one of the following names: max-reliability, max-throughput, min-delay, min-monetary-cost, normal. tos=<tos-value><tos-value> := <number> | max-reliability | max-throughput | min-delay | min-monetary-cost | normal
ip	Specifies that the vlan packet encapsulates an IP packet. If this is specified then it can be followed by any expression that is valid for the match ip command (see above).
tcp	Specifies that the vlan packet encapsulates a TCP packet. If this is specified then it can be followed by any expression that is valid for the match tcp command (see below).
udp	Specifies that the vlan packet encapsulates a UDP packet. If this is specified then it can be followed by any expression that is valid for the match udp command (see below).

Examples

Here are examples of using the **match vlan** command:

```
class-map match-any cmap0
match vlan priority=3 udp src=11.24.174.59/32 source-port=28406 dst=181.20.240.119/32
destination-port=63049 precedence=flash-override
match vlan id=726 udp src=54.195.30.128/32 dst=208.114.98.22/32 destination-port=12270
tos=7
match tcp src=196.87.26.102/10 source-port=30422 dst=76.125.32.31/2 destination-
port=42571 tos=7
match udp src=75.83.226.82/28 dst=93.20.122.177/14 destination-port=49707 tos=3
match ip dst=94.47.230.18/32 tos=14
```

max-reserved-bandwidth

Mode

Local-site router interface configuration
`host(config-local-site-router-if)#`
Local-site router interface configuration
`host(config-local-site-router-pif)#`
Site router interface configuration
`host(config-site-router-if)#`
Site router peer-interface configuration
`host(config-site-router-pif)#`

Usage Guidelines

An interface defaults to only allowing 75 percent of its bandwidth for policy-maps and classes if max-reserved-bandwidth is not used to adjust this limit. This value is used when determining whether sufficient bandwidth is available on an interface when used with other queue allocation commands in policy-map classes, such as **priority** and **bandwidth**. To change the percentage of interface bandwidth allocated for use with policy-maps and classes, use the **max-reserved-bandwidth** command. A default value of 75 percent is applied to each interface you create.

This command is available in the interface and peer-interface context. The default value is not displayed when using the **show config** command, but can be displayed with the **show** command.

max-reserved-bandwidth *percent*
no max-reserved-bandwidth *percent*

Syntax Description

percent	Specifies the percentage of the interface capacity to reserve. Range: 1 – 100%. Default: 75%

Example

The following example sets the maximum reserved bandwidth for the interface to be 70%:

```
interface Serial1/0
      max-reserved-bandwidth 70
```

measure-bandwidth

Mode

Monitor-queuing-map Configuration
`host(config-mqmap)#`

Usage Guidelines

To enable Corvil Bandwidth measurement, use the **measure-bandwidth** command. The optional keywords enable detection of events using the configured bandwidth or percentage threshold, and triggering an event if this threshold is met or exceeded. The QoS target values used for Corvil Bandwidth calculation are those defined by queuing-targets in the associated monitor-queuing-map, or the associated monitor-queuing-map's assumed default values for queuing-targets. The **no** version of this command disables Corvil Bandwidth measurement.

measure-bandwidth [event-threshold **{bandwidth** *kbps* **| percent** *percent***}**
no measure-bandwidth

Syntax Description

kbps	Specifies the event threshold bandwidth value in kilobits per second. Range: 1-10000000 kbps. No default.
percent	Specifies the event threshold bandwidth value as a percentage of the link rate. Range: 1-1000% Default: 100%

Examples

To enable Corvil Bandwidth measurement without any configured thresholds, use the following:

```
measure-bandwidth
```

To enable Corvil Bandwidth measurement with an event threshold to trigger event detection when the measured Corvil Bandwidth is 1024 kbps, use the following:

```
measure-bandwidth event-threshold bandwidth 1024
```

To enable Corvil Bandwidth measurement with an event threshold to trigger event detection when the measured Corvil Bandwidth is 80% of the link rate, use the following:

```
measure-bandwidth event-threshold percent 80
```

In this example monitor-queuing-map, event detection is triggered when the measured Corvil Bandwidth is 66% of the link rate:

```
monitor-queuing-map high-priority
```

```
measure-microburst milliseconds 5 event-threshold percent 100
queuing-targets delay-milliseconds 50
size-for percent-packets 99 busy-period hours 1
estimate-service-level event-thresholds delay loss
measure-bandwidth event-threshold percent 66
```

measure-microburst

Mode

Monitor-queuing-map Configuration
`host(config-mqmap)#`

Usage Guidelines

The system provides the ability to measure peak bit-rates over user-specified timescales. When configured, the microburst feature displays three peak plots on the same bit-rate graph. Two of the plots are defined for fixed measurement intervals. The third plot is user-configurable.

Peak bit-rates will be made available for the following objects:

- Interfaces
- Classes
- Applications and flow peaks can only be generated where a nested application class has been configured.

To enable microburst measurement and define the microburst measurement interval, use the **measure-microburst** command. There is an optional switch to basic or 'raw' microburst measurement. There are also optional keywords to enable detection of events using the configured bandwidth or percentage threshold, and triggering an event if this threshold is met or exceeded. The **no** version of this command disables variable peak measurement.

measure-microburst [raw] milliseconds *msecs* **[event-threshold { bandwidth** *kbps* **| percent** *percent* **}]**
no measure-microburst

Syntax Description

raw	Specifies basic microburst measurement, disabling shaping detection. We recommend that you leave the shaping detection feature enabled, because it allows you to identify traffic from a remote site to the local site that is being shaped. For example, if you are monitoring a 2 Mbps link from a remote site, and the measured microburst values are flat-lining at a lower rate, say 1 Mbps, then the traffic from the remote site to the local site is being shaped to this rate.
msecs	Specifies the peak-rate measurement value in milliseconds. Range: 1 – 10000. Default: 50
kbps	Specifies the event threshold bandwidth value in kilobits per second. Range: 1-10000000 kbps. No default.
percent	Specifies the event threshold bandwidth value as a percentage of the link rate.

	Range: 1-1000%. Default: 100%

Examples

To enable microburst measurement with a resolution of 50 milliseconds, use the following:

```
measure-microburst milliseconds 50
```

To enable microburst measurement with an event threshold to trigger event detection when the measured microburst is 1024 kbps, use the following:

```
measure-microburst event-threshold bandwidth 1024
```

To enable microburst measurement with an event threshold to trigger event detection when the measured microburst is 80% of the link rate, use the following:

```
measure-microburst event-threshold percent 80
```

In this example monitor-queuing-map, event detection is triggered when the measured 5 millisecond microburst reaches the link rate:

```
monitor-queuing-map high-priority
  measure-microburst milliseconds 5 event-threshold percent 100
  queuing-targets delay-milliseconds 50
  size-for percent-packets 99 busy-period hours 1
  estimate-service-level event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
```

measure-ping

Mode

Monitor-end2end-map Configuration
`host(config-me2emap)#`

Usage Guidelines

To enable ping measurements for monitoring end-to-end connections between the local site and remote sites, use the **measure-ping** command. The optional keywords determine the ping attributes and enable detection of events if configured thresholds for delay or loss of ping packets. The **no** version of this command disables ping measurement.

measure-ping [interval-milliseconds *msecs***] [size-bytes** *bytes***]**
[availability-threshold <*packets*>**]**
[event-thresholds [delay-milliseconds *dmsecs***] [loss]]**
no measure ping

Syntax Description

msecs	Specifies the number of milliseconds in the interval between ping packets. Range: 500-1000000 msecs. Default 10000 msecs.
bytes	Specifies the IP layer size of the ICMP ping packet. Range: 36-1500 bytes. Default: 36 bytes.
packets	Specifies the number of consecutive ICMP ping packets dropped before the site is considered unavailable. Range: 1-100 packets Default: 10 packets
dmsecs	Specifies the number of delay milliseconds. Range: 1-10000 ms. No default.
loss	Specifies that and event is raised if any packet loss occurs. No default.

Examples

To enable default end-to-end ping measurement without any configured thresholds, use the following:

```
measure-ping
```

To enable end-to-end ping measurement with an event threshold to trigger event detection when delay exceeds 500ms, use the following:

```
measure-ping event-thresholds delay-milliseconds 500
```

To enable end-to-end ping measurement with an event threshold to trigger event detection in case of packet loss, use the following:

```
measure-ping event-thresholds loss
```

monitor-queuing

Mode

Policy-map configuration
`host(config-pmap)#`
Policy-map Class configuration
`host(config-pmap-c)#`

Usage Guidelines

To create a policy-map or class entry for a previously configured monitor-queuing-map, use the **monitor-queuing** command. To remove a policy-map or class entry for a monitor-queuing-map, use the **no** form of this command.

You configure measurement of the parameters specified by a monitor-queuing-map by applying the latter with a **monitor-queuing** command inside a policy-map, for example:

```
policy-map pmap
      monitor-queuing mq1
      class cls
            monitor-queuing mq1
```

It is important to note the positioning of **monitor-queuing** commands within a policy-map. For example, in the following policy-map's configuration the indentation of the fragment suggests that the user intends for the monitor-queuing-map named mq1 to apply to the policy-map as a whole. But the last line is interpreted as part of the class named cls, and not part of the policy-map context:

```
policy-map pmap
      class cls
            bandwidth percent 10
      monitor-queuing mq1
```

This results in mq1 being applied to class cls only. To achieve the desired effect, you insert an explicit exit command between the bandwidth and monitor-queuing commands. For greater clarity, the **monitoring-queue mq1** command should be placed in the policy-map before any class configuration, as shown below:

```
policy-map pmap
      monitor-queuing mq1
      class cls
            bandwidth percent 10
```

Although a monitor-queuing-map enables Corvil Bandwidth and service-level estimation, these quantities are not always computed. In particular, they are never computed at the interface level and they are never computed in any class on peer-interfaces or a local site (inbound direction of an interface from the perspective of a site (regardless of local or remote). Nevertheless, there is no restriction on the use of monitor-queuing-maps in these contexts; where bandwidth and service-level targets are specified, they will generate a warning to the user that they cannot be applied, and will be ignored.

When a configuration containing these inappropriate applications of QoS-targets are reloaded, the warnings will be reissued.

There is a single global default monitor-queuing-map which cannot be deleted. It is named monitor-queuing-default by analogy with class-default. If no monitor-queuing command is used within a class, the default is applied. If no monitor-queuing command is used within policy-maps, no monitor-queuing is applied. That is, the following configuration fragment

```
policy-map pmap
  class cls
```

results in the same policy-map being created as the more explicit one

```
policy-map pmap
  no monitor-queuing
  class cls
   monitor-queuing monitor-queuing-default
```

The parameters of monitor-queuing-default can be changed with the **monitor-queuing-map** command. For example, the default peak-rate timescale can be changed to 100ms with the following CLI fragment:

```
monitor-queuing-map monitor-queuing-default
  measure microburst milliseconds 100
```

Note that this also disables peak-rate triggers by default.

The default QoS-targets will be most useful when they configure all the possible QoS measurements, but such a broad configuration will not be appropriate in all contexts.

Warnings on inappropriate application of QoS-targets are generated only for user-created monitor-queuing-maps, and never for monitor-queuing-default.

monitor-queuing *name*
no monitor-queuing *name*

Syntax Description

name	Specify the name of the previously configured monitor-queuing-map (case-sensitive) to be referenced in the policy-map or class.

Example

In this example, having created a monitor-queuing-map called mqm and a policy-map called pmap_1, a policy-map entry for class_map1 is created:

```
monitor-queuing-map mqm
  measure microburst milliseconds 150
  measure-bandwidth
  measure congestion-indicator
  queuing-targets delay milliseconds 150
  size-for percent-packets 98 busy-period minutes 30

policy-map p_map1
  monitor-queuing mqm
```

monitor-end2end-map

Mode

Monitor-end2end-map Configuration
`host(config-me2emap)#`

Usage Guidelines

To create a monitor-end-to-end-map context with the specified unique name, use the **monitor-end2end-map** command. Applying this map in a policy-map measures the end-to-end quality of the network between two sites. Use the **no** version of this command to remove the specified monitor end2end map context.

monitor-end2end-map <*name*>
no monitor-end2end-map <*name*>

Syntax Description

name	Specifies a unique name for the monitor end2end map.

Examples

To create a new monitor-end2end-map, in this case named “low-speed”, use the following:

```
monitor-end2end-map low-speed
```

To enter the context of an existing monitor end2end map, in this case named “high-speed” to edit the configured parameters, use the following:

```
monitor-end2end-map high-speed
```

monitor-queuing-map

Mode

Monitor-queuing-map Configuration
`host(config-mqmap)#`

Usage Guidelines

To create a monitor-queuing-map context with the specified unique name, use the **monitor-queuing-map** command. Applying this map in a policy-map enables quality measurement features for an interface. When you are in monitor-queuing-map configuration mode, you can configure the following:

Microburst measurement – see the **measure-microburst** command.
Corvil Bandwidth and Bandwidth Sizing measurement – see the **measure-bandwidth**, **queuing-targets** and **size-for** commands
Expected Delay and Loss (service-level estimation) – see **estimate-service-level** command
Congestion Indicator measurement – see **estimate-service-level** and **size-for** commands
Queuing targets – see **queuing-targets** command

Use the **no** version of this command to remove the specified monitor-queuing-map.

monitor-queuing-map <*name*>
no monitor-queuing-map <*name*>

Syntax Description

name	Specifies a unique name for the monitor-queuing-map.

Examples

To create a new monitor-queuing-map, in this case named “low-speed”, use the following:

```
monitor-queuing-map low-speed
```

To enter the context of an existing monitor-queuing-map, in this case named “high-speed” to edit the configured parameters, use the following:

```
monitor-queuing-map high-speed
```

The following is an example of a complete monitor-queuing-map configuration:

```
monitor-queuing-map high-priority
  measure-microburst milliseconds 5 event-threshold percent 100
  queuing-targets delay-milliseconds 50
  size-for percent-packets 99 busy-period hours 1
  estimate-service-level event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
```

more

Mode

Configuration
`host(config)`

Usage Guidelines

To list the contents of files on the BQM file system, use the **more** command. If you are logged in as an admin user you can list files from the following file-systems: log: and cfg: : The config user can only list the contents of the cfg: file system.

more { log: | cfg]}[<*file-url*>**]**

Syntax Description

file-url	Specifies the name of the file to displays

Example

In this example, the specified configuration file in the cfg: directory on the file system is listed:

```
host(config)$ more cfg:bqm_2006-08-16-125812.cfg
!
!
!
!
!
!
!
port PortA
  ethernet auto
port PortB
  ethernet auto
port PortC
  ethernet auto
port PortD
  ethernet auto
port mgmt
  ethernet auto
!
!
!
!
service telnet
service http
service snmp
!
!
no snmp-server enable traps email
no snmp-server enable traps syslog
```

```
no snmp-server enable traps
!
!
!
snmp-server enable traps syslog destination 127.0.0.1
!
!
clock timezone UTC
end
```

no

Mode

All configuration modes

Usage Guidelines

To delete an object or entry, use the **no** command. An object that is being used by another object cannot be deleted. The ***** parameter is only available for the **capture**, **class-map**, **match**, **monitor-end2end-map, monitor-queuing-map, policy-map**, **interface** and **site** commands in configuration mode. For example, **no service-policy *** is not accepted. Partial maps are allowed in some cases, for example, **no class-map cm*** deletes all class-maps that match 'cm*'.

no <command> [*]

Syntax Description

<command>	Specify the full object name to be deleted.
*****	Use this wildcard to create a 'delete all' command. Only works with some commands such as **class-map, match,** and **policy-map**.

Examples

To illustrate the use of the **no** command, we'll first create a new class-map, and then delete it with the **no** command. In this example, class_map1 is created using the **class-map** command:

```
host(config)# class-map class_map1
host(config-cmap)# match udp src=172.18.12.1
host(config-cmap)#
```

Here you can see the results, using the show command:

```
host(config)# show
class-map class_map1 (match-any)
   type (match-any)
   match udp src=172.18.12.1/32
```

Now, to delete class_map1, use the **no** command:

```
host(config)# no class-map class_map1
```

Using the **show** command again, you can see that class_map1 has been successfully deleted:

```
host(config)# show
host(config)#
```

In this example, you can see how to 'delete all' using the no class-map * command. First, you can see that currently there are three class-maps. You issue the no class-map * command and you can see that all three class-maps have been deleted:

```
host(config)# show
class-map class-default (match-any)
   type (match-any)
   match any
class-map medium (match-any)
   type (match-any)
   match tcp destination-port=ftp(21)
   match tcp destination-port=telnet(23)
   match tcp destination-port=smtp(25)
   match tcp destination-port=pop3(110)
class-map voip (match-any)
   type (match-any)
   match udp dst=192.1688.10.1/32
   match udp dst=192.1688.11.1/32
host(config)# no class-map *
host(config)# show
host(config)#
```

ntp

Mode

Configuration

Usage Guidelines

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command. This commands set the key for access to trusted time sources. No servers are configured by default. If a server is configured, by default NTP support for version number 4 and 3, no authentication key is used.

ntp server { [*IP address* | *hostname*] [**prefer**] }
no ntp server *IP address* | *hostname*]

Syntax Description

IP address	Specify the IP v4 dotted decimal address of the server providing the clock synchronization .
hostname	Specify the DNS host name of the server providing the clock synchronization .
prefer	Specifies that the server is referenced in this command is preferred over other configured NTP servers.

Example

In this example, the **ntp** command is used to switch on time synchronization using the server with IP address 192.168.128.4:

```
host(config)# ntp server 192.168.128.4
host(config)#
```

password

Mode

All

Usage Guidelines

To set your login password, use the **password** command. Additionally, the admin user can change the monitor and config users' passwords. Valid passwords comprise a mixture of between five and eight upper and lowercase, alphanumeric and non alphanumeric characters.

You can also use the **password** command to configure a password for packet capture.

password [<*username*>**]**

Syntax Description

username	As the admin user, specify the username whose password you want to change. The supported users are as follows: admin, config or monitor. The monitor user is for GUI use only. CLI login is not possible with this user name.

Example

Use the following to change the config user password:

```
host(config)# password config
Changing password for config
Old password:
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:
password: The password for config has been changed.

host(config)#
```

peer-interface

Mode

Local-site router configuration
`host(config-local-site-router)#`
Site router configuration
`host(config-site-router)#`

Usage Guidelines

When you are constructing the network model for MPLS VPN, Internet VPN, Private VPN deployments, you need to specify the PE router interface to which a given site router interface is connected. To specify a peer interface for a router to measure traffic output from a data center to a site, you use the **peer-interface** command. You use the **service-policy** command to attach a traffic policy to the model peer interface. See the **service-policy** command for more information.

The BQM measurement interface names PortA, PortB, PortC and PortD are fixed and cannot be deleted.

peer-interface <*interface name*>
no peer-interface <*interface name*>

Syntax Description

interface name	Specifies a name for the model peer interface.

Examples

In this MPLS VPN, Internet VPN, Private VPN deployment example, interface and associated peer interface pairs are defined for each configured site:

```
local-site dataCenter
      subnet 192.168.5.0/24

  router core1

      interface FastEthernet0
            description “Link to Provider MPLS cloud”
            bandwidth 10000
            service policy output mpls-policy
      peer-interface FastEthernet0
            description “interface on PE router”
            bandwidth 10000
            service policy output pe-policy

site siteA
      subnet 192.168.1.0/24
      ping-address 192.168.1.3
```

```
      router stab1

            interface Serial0/1
                  description “Link to provider mpls cloud”
                  bandwidth 512
                  service policy output low-speed
            peer-interface Serial0/1
                  description “interface on PE router”
                  bandwidth 512
                  service policy output pe-policy

site siteB
      subnet 192.168.2.0/24
      ping-address 192.168.2.3

      router stab2

            interface Serial0/1
                  description “Link to provider mpls cloud”
                  bandwidth 256
                  service policy output low-speed
            peer-interface Serial0/1
                  description “interface on PE router”
                  bandwidth 256
                  service policy output pe-policy
```

ping

Mode

All

Usage Guidelines

To verify the physical connection to a different network appliance, use the **ping** command **ping** command uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. The **ping** command works only from the management (mgmt) port. It does not send packets on the PortA, PortB, PortC, or PortD measurement ports. The pings will continue until you type Ctrl+C.

```
ping [ip] {ip-address} [data [hex-data-pattern] | df-bit
            | [repeat <repeat-count>] | [size <datagram-size>]
            |[source <source-address>] [timeout <seconds>]]
```

Syntax Description

ip <*ip address*>	Specifies the target IP v4 address. Only IP Addresses are supported. This release does not support the use of names with commands.
data <*hex-data-pattern*>	Specifies the data pattern. <0 – FFFF>, no default
df-bit	Enables the "do-not-fragment" bit in the IP header. Default off
repeat <*count*>	Specifies the number of ping packets that will be sent to the destination address. <1-2147483647>, default 5
size <*datagram-size*>	Specifies the size of the datagram. <36-1500>, default 56
source <*source-address*>	Specifies the source ip address. Only IP Addresses are supported. This release does not support the use of names with commands.
timeout <*seconds*>	Specifies the timeout interval. <0-3600>, default 2

Example

In this example, the connection to the router with IP address 10.10.10.10 is verified:

```
host(config)# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.168 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.174 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.174 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=64 time=0.161 ms
```

```
--- 10.10.10.10  ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.161/0.169/0.174/0.010 ms
host(config)#
```

ping-address

Mode

Site configuration
`host(config-site)#`

Usage Guidelines

The BQM generates end-to-end traffic performance statistics based on ICMP round trip times to a specified host address on a site subnet. To specify an always-available ICMP responder host address on the defined site subnet, use the **ping-address** command.

The host address may be for a router or a subnet host, but it is recommended to use an always-available host address. This is because a busy router may deprioritize ICMP requests and thus contribute to inaccurate round trip results. If a router interface address is used it should be the LAN interface address.

ping-address <*host address***>**

Syntax Description

<*host address*>	Specifies the target always-available host address on a site subnet. Only IP Addresses are supported. This release does not support the use of names with commands.

Example

In this example, the address 192.168.1.3 is used for the subnet ping address on which to base round trip ICMP measurements:

```
site siteA
      subnet 192.168.1.0/24
      ping-address 192.168.1.3
      router stab1

            interface Serial0/1
                  description “Link to data center”
                  bandwidth 512
                  service policy output low-speed
                  connects-to DataCenter core1 Serial0/1
```

policy-map

Mode

Configuration
`host (config)#`

Usage Guidelines

To create a new policy-map, use the **policy-map** command.

The main purpose of a policy-map is to reference a set of class-maps and a monitor-queuing-map. A policy-map may contain a number of class-maps, each with its own class-specific features. A packet traverses the class-maps in the order in which the class-maps appear in the policy-map, and, by default, is consumed by the first class-map that matches the packet. For example, if a policy-map contains a class-map for http traffic, followed by a second class-map for tcp traffic then any http packets will only match with the http class-map. For more information on how to configure class-maps, see the **class-map** command section.

The following restrictions apply when working with policy-maps:

- A policy-map may contain at most one class with a priority command – where you model the priority queue in an LLQ scheduling system.
- A policy-map when attached to an interface cannot utilize more bandwidth than available on an interface. That is, it cannot utilize more than 100% of a link or more capacity (in kbps) than the link has available.

policy-map <*policy-map name*>
no policy-map <*policy-map name*>

Syntax Description

policy-map name	Specify a unique name for the new policy-map.

Examples

The following example creates a policy-map called policy1 and configures two class policies included in that policy-map. The class policy called class1 specifies policy for traffic that matches the configured source IP address.

```
! The following commands create class-map class1 and defines its match criteria:
class-map class1
  match ip src=192.168.10.1

! The following commands create the policy-map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1

class class1
  bandwidth 2000
```

```
queue-limit 40
```

All traffic that fails to meet the matching criteria belongs to the default traffic class (class-default). The default traffic class is user-configurable, but the default traffic class cannot be deleted.

port

Mode

Configuration
`host(config)#`

Usage Guidelines

To enter port configuration mode, use the **port** command. You can then use the **ethernet** command to change port duplex and speed parameters. This is how the Ethernet settings for the physical ports are configured.

port *port_name*

Syntax Description

port_name	Specify the BQM port to be configured: the physical measurement ports (PortA, PortB, PortC, PortD) or the management port (mgmt).

Example

In this example, the **port** command is used to enter port configuration mode for the PortA measurement interface:

```
host(config)# port PortA
host(config-port)# show
ethernet auto
```

ppp

Mode

Site router interface configuration
```
host (config-site-router-if)#
```

Usage Guidelines

Priority network traffic, such as VoIP packets, can suffer long delays due to the time taken to serialize large packets onto slow links. For example, on a 56 kbps serial line, it takes over 200 ms to serialize a 1500-byte packet. A recommended end-to-end delay for VoIP packets is just 150 ms. To solve this problem it is necessary to use packet fragmentation mechanisms such as Cisco's Link Fragmentation and Interleaving (LFI). The system models LFI scheduling, fragmenting large data packets into smaller ones and interleaving voice packets among the fragments reduces jitter and delay.

The configured LFI value represents the maximum tolerable delay to be incurred by fragmented packets. The packet fragment size for fragmenting classes is based on the required delay. Cisco recommends fragmenting data packets to sizes that incur no more than a 10-millisecond delay. LFI configuration is typically only applied to links less than dedicated half-T1 (768 kbps). Although you can enable LFI for a WFQ or FIFO (single-class WFQ) scheduler, no fragmentation or interleaving actually occurs. Therefore the Corvil Bandwidth will not change with LFI enabled on an interface with either WFQ or FIFO schedulers enabled. For voice applications, the recommended serialization delay on a per-hop basis is 10 ms and should not exceed 20 ms.

To utilize fragment delay on a Multilink PPP (MLP) bundle, the **ppp multilink interleave** command must first be used to enable the functionality. This command uses a default value of 30 ms, which may then be modified by use of the **ppp multilink fragment delay** command. To reset the maximum delay to the default value, use the no form of the **ppp multilink fragment delay** command. To disable fragment delay, use the no form of the **ppp multilink interleave** command. Note that use of the **ppp multilink fragment dela***y* command without a preceding **ppp multilink interleave** command will generate an error. Similarly, use of the no option must be in ordered sequence with the fragment delay value removed first and then interleave disabled. This command is available from the site router interface configuration context.

ppp multilink {interleave **|** fragment delay *delay max*}
no ppp multilink {interleave **|** fragment delay *delay max*}

Syntax Description

interleave	Interleave must be specified before fragment delay. When interleave is switched on the fragment delay defaults to 30 milliseconds.
fragment delay *delay max*	Maximum amount of time, in milliseconds, that should be required to transmit a fragment. The range is from 1 to 1000 milliseconds.

Example

The following example requires an interface to have a maximum bound on delay of 20 milliseconds:

```
interface Serial1/0
ppp multilink interleave
ppp multilink fragment delay 20
```

priority

Mode

Policy-map Class configuration
`host (config-pmap-c)#`

Usage Guidelines

To allocate a certain amount of guaranteed bandwidth to a class, use the **priority** command in policy-map class configuration mode. This command is used to model low latency queuing (LLQ), providing priority queuing (PQ) for class-based weighted fair queuing (CBWFQ) configured on the router. This allows delay-sensitive data such as voice to be sent before packets in other queues. The unit for the **priority** command in the priority class can be different from the bandwidth unit of the non-priority class. The following restrictions apply when using the priority command:

- A policy-map class containing a **priority** command cannot contain a **bandwidth** command.
- The **priority** command is not allowed in a class-default class.

priority {*bandwidth-kbps* | percent *percentage*} [burst]
no priority {*bandwidth-kbps* | percent *percentage*} [burst]

Syntax Description

bandwidth-kbps	Guaranteed allowed bandwidth, in kbps, for the priority traffic. The amount of guaranteed bandwidth varies according to the interface in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the non-priority traffic is not starved. Range: 8 – 2000000 kbps
percent *percentage*	Specifies that the amount of guaranteed bandwidth will be specified by the percentage of available bandwidth. The percentage can be a number from 1 to 100. Range: 1 – 100%
burst	Specifies the burst size in bytes. The burst size configures the system to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. Range: 32 to 2000000 bytes.

Example

Here is an example of using the **priority** command to set the class named ‘voice’ as the priority class in the policy-map. The other classes specified are all bandwidth classes with proportionate shares of the remaining available bandwidth:

```
policy-map priority_voice
  class voice
    priority 1000 burst 250
  class transact
    bandwidth remaining percent 15
  class best-effort
    bandwidth remaining percent 10
  class class-default
```

priority-level

Mode

Policy-map class configuration
`host (config-pmap-c)#`

Usage Guidelines

To specify a strict priority level (high, medium, normal or low) for a class, use the **priority-level** command. Note that the implicit class 'class-default' uses the 'normal' priority level unless specified differently. To remove a previously specified `priority-level` for a class, use the no form of this command.

The following restrictions apply when using the **priority-level** command:

- If multiple priority queues are defined, then no `bandwidth`, `priority kbps` or `priority percent` *`percentage`* commands are permitted.
- If multiple `priority-level` queues are defined then associated queue sizes with the Cisco defaults of 20, 40, 60 and 80 for `high`, `medium`, `normal` and `low`, respectively, are assumed, unless otherwise specified.
- No more than a single instance of each `priority-level` queue shall be allowed in each policy-map, that is, a policy-map cannot have the same level appear twice in a policy-map.
- Only a single policy-map class can be mapped to a `priority-level` queue.
- Unless otherwise specified, a class `class-default` in a policy-map is assumed to be associated with a `normal` priority queue.

priority-level {high | medium | normal | low}
no priority-level {high | medium | normal | low}

Syntax Description

high | medium | normal | low	Specifies the priority level of the class.

Example

Here is an example of using the **priority-level** command to define multiple priority queues:

```
class-map match-all prlist1
      match udp port=69       !TFTP

class-map match-all prlist2
      match udp port=111      !RPC

class-map match-all prlist3
      match tcp port=25       !SMTP
```

```
class-map match-all prlist4
      match udp port=2049     !NFS

class-map match-all prlist5
      match tcp port=23       !Telnet
      match class-map=acllist6

policy-map prp1
      class prlist4
            priority-level high
            queue-limit 30
      class prlist2
            priority-level medium
            queue-limit 60
      class prlist2
            priority-level low
            queue-limit 100

      !assume class class-default will receive normal priority
      !queue unless otherwise specified

policy-map prp2
      class prlist5
            priority-level medium
      class class-default
            priority-level low
```

queuing-targets

Mode

Monitor-queuing-map Configuration
`host(config-mqmap)#`

Usage Guidelines

To configure the delay target for Corvil Bandwidth and Expected Loss and Delay calculation, use the **queuing-targets** command. The **no** version of the command removes any queuing-targets parameters. If the **queuing-targets** command is absent from a monitor-queuing-map (or the **no queuing-targets** command is explicitly added), then Corvil Bandwidth and Expected Delay and Loss calculations will be disabled for any class to which the monitor-queuing-map is applied.

The targets specified here serve as the QoS targets for calculating Corvil Bandwidth and also for Expected Delay and Loss calculation. When these parameters are used as QoS-targets for Corvil Bandwidth, the system calculates the minimum bandwidth required to keep per-packet delay within the delay target and prevent loss due to buffer-overflow.

Using the command **queuing-targets** with no parameters enables loss protection by default.

queuing-targets [delay-milliseconds *msecs*]
no queuing-targets

Syntax Description

delay-milliseconds *msecs*	Specifies the number of milliseconds delay. Range: 5 -10000 kbps. Default: 500

Examples

To configure a delay queuing-target of 150 milliseconds and to enable loss tracking, use the following:

```
host(config–mqm)$ queuing-targets delay-milliseconds 150
```

queue-limit

Mode

Policy-map Class configuration
`host (config-pmap-c)#`

Usage Guidelines

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy-map, use the **queue-limit** command in policy-map class configuration mode. To remove the queue packet limit from a class, use the no form of this command.

A policy-map class containing a **queue-limit** command must have a **bandwidth** command used first, unless used with the **priority-level** command . That is, in order to modify the queue size of any policy-map class, including the class `class-default` either a **bandwidth** or **priority-leve**l command must first be used.

The *Congestion Analysis* tab includes a **Corvil Bandwidth – Queue Length** graph based on the queue length configured for a class using this command. The Corvil Bandwidth values plotted represent the minimum bandwidth required to avoid packet loss due to queue buffer overflow. For example, if the queue length configured for the class is 64 packets, then the graph displays the bandwidth required to prevent the queue for the class traffic building up past 64 packets.

If you do not configure an explicit queue length limit, then the default value of 64 packets is used by the system when calculating the values plotted in the **Corvil Bandwidth – Queue Length** graph.

queue-limit *number-of-packets*
no queue-limit *number-of-packets*

Syntax Description

number-of-packets	Specify the maximum number of packets that the queue for this class can accumulate. Range: 16 – 2000 packets. No default value.

Example

Here is an example of using the queue-limit command:

```
policy-map policy1
 class class1
  bandwidth 1500
  queue-limit 64
```

reload

Mode

Configuration
`host(config)#`
You must be logged in to the BQM as an admin user to use this command.

Usage Guidelines

To reboot the BQM with the current system software, use the **reload** command. If the standby-system-image parameter is used, the command reboots the machine with the version of the software installed on the standby system.

reload [standby-system-image]

Syntax Description

standby-system-image	Reloads the system image from the standby image.

Example

In this example, the system standby image is loaded on reboot:

```
host# reload standby-system-image
```

rename

Mode

Configuration
`host(config)#`

Usage Guidelines

To rename a named class-map, custom application, interface, local-site, monitor-queuing-map, peer-interface, policy-map, router or site, use the **rename** command. Note that *peer-interface* names, because they must align with their corresponding *interface*, are renamed when their associated *interface* is renamed. Similarly a *class* is renamed when their associated *class-map* is renamed.

rename {**class-map** | **custom application** | **monitor-queuing-map** | **policy-map** | **site |** } *old-name new-name*
rename local-site *new-name*
rename router *site-name old-name new-name*
rename interface *site-name router-name old-name new-name*

Syntax Description

site-name	Specifies site for router or interface renaming.
router-name	Specifies site and router name for interface renaming.
old-name	Specifies the old name for class-map, custom application, interface, monitor-queuing-map, policy-map, router or site. Note, not required for local-site as only a single local-site is allowed.
new-name	Specifies the name for the class, class-map, custom application, interface, local-site, monitor-queuing-map, policy-map, router or site. Names comprising more than one word must be enclosed in double quotes (“”).

Example

In this example a router in a site named dublin is renamed from rtr-1 to dubrouter-1:

```
host# rename router dublin rtr-1 dubrouter-1
```

restore

Mode

Configuration
`host(config)`

Usage Guidelines

To restore the BQM configuration and database, and/or capture files from a specified source, use the **restore** command. The source may be an accessible filesystem , an ftp server or a host accessible via ssh or scp. If the restore is via ftp or scp, you are prompted for the username and password. Any restore action will cause the system to be halted during the restore process. The user will be logged out.

In the case of ftp or scp restores, the host name (resolvable via DHCP) or host IP address must be given,

For information on how to back up the system configuration, see the **backup** command.

restore {[**data**] | [**data-with-captures**]} {backup:*filename* | [ftp://[*hostname* | *IP address*]/*filename*] [*user*] [*password*]] | [scp://[*hostname* | *ip address*]/*filename*}[*user*] [*password*]]}

Syntax Description

backup:path	Selects restore from an accessible file system.
ftp://hostname/path	Selects restore from an FTP server.
scp://hostname/path	Selects restore from a remote machine via ssh or scp.
user	Specifies the login username (ftp and scp.)
password	Specifies the login password (ftp and scp).

Example

In this example, the system configuration is restored (without capture files) from a server /tmp directory with IP address 192.16.7.2 using scp where the username and password are also provided:

```
host(config)#restore system-only scp://192.16.7.2/tmp/cfg_bck_090606 admin adminP4sswd
Are you sure you want to restore. This will log you out (y/n)?y
host(config)#
```

router

Mode

Local-site configuration
`host(config-local-site)#`
Site configuration
`host(config-site)#`

Usage Guidelines

When you are the network model for a deployment, you define at least one router for each configured site. To define a router for a site, you use the **router** command. To remove a router from a site you use the no form of the command.

router <*name* >
no router <*name*>

Syntax Description

name	Specify a unique name for the configured site router.

Example

In the following example, each site has a router defined (siteA – stab1; siteB – stab2):

```
site siteA
      subnet 192.168.1.0/24
      ping-address 192.168.1.3

      router stab1

            interface Serial0/1
                  description “Link to data center”
                  bandwidth 512
                  service policy output low-speed
                  connects-to DataCenter core1 Serial0/1

site siteB
      subnet 192.168.2.0/24
      ping-address 192.168.2.3

      router stab2

            interface Serial0/1
                  description Link to data center
                  bandwidth 512
```

```
service policy output low-speed
connects-to DataCenter core1 Serial0/2
```

service

Mode

Configuration
`host (config)#`

Usage Guidelines

To allow network services on the device to be enabled/disabled, use the **service** command. Currently only the telnet, http and snmp services are supported. To disable use the **no** form of the command. By default all services are enabled. This command is saved as part of the startup and running configurations. You can use the **show** command to check the current service status.

service *service-name*
no service *service-name*

Syntax Description

service name	Specify the name of the service to be enabled. Currently only the telnet, http and snmp services are supported.

Example

In this example, the telnet service is enabled:

```
host (config)# service telnet
```

service-policy

Mode

local-site router interface/peer-interface configuration
site router interface/peer-interface configuration

```
host (config-local-site-router-if)#
host (config-local-site-router-pif)#
host (config-site-router-if)#
host (config-site-router-pif)#
```

Usage Guidelines

To attach a policy-map to an interface or peer interface, to be used as the service policy for that interface, use the **service-policy** command. You must specify a direction for the policy that matches the direction of the traffic being seen by the configured interface. To remove a service policy from an interface or peer interface, use the no form of the command. Only a single service-policy may be attached to an interface or peer-interface at any one time.

service-policy output *policy-map-name*
no service-policy output *policy-map-name*

Syntax Description

policy-map name	Specify the name of the configured policy-map to use within the current policy-map.

Example

In this example, having defined a site, router and an interface, a previously defined policy-map named outbound is applied to the interface:

```
host(config)$ site Dublin
host(config-site)$ router local
host(config-site-router)$ interface Serial1/0
host(config-site-router-if)$ service-policy output outbound
```

setup

Mode

All
You can only use this command if you are logged in as an admin user.

Usage Guidelines

To set up the BQM, involving the setup of the BQM IP address, subnet mask, hostname, the adjacent router's IP address, and the IP address of the Domain Name Server (DNS) for DNS name resolution, use the **setup** command. This is automatically run on the first admin login and on subsequent logins if you quit the first setup (**Ctrl+C**) or you do not change the supplied default values.

Syntax Description

This command prompts you for the following information:

`IP address`	Accept the default IP address and prefix (192.0.2.1/24) by pressing Enter or specify an IP address for the BQM. If you specify a prefix length when entering the IP Address, you will be automatically shown the appropriate subnet mask in the next step.
`Netmask`	Accept the default value (255.255.255.0) by pressing Enter or specify a subnet mask for the BQM.
`Router`	Accept the default value (192.0.2.254) by pressing Enter or edit it to specify an IP address for the adjacent router.
`Domain-name-server`	Specify an IP address for DNS name resolution.
`Hostname`	Accept the default hostname (BQM) by pressing Enter or edit it to specify a hostname for the BQM.

Example

Here is an example of using the **setup** command:

```
host(config)$ setup

IP address: 192.10.5.1/24
Netmask: 255.255.255.0
Router: 192.10.5.254
Domain-Name-Server: 192.10.5.1
Hostname: corphq_nyc
```

show

Mode

All

Usage Guidelines

To list the contents of each available context, use the **show** command. It is a recursive listing by default. You can search with wildcards (*) when displaying the entries for captures, class-maps, custom-applications, local-sites, interfaces, monitor-end2end-maps, monitor-queuing-maps, ntp, peer-interfaces, policy-maps, , and sites, The **show config** command displays captures, class-maps, custom-applications, interfaces, local-sites, monitor-end2end-maps, monitor-queuing-maps, ntp, peer-interfaces, policy-maps, ,routers, sites and snmp-server. Hence, whether with the current **show** or with **show config** command, a search can be made for a specific set of named class-maps.

The **show interfaces** and **show peer-interfaces** commands can be used to display the "Top N" talkers, listeners, conversations (flows) and applications (if configured) sorted by bytes on a specified interface or peer-interface respectively.

You can display the versions of software utilized on the device along with details of the devices hardware and configuration using **show version** , and which users are currently active on the device using **show users**.

The **show alerts** command displays BQM alerts on the CLI. The output is sorted by time and then by measurement point.

Allowed combinations are displayed below:

show [-s] [-n]

show alerts [category {monitoring | system}]
[severity {informational | warning | minor | major | severe}]
[timerange{*hour* | *day* | *week* }]

show audit [timerange *hour* | *day* | *week*}]

show [capture | class-map | custom-application | local-sites | monitor-queuing-map | monitor-end2end-map | policy-map | sites | snmp-server [<*name*>[*]]

show config [class-map | custom-application | local-sites | interfaces | monitor-queuing-map | monitor-end2end-map | peer-interfaces | policy-map | sites | snmp-server [<*name*>[*]]

show detailed-config

show faults-info

show file-systems

show interface <*site*> <*router*> <*name*> [stats { [class <*class*>]
[top <*n*>] [applications|conversations|listeners|talkers]
[ascending|descending] }]

show interfaces [<*name*>[*]] [stats { [class <*class*>]
[top <*n*>] [applications|conversations|listeners|talkers]
[ascending|descending] }]

show peer-interface <*site*> <*router*> <*name*> [stats { [class <*class*>]
[top <*n*>] [applications | conversations | listeners | talkers]
[ascending | descending] }]

show peer-interfaces [<*name*>[*]] [stats { [class <*class*>]
[top <*n*>] [applications | conversations | listeners | talkers]
[ascending | descending] }]

show ports

show tech-support

show users

show version

Syntax Description

category	Specifies category of the alerts to display, either monitoring of system alerts. Default to all alert categories.
severity	Specifies severity of the alerts to display. Defaults to all alert severities.
timerange	Specifies time range of alerts or audit trail to display, either last hour, last day or last week. Defaults to all alerts or all audit trails.
-n	Use this switch to show a non-recursive listing of contents.
-s	Use this switch to show an abbreviated listing of contents.
alerts	Displays the current list of alerts on the BQM.
audit	Displays a list of recent changes performed on the BQM.
capture [<*name*>[*]]	Displays the current packet capture status for the selected instance if named, or for all configured packet capture instances if a name is not specified.

	The following information is displayed: • Capture configuration details • current capture status • total size of capture file and size limit • time limit • number of captured/dropped frames The following describes the displayed packet capture status values: Idle – packet capture not active, capture file is closed (or not yet created) Running – packet capture in progress Paused – packet capture has been paused Size reached – packet capture has been stopped because the file size limit has been reached Time reached – packet capture has been stopped because the time limit has been reached.
class-map [<*name*>[*]]	Displays the list of configured class-maps and their associated match rules.
local-site [<*name*>[*]]	Displays the configured local-site details.
custom-application [<*name*>[*]]	Displays the list of configured custom applications.
detailed-config	Displays the detailed current operating configuration.
faults-info	Displays an overview of the enable/disable state of the various faults.
file systems	Displays the used/free space information on the available file system. The information displayed includes the following: • name of file system • total size of file system in KB • free space of file system in KB
interface <*site*> <*router*> <*name*> [stats { [class <*class*>] [top <*n*>] [applications|conversations|listeners|talkers] [ascending|descending] }]	Displays details for a specific named interface, its attached service-policies and classes, where the available parameters are as follows: *site* specifies the name of the site containing the interface. *router* specifies the name of the router containing the interface. *name* specifies the name of a chosen interface. *class* specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.] *n* number of applications, conversations, listeners or talkers to display. Note that fewer items than those requested may be displayed if there are insufficient numbers, [Default: 10] ascending sort display with largest quantity at the top. [Default: ascending]. descending sort display with smallest quantity at the top. [Default: ascending].
interfaces [<*name*>[*]] stats [class<*class*>	Displays the list of configured interfaces, their attached service-policies and

top <*n*> [applications | conversations | listeners | talkers] [ascending | descending]	classes, where the available parameters are as follows: *name* specifies the name of a chosen interface. *class* specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.] *n* number of applications, conversations, listeners or talkers to display. Note that fewer items than those requested may be displayed if there are insufficient numbers, [Default: 10] ascending sort display with largest quantity at the top. [Default: ascending]. descending sort display with smallest quantity at the top. [Default: ascending].
monitor-queuing-map [<*name*>[*]]	Displays the list of monitor-queuing-maps or specific monitor-queuing-map(s) with wildcarding. The monitor-queuing-map(s), if they exist, are displayed.
peer-interface <*site*> <*router*> <*name*> [stats { [class <*class*>] [top <*n*>] [applications|conversations|listeners|talkers] [ascending|descending] }]	Displays details for a specific named peer-interface, its attached service-policies and classes, where the available parameters are as follows: *site* specifies the name of the site containing the peer-interface. *router* specifies the name of the router containing the peer-interface. *name* specifies the name of a chosen interface. *class* specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.] *n* number of applications, conversations, listeners or talkers to display. Note that fewer items than those requested may be displayed if there are insufficient numbers, [Default: 10] ascending sort display with largest quantity at the top. [Default: ascending]. descending sort display with smallest quantity at the top. [Default: ascending].
peer-interfaces [<*name*>[*]] stats [class<*class*> top <*n*> [applications | conversations | listeners | talkers] [ascending | descending]	Displays the list of configured peer interfaces, their attached service-policies and classes, where the available parameters are as follows: *name* specifies the name of a chosen peer interface. *class* specifies an optional class associated with the chosen peer interface [Default: All classes associated with the peer interface.] *n* number of applications, conversations, listeners or talkers to display. Note that fewer items than those requested may be displayed if there are insufficient numbers, [Default: 10]

	ascending — sort display with largest quantity at the top. [Default: ascending]. descending — sort display with smallest quantity at the top. [Default: ascending].
policy-map [<*name*>[*]]	Displays the list of configured policy-maps, and their associated classes.
ports	Displays configured information for the management and measurement ports on the BQM.
routers	Displays the configured router details.
config [class-map|local-site|custom-application|interfaces| monitor-end2end-map|monitor-queuing-map |peer-interfaces|policy-map|sites|snmp-server] [<*name*>[*]]	Displays the current operating configuration or specific class-maps, interfaces, monitor-queuing-maps, peer interfaces, policy-maps, and sites (including associated routers and interfaces) with wildcards.
sites [<*name*>[*]]	Displays the list of sites configured on the BQM.
snmp-server	Displays the current SNMP server configuration details.
tech-support	Displays detailed system status and configuration information for use by technical support. You must be logged in to the BQM as an admin user to use this command.
users	Listing of the currents users using the device. The IP address is shown for CLI users, but not GUI users. If a user is logged in via the serial line, the host column displays 'serial-line'.
version	Detailed description of the device.

Examples

The following examples illustrate the use of some of the **show** command options:

```
host(config)# show class-map

class-map besteffort (match-any)
  match ip dscp=0
class-map bulk (match-any)
  match ip dscp=10
class-map class-default (match-any)
  description "Default class-map"
  match any
class-map critical (match-any)
  match ip dscp=26
  match ip dscp=48
  match ip dscp=24
class-map realtime (match-any)
```

```
  match ip dscp=46
  match ip dscp=40
class-map video (match-any)
  match ip dscp=18
  match ip dscp=16


host(config)# show policy-map

policy-map low_speed
  monitor-queuing low_speed
  class class-default
policy-map mpls_policy
  class realtime
    monitor-queuing low_speed
    bandwidth 25
  class critical
    monitor-queuing low_speed
    bandwidth 20
  class video
    monitor-queuing low_speed
    bandwidth 20
  class bulk
    monitor-queuing low_speed
    bandwidth 10
  class besteffort
    monitor-queuing low_speed
  class class-default
policy-map pe-policy
  class realtime
  class class-default

host(config)# show interfaces

site Local-site, router "core1"
  interface Serial0/1
    description "Link to Remote Site 1"
    bandwidth 512
    max-reserved-bandwidth 75
    service-policy output low_speed
      Traffic Stats  - 0 bps mean, 0 bps 1s peak, 0 bps 5ms peak
                     - 0 bps 50ms peak (configured)
                     - 0 packets, 0 bytes
      class class-default
        Traffic Stats  - 0 bps mean, 0 bps 1s peak, 0 bps 5ms peak
                       - Corvil Bandwidth not configured
                       - 0 bps 50ms peak (configured)
                       - 0 bps 500ms peak (delay-target)
                       - 0 packets, 0 bytes
site Local-site, router "core2"
  interface Serial0/1
    description "Link to Remote Site 1"
    bandwidth 512
    max-reserved-bandwidth 75
    service-policy output low_speed
```

```
      Traffic Stats  - 0 bps mean, 0 bps 1s peak, 0 bps 5ms peak
                     - 0 bps 50ms peak (configured)
                     - 0 packets, 0 bytes
      class class-default
        Traffic Stats  - 0 bps mean, 0 bps 1s peak, 0 bps 5ms peak
                       - Corvil Bandwidth not configured
                       - 0 bps 50ms peak (configured)
                       - 0 bps 500ms peak (delay-target)
                       - 0 packets, 0 bytes
site "Remote Site 1", router "remote1"
-- More --

host(config) # show interfaces FastEth0 stats top 5 applications
site NewYork, router core
  interface FastEth0
    bandwidth 100000
    max-reserved-bandwidth 75
    service-policy output edge-policy
```

To display the current list of users logged in to the BQM, use the **show users** command:

```
host(config)$ show users
        User              Connection    From            Host
        ------------------------------------------------------------
        root              Terminal      Oct 30 09:56    192.16.4.28
        root              Terminal      Oct 30 10:44    192.16.3.74
        admin             Terminal      Oct 10 12:07    192.16.1.171
        config            Terminal      Oct 10 12:08    192.16.1.171
        config            GUI           Oct 10 09:00    -
```

In this example of using wildcards (*), all class-maps which start with the letters “ap” are displayed:

```
host(config)# show config class-map ap*
```

Similar commands can also be performed for policy-maps, interfaces, and sites.

In this example, the **show file-systems** command is used to display the file system information:

```
host(config)# show file systems
File system    Size (KB)       Used  Available  Used%
disk0:         34928452     129208   34799244     0%
host(config)#
```

In this example, the **show capture** command is used to display the information on the configured packet capture instances. In this example, there is a single packet capture instance configured (with default time limit, file size limit and snaplength values), but it is not running:

```
host(config)# show capture
capture ethernet1
  disabled
  size 64 MB (default)
```

```
  snaplength 64 (default)
  duration unlimited (default)
  state: idle
  captured data size: 0B
  captured: packets: 0, len: 0, caplen: 0
  dropped:  packets: 0, len: 0, caplen: 0
```

In the following example, the **show faults-info** command is used to display an overview of the enable/disable state of both quality alarms and system alerts:

```
host(config)# show faults-info
Name                                Snmp Enabled    Syslog Enabled  Email Enabled
Default fault type                  True            True            False
System Shutdown                     True            True            True
System Startup                      True            True            True
Fan Failure                         True            True            True
Fan Failure Clear                   True            True            True
Power Supply Failure                True            True            True
Power Supply Failure Clear          True            True            True
Hard Drive Failure                  True            True            True
Hard Drive Failure Clear            True            True            True
Port Down                           True            True            True
Port Down Clear                     True            True            True
Database Fault                      True            True            True
Database Fault Clear                True            True            True
System Throughput High              True            True            True
System Throughput Clear             True            True            True
License Near Expiration             True            True            True
License Near Expiration Clear       True            True            True
License Expired                     True            True            True
License Expired Clear               True            True            True
License Invalid                     True            True            True
License Invalid Clear               True            True            True
Memory Usage High                   True            True            True
Memory Usage Clear                  True            True            True
Soft Disk Threshold Exceeded        True            True            True
Soft Disk Threshold Clear           True            True            True
Hard Disk Threshold Exceeded        True            True            True
Hard Disk Threshold Clear           True            True            True
Watchdog Restart                    True            True            True
CPU Utilization High                True            True            True
CPU Utilization Clear               True            True            True
CPU Failure                         True            True            True
CPU Failure Clear                   True            True            True
Temperature High                    True            True            True
Temperature High Clear              True            True            True
E2E Delay Threshold Exceeded        True            True            False
E2E Delay Threshold Clear           True            True            False
E2E Loss Detected                   True            True            False
E2E Loss Clear                      True            True            False
E2E Availability Issue              True            True            False
E2E Availability Issue Clear        True            True            False
Congestion Threshold Exceeded       True            True            False
Congestion Threshold Clear          True            True            False
```

```
Micro-Burst Detected                    True            True            False
Micro-Burst Clear                       True            True            False
Corvil Bandwidth Threshold Exceeded     True            True            False
Corvil Bandwidth Threshold Clear        True            True            False
Expected Queuing Loss Threshold Exceeded True           True            False
Expected Queuing Loss Threshold Clear   True            True            False
Expected Queuing Delay Threshold Exce... True           True            False
Expected Queuing Delay Threshold Clear  True            True            False
Expected Policing Threshold Exceeded    True            True            False
Expected Policing Threshold Clear       True            True            False

host(config)#
```

shutdown

Mode

Configuration
`host(config)#`
Port configuration
`host(config-port)#`

Usage Guidelines

To specify which physical monitoring ports are not in use, use the **shutdown** command in port configuration mode. Some BQM deployments will not use all monitoring ports. This allows the system monitoring service to raise an alert if the network link at a non-shutdown port goes down.

Only monitoring ports can be shut down; the management port cannot be shut down.

If a monitoring port is shut down then any traffic arriving at that port is discarded. In practice the situation should not normally occur because only ports that have no physical network link should be shut down.

If the **shutdown** command is used in configuration mode, the BQM will attempt to shut down

shutdown
no shutdown

Syntax Description

This command has no keywords or parameters.

Example

In the following example, physical port PortC is shut down because it is not connected to the network:

```
host(config)$ port portC
host(config-port)$ shutdown
host(config-port)$
```

In the following example, the BQM is shut down:
`host(config)$ shutdown`
`host(config)$` You will have to power-cycle the device to start it up again. Are you sure
you want to shutdown (y/n)?

`If 'y' is input the BQM shall shutdown and a power cycle is necessary to restart it.`

site

Mode

Configuration
`host(config)#`

Usage Guidelines

When you are configuring the network model for a deployment, you define sites. To define a site, you use the **site** command. To remove a site you use the **no** form of the command.

To give a site a name with multiple words, place the name between italics when using the command.

site <*name* >
no site <*name*>

Syntax Description

name	Specify a unique name for the configured site.

Example

In the following example, siteA and siteB are configured:

```
site siteA
      subnet 192.168.1.0/24
      ping-address 192.168.1.3

      router stab1

            interface Serial0/1
                  description “Link to data center”
                  bandwidth 512
                  service policy output low-speed
                  connects-to DataCenter core1 Serial0/1

site siteB
      subnet 192.168.2.0/24
      ping-address 192.168.2.3

      router stab2

            interface Serial0/1
                  description “Link to data center”
                  bandwidth 512
```

```
service policy output low-speed
connects-to DataCenter core1 Serial0/2
```

size

Mode

Configuration
`host(config-capture)`

Usage Guidelines

To set the packet payload size limit for a selected packet capture instance, use the **size** command in capture configuration mode. If you do not specify a size limit using the **size** command, the packet capture size limit is determined by available disk space. You can the **capture-settings** command to set the proportion of disk space available for manual packet capture. To reset the size limit for a selected packet capture instance to the default value, use the no form of the command. If you specify a file size when using the **no size** command, the file size value is ignored.

size <*size*>
no size [<*size*>**]**

Syntax Description

size	Specifies the file size limit in megabytes. Allowed range: 1 – 64000 MB Default: None

Example

In this example, the packet capture instance is defined, attached to an interface and has a time limit and file size limit of 1GB applied:

```
host(config)# capture serial1
host(config-capture)# attach interface serial1 output
host(config-capture)# size 1000
host(config-capture)# duration 60
```

In the following example, the capture file size limit from the previous example configuration is increased to 10GB:

```
probe(config)# capture serial1
probe(config-capture)# size 10000
```

size-for

Mode

Configuration
`host(config-mqmap)`

Usage Guidelines

To calculate bandwidth-sizing based on Corvil Bandwidth, use the **size-for** command when defining a monitor-queuing-map. The *percent-packet* parameter allows the user to permit a fraction of the packets during the defined *busy-period* to violate the configured queuing-targets. Permitting a certain fraction of the packets to violate the queuing targets allows a statistical softening of the required bandwidth down from that needed to guarantee no loss or delay for every single packet.

You use the *busy-period* parameter to specify the period of time that has been identified for the network as seeing the most traffic. So if the network busy period has been identified as 30 minutes, you will want to make sure that the sizing calculation takes every 30-minute period of traffic into account. The resulting sizing calculation is sufficient to ensure that the QoS-targets are met for the configured fraction of packets over any consecutive period of length *busy-period*. For example, if *percent-packets* is set to 99% and *busy-period* is set to 30 minutes, and bandwidth-sizing is carried out for a 24-hour period, then the resulting size value guarantees that over each of the 210 groups of six consecutive 5-minute periods that fit entirely within the full 24 hours, no more than 1% of the packets that arrive during any given half-hour period are delayed by more than the defined delay-target.

size-for percent-packets *percent* **busy-period {minutes** *mins* **| hours** *hours* **| day | week}**
no size-for

Syntax Description

percent	Specifies the percentage of packets allowed to exceed the configured queuing targets during the specified busy-period. Range: 0.0-100.0000%. (Six significant figures) Default: 99%.
mins	Specifies the number of minutes in the busy period. Range: 5–1440 minutes. Values allowed: 5, 60, 120, 240 minutes. Default: 60 minutes.
hours	Specifies the number of hours in the busy period. Values allowed: 1, 2, 4 hours. Default: 1 hour.
day	Specifies the number of days in the busy period. Values allowed: 1

	Default: none
week	Specifies the number of weeks allowed in the busy period. Values allowed: 1 Default: none

Example

In this example monitor-queuing-map, bandwidth sizing is calculated such that 99% of packets in every one-hour period are protected from loss and are delayed by no more than 50 milliseconds (see the queuing-targets configuration):

```
monitor-queuing-map high-priority
  measure-microburst milliseconds 5 event-threshold percent 100
  queuing-targets delay-milliseconds 50
  size-for percent-packets 99 busy-period hours 1
  estimate-service-level event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
```

snaplength

Mode

Capture configuration mode
`host(config-capture)#`

Usage Guidelines

To configure the number of bytes captured from the beginning of the Ethernet frame, use the **snaplength** command. You can use this command to limit the snapshot length for the selected packet capture instance. To remove the snapshot length limit for the selected packet capture instance, use the **no snaplength** command. With snapshot length set to zero, only packet headers will be stored. If you do not set a limit using this command, the default snapshot length of 38 bytes is used by the system. Configure a value of zero to capture only values necessary for the 16-byte pcap header (timestamp, packet length, captured size).

The maximum snaplength is 9216 bytes to allow for Ethernet jumbo frames and the ATM WAN MTU size of 9180 bytes.

An error is displayed if you run this command while the packet capture is running.

snaplength <*length*>
no snaplength <*length*>

Syntax Description

<length>	Specifies the length in bytes to which to set the snapshot length. Allowed range: 0 – 9216 bytes Default: 38 bytes (this does not include the 16-byte pcap header that is always captured in addition to the packet data.)

Example

In this example, the **snaplength** command is used to set the snapshot limit to 1024 bytes:

```
host(config-capture)# snaplength 1024
host(config-capture)#
```

snmp-server

Mode

Configuration mode
`host(config)#`

Usage Guidelines

The SNMP access to the BQM's SNMP community strings are set to 'public'.

Use the **snmp-server enable traps** command to enable server state change SNMP traps or notifications. To disable, use the **no** form of the command. If you enter the command with no keywords, all notification types (email, syslog) are enabled. If you enter the command with a particular notification keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option. The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host(s) receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

SNMP notifications are sent as trap requests, the system does not support inform requests. This command enables or disables server state change notifications, when enabled, will be sent when the server moves from an “up” to “dead” state, or when a server moves from a “dead” to an “up” state, where:

1. up(1) - server is responding to requests
2. down(2) – server failed to respond to requests.

Standard system fault logging is disabled by default. If logging has been disabled on your system (using the **no snmp-server enable traps syslog** command), logging must be re-enabled by setting the command **snmp-server enable traps syslog** .

To specify a remote host to log system fault messages, use the **destination** form of the command. To remove a specified logging host from the configuration, use the **no snmp-server enable traps syslog destination** form of this command.

The **snmp-server enable traps syslog** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

snmp-server enable traps syslog [[**destination** <*hostname|ip-address*> [**port** <*port*>]] |

Syntax Description

<*hostname|ip-address*>	Specifies a DNS hostname or IP v4 dotted decimal address of the syslog server. We recommend that you use IP addresses when specifying destination servers. You can enter a hostname when using the **snmp-server** command to define a server destination, but you have to use the server IP address when using the **no snmp-server command** to remove a destination server.
port<*port*>	Specifies the port number for the fault syslog server to which fault syslog notifications are to be sent.

	Default: UDP port 514.

The **snmp-server enable traps email** command is to specify which host or hosts receive email SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

snmp-server enable traps email [**server** <*hostname|ip-address*> **from** <*from-address*>] |
[[**destination** <*hostname|ip-address*> [**port** <*port*>]

Syntax Description

<*hostname|ip-address*	Specifies the fully qualified domain name of the e-mail server to be used to forward the e-mail, e.g. mailserver.corvil.com. We recommend that you use IP addresses when specifying destination servers. You can enter a hostname when using the **snmp-server** command to define a server destination, but you have to use the server IP address when using the **no snmp-server command** to remove a destination server.
from-address	Specifies the e-mail address from which the e-mail is sent, for example bqm@acme.com
<*hostname|ip-address*>	Specifies a DNS hostname or IP v4 dotted decimal address of the syslog server. We recommend that you use IP addresses when specifying destination servers. You can enter a hostname when using the **snmp-server** command to define a server destination, but you have to use the server IP address when using the **no snmp-server command** to remove a destination server.
port<*port*>	Specifies the port number for the fault syslog server to which fault syslog notifications are to be sent. Default: UDP port 514.

Use the **snmp-server host** command to specify which host(s) receive SNMP notifications. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host <*hostname|ip address*> **traps** <*community-string*> **udp-port** *port*

Syntax Description

<*hostname|ip address*>	Specifies the DNS hostname or IP address of the host to which SNMP notifications are sent. The *ip-address* is an IP v4 address. The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs. We recommend that you use IP addresses when specifying destination servers. You can enter a hostname when using the **snmp-server** command to define a server destination, but you have to use the server IP address when using the **no snmp-server command** to

	remove a destination server.
traps	Specifies that notifications should be sent as traps. This is the default.
<*community-string*>	Specifies the password-like community string sent with the notification operation. **NOTE:** You can set this string using the **snmp-server host** command by itself, but we recommend that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	Specifies the User Datagram Protocol (UDP) port number of the NMS host to which SNMP notifications or informs are to be sent. Range: 0 – 65535. Default: 162.

Use the **snmp-server fault** command to specify the severity level for a specified fault and to enable reporting of the fault to the various reporting services: SNMP trap, syslog and email. The command allows for the severity levels of a specified fault and its frequency of reporting to be specified, for SNMP traps, for syslog and for email notifications, and whether these individual settings are enabled or disabled. To disable reporting for the specified fault from the configuration, use the **no** form of this command.

Note that the global configuration commands to enable or disable reporting of faults take precedence over an individual fault's setting. For example, if a specific fault was enabled to report its occurrence to SNMP traps, but the setting **no snmp-server enable traps** was in effect, then no SNMP trap fault notifications would be reported.

Using the command **snmp-server fault** <*name*> without any optional parameters causes the default setting for the <*name*> fault to be applied. Use of the command **no snmp-server severity**<*name*> without any optional parameters causes all optional parameters for the <*name*> fault to be disabled, that is, the equivalent of issuing the following command: **no snmp-server fault** *name* **report-traps report-syslog**.

snmp-server fault <*name*> [traps *traps-severity*] [report-traps] [syslog *syslog-severity*][report-syslog][freq *frequency*]

Syntax Description

name	Specifies the name of the fault. Congestion Threshold Clear The Congestion Indicator is back within the configured threshold. Congestion Threshold Exceeded The Congestion Indicator crossed the configured threshold. Corvil Bandwidth Threshold Clear The Corvil Bandwidth measurement indicates the class bandwidth is back within threshold. Corvil Bandwidth Threshold Exceeded The Corvil Bandwidth measurement indicates the class bandwidth threshold has been exceeded. CPU Failure CPU Failure detected. CPU Failure Clear CPU Failure cleared. CPU Utilization Clear High CPU Utilization cleared. CPU Utilization High High CPU Utilization detected. Database Fault Database fault detected. Database Fault Clear Database fault cleared. Default fault type Default fault type E2E Availability Issue Connectivity to the site is currently unavailable.

	E2E Availability Issue Clear — Connectivity to the site is available again. E2E Delay Threshold Clear — The measured end to end delay is back within the configured threshold. E2E Delay Threshold Exceeded — The measured end to end delay crossed the configured threshold. E2E Loss Clear — The measured end to end loss is back within the configured threshold. E2E Loss Detected — The measured end to end loss crossed the configured threshold. Expected Policing Threshold Clear — The Expected Policing is back within the configured threshold. Expected Policing Threshold Exceeded — The Expected Policing crossed the configured threshold. Expected Queuing Delay Threshold Clear — The Expected Queuing Delay is back within the configured threshold. Expected Queuing Delay Threshold Exceeded — The Expected Queuing Delay crossed the configured threshold. Expected Queuing Loss Threshold Clear — The Expected Queuing Loss is back within the configured threshold. Expected Queuing Loss Threshold Exceeded — The Expected Queuing Loss crossed the configured threshold. Fan Failure — Fan failure detected. Fan Failure Clear — Fan failure cleared. Hard Disk Threshold Clear — Hard disk threshold exceeded cleared. Hard Disk Threshold Exceeded — Hard disk threshold exceeded detected. Hard Drive Failure — Hard drive failure detected. Hard Drive Failure Clear — Hard drive failure cleared. License Expired — License is expired. License Expired Clear — License expired cleared. License Invalid — License invalid detected. License Invalid Clear — License invalid cleared. License Near Expiration — License will expire soon. License Near Expiration Clear — License near expiration cleared. Memory Usage Clear — High Memory usage cleared. Memory Usage High — High Memory usage detected. Micro-Burst Clear — Micro-Bursts exceeding the configured bandwidth threshold have been cleared. Micro-Burst Detected — Micro-Bursts exceeding the configured bandwidth threshold have been detected. Port Down — Port down detected. Port Down Clear — Port down cleared. Power Supply Failure — Power supply failure detected. Power Supply Failure Clear — Power supply failure cleared. Soft Disk Threshold Clear — Soft disk threshold exceeded cleared. Soft Disk Threshold Exceeded — Soft disk threshold exceeded detected. System Shutdown — The System has shutdown. System Startup — The System has startup. System Throughput Clear — High System Throughput cleared. System Throughput High — High System Throughput detected. Temperature High — High Temperature detected. Temperature High Clear — High Temperature cleared. Watchdog Restart — System Watchdog has restarted. NOTE: Names containing spaces must be delimited by quotes, for example: “Watchdog Restart”

traps-severity	Specifies the trap severity value for the fault, one of the following values: Informational – events that need communicating but do not cause failures Warning – typically used for thresholds that warn of an impending failure Minor – not used for defaults Major – an event that has the potential to make CorvilNet no longer operational Severe – CorvilNet no longer operational
syslog-severity	Specifies the syslog severity value for the fault, one of the following values: emergency alert critical error warning notification informational debugging
report-traps	Enables reporting of the fault to the trap reporting service. Trap reporting is disabled by default.
report-syslog	Enables reporting of the fault to the syslog reporting service. Syslog reporting is disabled by default.
report-email	Enables reporting of the fault to the e-mail reporting service. E-mail reporting is disabled by default.
freq *frequency*	Specifies the frequency of fault reporting to SNMP trap, syslog and email; one of the following values: Every Hourly Daily Default: Every

Example

In this example, the **snmp-server** command is used to set the SNMP community read-only string to public:

```
host(config)# snmp-server community public RO
host(config)#
```

In this example the system is enabled to send all traps to the host specified by the IP address, using the community string defined as public:

```
host(config)# snmp-server enable traps
host(config)# snmp-server host 192.168.5.3 public
```

start

Mode

Configuration
`host(config-capture)#`

Usage Guidelines

To start packet capture for a packet capture instance from capture configuration mode, use the **start** command. When you use this command, capture files are opened and packet capture is started for the named instance, or for all configured capture instances if a name is not specified. To stop packet capture, use the no form of this command. In this case the packet capture is stopped for the named capture instance, or for all instances if a name is not specified.

A warning is displayed if the amount of free disk space available is less than the file size limit for the configured capture instance.

start <*name*>
no start <*name*>

Syntax Description

Name	Specify the name of the previously configured packet capture instance for which to start capturing packets.

Example

In this example, packet capture instance called serial1 is started:

```
host(config-capture)# start serial1
```

start capture

Mode

Configuration
`host(config)#`

Usage Guidelines

To start packet capture for a previously configured capture instance, use the **start capture** command from configuration mode. When you use this command, capture files are opened and packet capture is started for the named instance, or for all configured capture instances if a name is not specified. To stop packet capture, use the no form of this command. In this case the packet capture is stopped for the named capture instance. Use **no start capture *** to stop all packet capture.

A warning is displayed if the amount of free disk space available is less than the file size limit for the configured capture instance.

start capture <*name*>
no start capture <*name*>

Syntax Description

Name	Specify the name of the previously configured packet capture instance for which to start capturing packets.

Example

In this example, packet capture instance called serial1 is started:

```
host(config)# start capture serial1
```

status

Usage Guidelines

To report the current status of the BQM, use the **status** command.

status [-h]

Syntax Description

-h	Use this switch to display interface statistics in a more user-friendly format.

Examples

To report the current status of the BQM, use the following:

```
host(config)# status
Cisco Bandwidth Quality Manager software: Version 3.0 (3.0-B1.1.17951)
CorvilMeter software: CDK_3_0_BUILD_14 (conf Jun 23 07:32:30 2006)
Application Recognition Module: ARM (full) v3.4.1
System type: 1
Logging: <off>
Access control: unrestricted
Running configuration: not saved (*)
 uptime is 2 hours, 3 minutes, 36 seconds


License system id: 03faad7bb2fcec60de
License status: valid
License features: BandwidthLimit=1000 Mbps
License evaluation time total: unlimited
License evaluation time remaining: 29 days, 10 hours, 23 minutes, 39 seconds




cpu #0: "Intel(R) Xeon(R) CPU            5160  @ 3.00GHz", 4096 KB cache, 0%
cpu #1: "Intel(R) Xeon(R) CPU            5160  @ 3.00GHz", 4096 KB cache, 1%
cpu #2: "Intel(R) Xeon(R) CPU            5160  @ 3.00GHz", 4096 KB cache, 0%
cpu #3: "Intel(R) Xeon(R) CPU            5160  @ 3.00GHz", 4096 KB cache, 0%
5-minute average load (all CPUs): 0%

disk #0: "", total=287239336 KB, used=1285860 KB (0%)
disk #1: "", total=288257368 KB, used=32840 KB (0%)

14 fan component(s), 0 alert(s)
```

```
3 power supply component(s), 0 alert(s)
6 temperature sensor component(s), 0 alert(s)
BIOS date: 07/20/06

Memory: total=4148528 KB, cached=347300 KB, used=2265228 KB (55%)
        5-minute average usage: 55%

System throughput: 30%



Interface      Received              Sent
---------      --------              ----
mgmt:
        bytes  2923669               5543880
      packets  30946                 14945
 dropped pkts  0
  NIC dropped  0
   error pkts  0

PortA:  *** down 2 hours, 3 minutes, 36 seconds ***
        bytes  0                     0
      packets  0                     0
 dropped pkts  0
  NIC dropped  0
   error pkts  0

PortB:  *** down 2 hours, 3 minutes, 36 seconds ***
        bytes  0                     0
      packets  0                     0
 dropped pkts  0
  NIC dropped  0
   error pkts  0

PortC:
        bytes  0                     0
      packets  0                     0
 dropped pkts  0
  NIC dropped  0
   error pkts  0

PortD:
        bytes  1102415376            0
      packets  4003014               0
 dropped pkts  0
  NIC dropped  0
   error pkts  0




Configuration totals:
            class-maps: 1
               matches: 1
            interfaces: 9
```

```
  monitor-queuing-maps: 1
  monitor-end2end-maps: 5
       peer-interfaces: 2
           policy-maps: 1
               routers: 3
                 sites: 2
    configured classes: 1
        active classes: 11
      service policies: 11

Packets dropped during disk capture: 0


host(config)#
```

subnet

Mode

Configuration
`host(config-site)#`

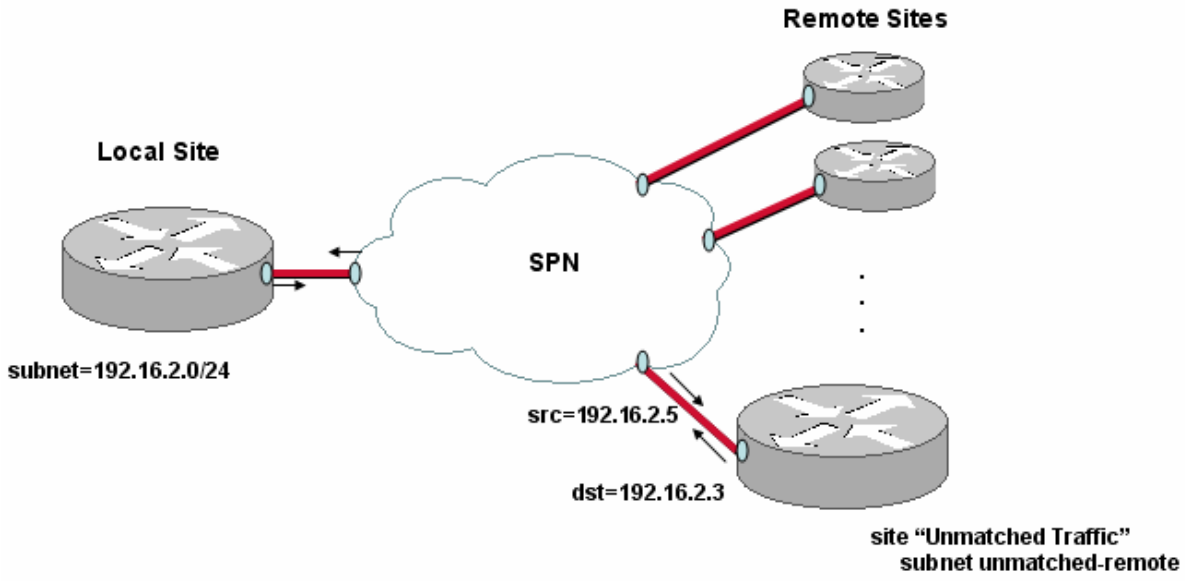
Usage Guidelines

When you are developing the network model for a deployment, you define subnets for each site. To define a subnet for a site, you use the **subnet** command. To remove a site you use the no form of the command. In general, configured subnets are used to identify traffic that originates from or is destined to a particular site, and so to determine the direction of traffic. The network model treats traffic from the perspective of a site, so traffic with a destination address that matches a configured site subnet is considered inbound to the site and traffic with a source address matching the site subnet is considered to be outbound from the site.

The prefix or network mask is applied to the presented IP address before saving the presented value. For example: subnet 1.2.3.4/24 is converted to 1.2.3.0/24 before saving the presented address. All comparisons are performed on the converted address when adding or removing subnets, hence the converted addresses must match to be considered equivalent when adding or removing an address.

Unmatched Traffic
The default BQM configuration includes a single remote site named Unmatched Traffic. As you add remote sites to the network model, the traffic being measured by the Unmatched Traffic remote site decreases. By default the Unmatched Traffic site subnet definition uses the **subnet unmatched-remote** command. So the Unmatched Traffic site always picks up any traffic that is not already matched by configured remote sites.

Similarly, if you configure a remote site with the **subnet unmatched-remote** command, interfaces and peer-interfaces within the site only see traffic that is unmatched by all other remote sites. Additionally, if the local site has subnets defined then those subnets are used to further exclude traffic that is internal to the local site, and to separate unmatched traffic between the peer-interface and interface according to the traffic direction.



For example, if the local site has subnet 192.16.2.0 configured and the remote site sees traffic with a destination address of 192.16.2.3, then those packets are deemed to be outbound from the remote site to the local site. Traffic with a source address of 192.16.2.5 is deemed to be inbound to the remote site from the local site. In this way the local site subnet configuration is used to determine traffic direction at the remote site.

If you delete the default Unmatched Traffic remote site for any reason, and you want to redefine a remote site as this kind of 'catch-all' remote site, you use the **subnet unmatched-remote** command when defining the site.

subnet {<*ip address* >[<*prefix*> | <*netmask*>]} | **unmatched-remote**
subnet {<*ip address* >[<*prefix*> | <*netmask*>]} | **unmatched-remote**

Syntax Description

ip address	Specify an IP address for the configured site or local-site subnet. No default.
prefix	Specify the prefix value to identify the subnet. No default.
netmask	Specify a subnet network mask as a contiguous dotted decimal value. For example: 255.255.255.0 No default.
unmatched-remote	Specifies on interfaces and peer-interfaces within the site, only see remote traffic that is unmatched by other normal remote sites.

Example

In the following example, two remote sites, dublin and london are configured with subnets:

```
site dublin
      subnet 192.168.1.0/24
      ping-address 192.168.1.3

      router stab1

            interface Serial0/1
                  description "Link to data center"
                  bandwidth 512
                  service policy output low-speed
                  connects-to DataCenter core1 Serial0/1

site london
      subnet 192.168.2.0 255.255.255.0
      ping-address 192.168.2.3

      router stab2

            interface Serial0/1
```

```
description “Link to data center”
bandwidth 512
service policy output low-speed
connects-to DataCenter core1 Serial0/2
```

subnet-filtering

Mode

Local-site router interface configuration
`host(config-site-router-if)#`
Local-site router peer-interface configuration
`host(config-site-router-pif)#`
Site router interface configuration
`host(config-site-router-if)#`
Site router peer-interface configuration
`host(config-site-router-pif)#`

Usage Guidelines

Subnet filtering applies when a site has subnets defined with the **subnet** command. To enable interface packet filtering based on either configured site subnet, or traffic source or destination address on local or remote site interfaces or peer interfaces, use the **subnet-filtering** command. This command is automatically invoked for interfaces when you define site subnets. You do not need to explicitly add it to the configuration in this case.

Subnet filtering applies as follows:

- Remote site interfaces match packets that have a source address within any of that remote site's subnets. Note that packets with both a source and destination address within the remote site will be included.
- Remote site peer-interfaces match packets that have a destination address within any of that remote site's subnets. As above, packets with both a source and destination address within the remote site's subnets will be included here also.
- Remote site interfaces connected directly to the local site match packets that have a destination address within the remote site's subnets. This also matches packets with both a source and destination address within the remote site's subnets.
- Local-site interfaces will match packets that do not have a destination address within the local-site's subnets. This means that they will exclude traffic that is internal to the local-site's subnets, but they will include transit traffic that does not involve any local-site subnets.
- Local-site peer-interfaces will match packets that do not have a source address within the local-site's subnets. This means that they will exclude traffic that is internal to the local-site's subnets, but they will include transit traffic that does not involve any local-site subnets.

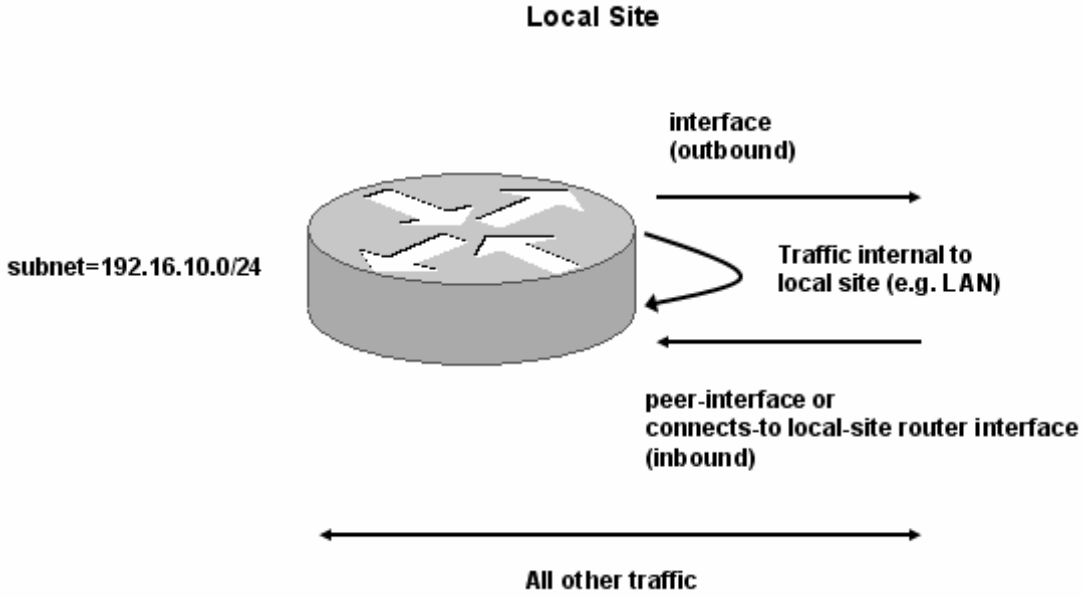
Defining sites with subnets is optional in the BQM configuration. Using **no subnet-filtering** indicates that you intend to ignore site subnets when matching traffic. So this is used when you are

- using the **attached-ports** to establish traffic filtering with the physical BQM ports (PortA, PortB, PortC, PortD, PortAC, PortBD)
- or the **filter-class** commands or if you define a particular set of match rules using a class-map

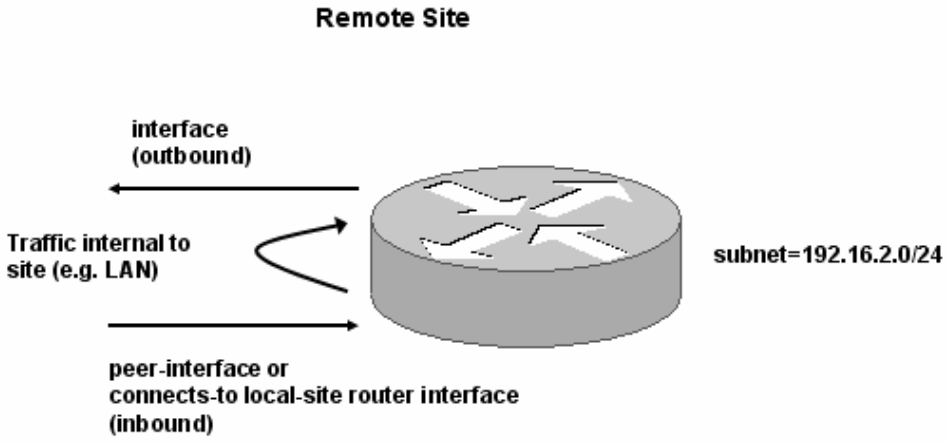
The use of the BQM physical ports (such as PortA, PortB and so on) in the default first day of service configuration requires subnet filtering to be explicitly disabled. So the default BQM configuration includes a **no subnet-filtering** command on each relevant interface. Note that the default BQM configuration has no subnets defined for any sites. For example, from the default configuration:

```
interface PortA
          attached-port PortA
          bandwidth 1000000
          max-reserved-bandwidth 75
          no subnet-filtering
          service-policy output default
            class class-default
```

Where local site interfaces or peer interfaces are filtered using the **attached-ports** command, it may be desirable to exclude traffic that is internal to the local site's subnets (that is, both source and destination address within the site).



Using the **subnet-filtering non-local-only** command switches to excluding only traffic where both the source and destination addresses fall inside the local site's subnets. The interface, peer-interface (or connected interface) and all other traffic seen by the BQM are included. Finally, since the default behavior effectively double-counts traffic that is internal to remote site subnets (once at the interface and once at the peer or connected interface), you can add a **subnet-filtering exclude-local** command that excludes traffic that is local to the site.



In the diagram above, using the exclude-local option excludes the traffic internal to the remote site, for example LAN traffic on the remote site subnet.

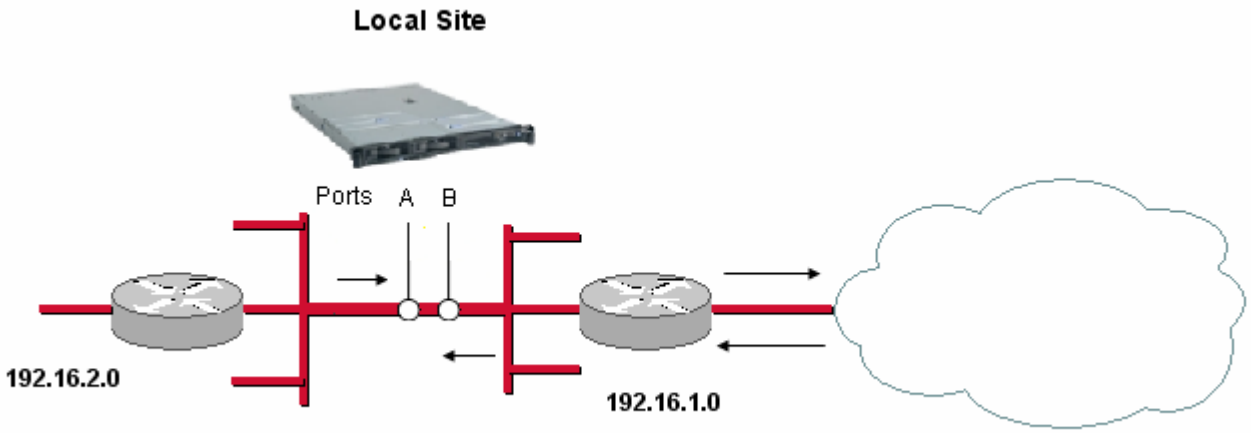
subnet-filtering {exclude-local | non-local-only}
no subnet-filtering

Syntax Description

subnet-filtering	Specifies the default operation of subnet-filtering: Remote interface: match src within remote site subnets Remote peer-interface: match dst within remote site subnets Connects-to local site interface: match dst within remote site subnets Local-site unconnected interface: match dst not within local-site subnets Local-site peer-interface: match src not within local-site subnets
subnet-filtering exclude-local	Specifies that for remote sites traffic that is internal to the remote site's subnet is excluded from measurement: Remote interface: match src but not dst within remote site subnets Remote peer-interface: match dst but not src within remote site subnets Connects-to local site interface: match dst but not src within remote site subnets Unconnected local site interface: match dst not within local-site subnets Local-site peer-interface: match src not within local-site subnets
subnet-filtering non-local-only	Specifies that for local sites traffic that is internal to the local site's subnets is excluded from measurement: Match any src or dst outside local site subnets (that is, exclude local site internal traffic).

Example

In the following example of using the **subnet-filtering non-local-only** command, the BQM sees traffic internal to the local site from two different local site subnets as well as the traffic going to and coming from the WAN. The configuration excludes the internal inter-LAN traffic while measuring only the traffic bound for or coming from the WAN. The BQM physical port PortA is used to measure outbound traffic and PortB is used to measure inbound traffic:




```
host(config-local-site)$ subnet 192.16.1.0
host(config-local-site)$ subnet 192.16.2.0
host(config-local-site)$ router default
host(config-local-site-router)$ interface default
host(config-local-site-router-if)$ attached-port portA
host(config-local-site-router-if)$ subnet-filtering non-local-only
host(config-local-site-router-if)$ peer-interface default
host(config-local-site-router-pif)$ attached-port portB
host(config-local-site-router-pif)$ subnet-filtering non-local-only
host(config-local-site-router-pif)$ show config
!
!
!
!
!
!
local-site Local-site
  subnet 192.16.1.0/32
  subnet 192.16.2.0/32
  router default
    interface default
      attached-port PortA PortB
      subnet-filtering non-local-only
    peer-interface default
      subnet-filtering non-local-only
```

terminal

Mode

All
`host(config)#`

Usage Guidelines

To set the number of lines of information displayed in the terminal screen at any one time, use the **terminal** command. The More prompt is displayed after the set number of lines of information. Configuring this value affects only the current session. Set to 0 to switch off the feature.

terminal <*parameter*>

Syntax Description

parameter	Supports the following parameter: length <*num*>. Specify the number of lines on screen (0 for no pausing).

Example

In this example the terminal length on screen is set to six lines:

```
host(config)# terminal length 6
host(config)#
```

trace-events

Mode

Policy-map Configuration
`host(config-pmap)#`

Usage Guidelines

Event detection is enabled by default on all interfaces, but it may not make sense to keep the rolling packet capture enabled for every single interface at all times. This command is used to disable event detection on a selected interface, or to re-enable event detection on an interface where it has been disabled.

Because the default is to have event detection enabled, so there is no need to use a **trace-events** command unless a **no trace-events** command has previously been issued.

trace-events
no trace-events

Examples

For example to enable automatic tracing of detected events on interfaces to which the policy-map named pmap is applied:

```
policy-map pmap
  trace-events
```

To disable automatic tracing of detected events:

```
policy-map pmap
  no trace-events
```

traceroute

Mode

Configuration
`host(config)#`

Usage Guidelines

To trace the route to a destination address on networks, use the **traceroute** command.

traceroute [**ip**] {*ip-address*} [[**numeric**]| [**port** <*number*>]
| [**probe** <*number hops*>] | [**source** <*source-address*>]
| [**ttl** <min. ttl> <max. ttl>] | [**timeout** <*seconds*>]]

Syntax Description

ip *ip address*	Specifies the target IP v4 address.
numeric	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
port *number*	Specifies a UDP port number. <1-65535>, default 33434
probe *number hops*	Specifies the number of hops <1-65535>, default 3
source <*source-address*>	Specifies the source address.
ttl *min. ttl*	Specifies the TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops. <0-255>,
ttl *max. ttl*	Specifies the maximum time to live value. The command terminates when the traceroute packet reaches the destination or when the value is reached. <0-255>, default 30
timeout <*seconds*>	Specifies the timeout value. <0-3600>, default 3

Example

Here is an example of the **traceroute** command:

```
host(config)# traceroute ip 192.168.128.10
host(config)#
```

10 Appendix A: Class-maps and Classification

A class-map is a collection of one or more match rules. Match rules can be combined together in a logical AND or a logical OR manner. If a network packet matches the combined match rules of a class-map then it is considered to have matched that class-map.

Class-maps are the first entities that need to be configured for traffic measurement on a BQM. Some examples of class-maps and match rules and their use are discussed below.

Matching Customer Traffic

For a Service Provider, IP traffic from/to particular customers can normally be identified by the source or destination address of the traffic. In this example, Customer 1 has been assigned the following banks of addresses, 192.168.11.0/24 and 172.241.12.0/28. To set up a class-map that matches traffic going to or coming from Customer 1, you create a class-map called Customer1 using the CLI and then add match rules to it for each bank of addresses:

```
host(config)# class-map Customer1
host(config-cmap)# match ip src=192.168.11.0/24
host(config-cmap)# match ip dst=192.168.11.0/24
host(config-cmap)# match ip src=172.241.12.0/28
host(config-cmap)# match ip dst=172.241.12.0/28
```

The **help** command can be entered at any time to display a list of valid commands. Use **help match** to discover the various valid expressions that can be part of a match rule.

Matching Prioritized Traffic

Traffic coming through a router may be tagged by the router according to its priority, typically using either the Precedence or the Differentiated Services Code Point (DSCP) marker. In this example the DSCP value is set to

46 for high priority traffic, to 10 for medium priority and 0 for all other traffic. To create a class-map for the high-priority traffic:

```
host(config)# config
host(config)# class-map HighPriority
host(config-cmap)# match ip dscp=46
```

Similar class-maps can be configured for the medium and low priority traffic:

```
host(config-cmap)# class-map MediumPriority
host(config-cmap)# match ip dscp=10
host(config-cmap)# class-map LowPriority
host(config-cmap)# match ip dscp=0
```

Matching Application Traffic

Application traffic on a network is often differentiated through the use of certain port numbers. For example, HTTP traffic typically uses port 80 and 443 (secure HTTP) for communication, e-mail (SMTP) uses port 25 and SNMP port 161. VoIP traffic might be directed towards a VoIP server so VoIP traffic could be classified by looking at the destination address.

In the following example, class-maps are used to classify VoIP, HTTP (secure and non-secure) and e-mail traffic, and also all traffic that does not fall into those three categories. VoIP may often be matched by the DSCP or Precedence values similar to the previous example. Alternatively, it might be identified as any traffic directed towards a set of VoIP gateway servers. In this example, VoIP is being classified as traffic destined for two VoIP servers at addresses 192.168.11.14 and 192.168.11.15

By default, match statements within a class-map are logically ORed together.

```
host(config)# class-map VoIP
host(config-cmap)# match ip dst=192.168.11.14
host(config-cmap)# match ip dst=192.168.11.15
```

HTTP traffic is TCP traffic that uses port 80 (non-secure) or port 443 (secure), so it is configured as traffic either originating from or destined for these ports:

```
host(config)# class-map HTTP
host(config-cmap)# match tcp port=80
host(config-cmap)# match tcp port=443
```

E-mail (SMTP) traffic is TCP traffic that uses port 25:

```
host(config)# class-map E-mail
host(config-cmap)# match tcp port=25
```

The next task is to define a class-map that matches all traffic that does not fall into the above three categories. This “other” traffic can be defined in logical terms, as follows:

Other = (NOT VoIP) AND (NOT HTTP) AND (NOT E-mail)

In a class-map you can reference traffic that matches or does not match another class-map by using the **match [not] class-map=<class-map name>** rule. So the rule **match not class-map=VoIP** matches non-VoIP traffic.

The **class-map** command has an optional parameter that determines if the rules within the class-map are combined in a logical AND or a logical OR manner:

OR class-map: **class-map match-any <class-map name>**
AND class-map: **class-map match-all <class-map name>**

Class-maps default to the match-any (OR) type, as in the previous three class-maps. However, defining the Other class-map as match-all (AND) includes the three NOT clauses as follows:

```
host(config)# class-map match-all Other
host(config-cmap)# match not class-map=VoIP
host(config-cmap)# match not class-map=HTTP
host(config-cmap)# match not class-map=E-mail
```

It is often not necessary to define a class-map that specifically matches all traffic not matched by a set of other class-maps. Defining a class-map that matches all traffic is often sufficient to catch traffic that was not matched by other class-maps when used correctly in a policy-map.

Class-map Logic

The following statements summarize the use of BQM class-map logic:

- Expressions within a single **match** rule are ANDed together
- Multiple **match** clauses within a class-map are either ORed together (a match-any class-map) or ANDed together (a match-all class-map)
- The meaning of a **match** clause can be inverted by using **not** as the first expression

In the following examples, expressions within a single match rule are ANDed together:

```
host(config)# class-map Cust1_HighPriority
host(config-cmap)# match tcp src=10.0.0.1 dscp=46
```

The match rule above matches all traffic that is TCP and originates from address 10.0.0.1 and has a DSCP value of 46. So, all expressions in a single match are ANDed together.

That is why, when defining the Customer1 class-map in the first example in this appendix, that multiple match clauses were used, one for each source and destination address. If the Customer1 class-map had been defined as follows, the match rules match all traffic that comes from address X and is destined for address X.

```
host(config)# class-map Customer1
host(config-cmap)# match ip src=192.168.11.0/24 dst=192.168.11.0/24
host(config-cmap)#  match ip src=172.241.12.0/28 dst=172.241.12.0/28
```

However, the real requirement is to match traffic that comes from address X or which is going to address X.

The following examples show how multiple match clauses within a class-map are either ORed together (a match-any class-map) or ANDed together (a match-all class-map). The next example identifies traffic that originates from one of several addresses, so a match-any (OR) class-map is used:

```
host(config)# class-map match-any Cust1
host(config-cmap)# match ip src=192.168.11.0/24
host(config-cmap)# match ip src=10.0.0.1
host(config-cmap)# match ip src=192.168.14.6/28
```

Class-maps that use match-all (AND) are usually needed when one or more match clauses refer to other class-maps. For example, to look for all Cust1 traffic (see above) that was destined for a HTTP server (port 80), you do the following:

```
host(config)# class-map match-all Cust1ToHTTP
host(config-cmap)# match tcp dstport=80
host(config-cmap)# match class-map=Cust1
```

You *can* define a **match-all** class-map that ANDs match clauses that have no reference to class-maps but this should be done with care, to avoid defining a nonsensical class-map, or one that can be reduced to a single clause, for example:

```
host(config)# class-map match-all NeverMatch
host(config-cmap)# match tcp dstport=21
host(config-cmap)# match tcp dstport=80
```

The NeverMatch class-map will never match any traffic as no packet will be destined for port 21 AND port 80.

```
host(config)# class-map match-all CanReduce
host(config-cmap)# match ip protocol=icmp
host(config-cmap)# match ip src=10.0.0.1
host(config-cmap)# match ip dscp=1
```

The CanReduce class-map can be reduced to the single clause **match ip protocol=icmp src=10.0.0.1 dscp=1**. The following is a sensible use of **match-all** without referring to class-maps:

```
host(config)# class-map match-all Sensible
host(config-cmap)# match not tcp any
host(config-cmap)# match not udp any
```

The Sensible class-map matches all non-UDP, non-TCP traffic. The following examples illustrate how to invert the meaning of a match clause by using **not** as the first expression. To match IP traffic:

```
host(config)# class-map IP
host(config-cmap)# match ip any
```

To match *non* IP traffic:

```
host(config)# class-map NonIP
host(config-cmap)# match not ip any
```

The use of **not** is usually straightforward but it can get complicated. For example, to set up a class-map to match TCP traffic that is not destined for a HTTP server you might think the following would work:

```
host(config)# class-map BadNonTcpHttp
host(config-cmap)# match not tcp dstport=80
```

However, this class-map matches non-TCP traffic as well as TCP traffic not destined for a HTTP server. The example above performs NOT (TCP AND HTTP), whereas the requirement is TCP AND NOT HTTP. So the correct solution, using a **match-all** class-map, is the following:

```
host(config)# class-map match-all GoodNonTcpHttp
host(config-cmap)# match tcp any
host(config-cmap)# match not tcp dstport=80
```

11 Appendix B: Common Application Static Port Assignments

The BQM can classify traffic using:

- Source and destination IP addresses
- IP protocol
- Source and destination port for TCP and UDP protocols
- DSCP and ToS markings
- Ethertype

Many applications can be classified by static TCP/UDP port assignments. In addition, within a particular site the ports used for particular applications that make dynamic port assignments are restricted to known ranges (for example, for the purpose of firewall filtering). The following table gives examples of common applications that are identified by static port assignments.

Protocol	Type	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	Kerberos Network Authentication Service
L2TP	UDP	1701	L2F/L2TP tunnel
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol
MS-PPTP	TCP	1723	Microsoft Point-to-Point Tunneling Protocol for VPN

MS-SQLServer	TCP	1433	Microsoft SQL Server
NetBIOS	TCP	137, 138	NetBIOS over IP
NetBIOS	UDP	137, 139	NetBIOS over IP
NFS	TCP/UDP	2049	Network File System
NNTP	TCP/UDP	119	Network News Transfer Protocol
Notes	TCP/UDP	1352	Lotus Notes
Novadigm	TCP/UDP	3460-3465	Novadigm Enterprise Desktop Manager
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
Printer	TCP/UDP	515	Printer
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
SMTP	TCP	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol
SNNTP	TCP/UDP	563	Secure NNTP
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

12 Appendix C: Supported Protocols

This appendix lists of supported protocols for matching application traffic. The names are case-insensitive when you use them with the **match application** command. Applications with names comprising multiple words should be placed between italics when specified in the command. For example, to match Dark Age of Camelot traffic, you use the following command:

```
host(config-cmap)$ match application “half-life ping”
```

OR

```
host(config-cmap)$ match application “Half-Life Ping”
```

Abacast	Abacast transfer	Agresso
Ares transfer	Audiogalaxy	Audiogalaxy transfer
Battle.net	BGP-4	BitTorrent tracker
BitTorrent transfer	BSD Rlogin	BuddyBuddy
Chat at chat.zone.com	Citrix ICA	ClubBox
ClubFolder	Congaltan	CoolDisk
CTS bookook	CTS bridge	CTS daewoo
CTS daishin	CTS dongyang	CTS generic
CTS hanyang	CTS hyundai	CTS kyobo
CTS Kyobo AnchorSpot2	CTS leading	CTS meritz
CTS miraeasset	CTS samsung	CTS sejong
CTS seoul	CTS shinyoung	CTS sk enstock
CTS truefriend	CTS woori	CVS login
CVS transfer	Dark Age of Camelot	Daum Messenger Touch
DCE RPC	Diablo 2	Direct Connect
Direct Connect ping	Direct Connect search result	Direct Connect transfer
DiskPop	DiskPot	DNS
DreamDisk	EBS lecture	eDonkey
eDonkey chat	eDonkey transfer	eXeem search
eXeem tracker	FileBee	FileGuri
FilePia	First Class	FLICKA
Foldero	FolderPlus	FreePop
FreePop transfer	FTP	FTP transfer

GameSpy chat	Genie	Gnutella
Gnutella server	Gnutella transfer	GroupWise
Half-Life	Half-Life ping	Hanafos QBic
Hangame GoStop	Hardmoa	Hello
HotDisk	HotDisk transfer	HotLine
HotLine transfer	HTTP	HTTP media stream
HTTP proxy	HTTP RealPlayer stream	iDisk
IMAP4	iPop	IRC
IRC DCC chat	IRC DCC transfer	ISO Transport Over TCP
JJangFile	JJangFile transfer	Kazaa
Kazaa server	Kazaa transfer	Kontiki
Kontiki transfer	LDAP	Lotus Notes
Lotus Sametime	Lunarstorm live	ManoLito
ManoLito transfer	MAPI over DCE RPC	MGCP
MGCP transfer	MMS	MSN messenger
MSN messenger chat	MSN messenger over HTTP	MSN messenger transfer
MySQL	Napster	Napster WinMX
Napster WinMX transfer	NateOn	NateOn fileroom
NateOn login	NateOn transfer	NeoFolder
NetWare	NNTP	NTP
OnFile	OpenFT transfer	OSCAR
OSCAR over HTTP	OSCAR P2P	p2pia
pcAnywhere	PDBox	PDBox ping
PDBox W	Peepop	Peepop search
PeerEnabler	PeerEnabler transfer	POP3
PPLive	Pruna Plus	RAdmin
Radmin Communication	Red Swoosh	Red Swoosh transfer
RPC v2	Rsync	RTP
RTSP	RTSP media stream	SIP
SIP pickup	SIP RTCP	SIP RTP
Skype-Hub2Hub	Skype-P2P	Skype-PS
Skype-SSL	Skype-TCP	Skype-UDP
SMB	SMTP	Socks v4
Socks v5	SoftEther	Soribada
Soulseek	Soulseek transfer	SpotLife
SSH	SSL v2	SSL v3
Steam	Sunfile	SunFolder
TDS	TeamSpeak	Terminal Services
Tinc VPN	TNS	Toto disk
Toto disk transfer	TPTEST	TPTEST transfer
undefined	Undetermined	Unreal Tournament
Unreal Tournament transfer	V-share	V-share search
VDisk	Ventrilo VoIP	VMware
VNC	WeDisk	WinNy v1
WinNy v2	World of Warcraft	World of Warcraft login
X11	Xfire	XMPP
Xtoc	Yahoo! messenger	Yahoo! webcam chat

13 Appendix D: Ethertype Identifiers

The Ethertype value appears following the Source Address field in a Version 2 Ethernet frame. The purpose for the Ethertype is to provide an identifier whereby the communications software can differentiate between various types of protocols. A different protocol handler is used for different function, and the Ethertype identifies the frame as belonging to one or another protocol family. The following table lists the Ethertype identifiers:

Value	Description
0000-05DC	IEEE 802.3 Length Fields
0101-01FF	Experimental (for development) -- Conflicts with 802.3 Length Fields
0200	Xerox PUP -- Conflicts with 802.3 Length Field
0201	PUP Address Translation -- Conflicts with 802.3 Length Fields
0600	Xerox XNS IDP
0800	DOD IP
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
0804	CHAOSnet
0805	X.25 Level 3
0806	ARP (for IP and CHAOS)
0807	Xerox XNS Compatibility
081C	Symbolics Private
0888-088A	Xyplex
0900	Ungermann-Bass network debugger
0A00	Xerox 802.3 PUP
0A01	Xerox 802.3 PUP Address Translation
0A02	Xerox PUP CAL Protocol (unused)
0BAD	Banyan Systems, Inc.
1000	Berkeley Trailer negotiation
1001-100F	Berkeley Trailer encapsulation for IP
1066	VALIS Systems
1600	VALID Systems
3C01-3C0D	3Com Corporation
3C10-3C14	3Com Corporation
4242	PCS Basic Block Protocol

5208	BBN Simnet Private
6000	DEC Unassigned
6001	DEC MOP Dump/Load Assistance
6002	DEC MOP Remote Console
6003	DEC DECnet Phase IV
6004	DEC LAT
6005	DEC DECnet Diagnostic Protocol: DECnet Customer Use
6007	DEC DECnet LAVC
6008	DEC Amber
6009	DEC MUMPS
6010-6014	3Com Corporation
7000	Ungermann-Bass download
7001	Ungermann-Bass NIU
7002	Ungermann-Bass diagnostic/loopback
7007	OS/9 Microware
7020-7028	LRT (England)
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe protocol
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostic type (obsolete)
8014	SGI network games (obsolete)
8015	SGI reserved type (obsolete)
8016	SGI "bounce server" (obsolete)
8019	Apollo
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse ARP (RARP)
8036	Aeonic Systems
8038	DEC LANBridge
8039	DEC DSM
803A	DEC Aragon
803B	DEC VAXELN
803C	DEC NSMV
803D	DEC Ethernet CSMA/CD Encryption Protocol
803E	DEC DNA
803F	DEC LAN Traffic Monitor
8040	DEC NetBIOS
8041	DEC MS/DOS
8042	DEC Unassigned
8044	Planning Research Corporation
8046	AT&T
8047	AT&T
8049	ExperData (France)
805B	VMTP (Versatile Message Transaction Protocol, RFC-1045, Stanford)
805C	Stanford V Kernel production, Version 6.0
805D	Evans & Sutherland
8060	Little Machines

8062	Counterpoint Computers
8065	University of Massachusetts, Amherst
8066	University of Massachusetts, Amherst
8067	Veeco Integrated Automation
8068	General Dynamics
8069	AT&T
806A	Autophon (Switzerland)
806C	ComDesign
806D	Compugraphic Corporation
806E-8077	Landmark Graphics Corporation
807A	Matra (France)
807B	Dansk Data Elektronic A/S (Denmark)
807C	Merit Intermodal
807D	VitaLink Communications
807E	VitaLink Communications
807F	VitaLink Communications
8080	VitaLink Communications bridge
8081	Counterpoint Computers
8082	Counterpoint Computers
8083	Counterpoint Computers
8088	Xyplex
8089	Xyplex
808A	Xyplex
809B	AppleTalk and Kinetics Appletalk over Ethernet
809C	Datability
809D	Datability
809E	Datability
809F	Spider Systems, Ltd. (England)
80A3	Nixdorf Computer (West Germany)
80A4-80B3	Siemens Gammasonics, Inc.
80C0	Digital Communication Associates
80C1	Digital Communication Associates
80C2	Digital Communication Associates
80C3	Digital Communication Associates
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Integraph Corporation
80CD	Harris Corporation
80CE	Harris Corporation
80CF-80D2	Taylor Inst.
80D3	Rosemount Corporation
80D4	Rosemount Corporation
80D5	IBM SNA Services over Ethernet
80DD	Varian Associates
80DE	Integrated Solutions TRFS (Transparent Remote File System)
80DF	Integrated Solutions
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	Kinetics, AppleTalk ARP (AARP)
80F4	Kinetics
80F5	Kinetics

80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107	Symbolics Private
8108	Symbolics Private
8109	Symbolics Private
8130	Waterloo Microsystems
8131	VG Laboratory Systems
8137	Novell (old) NetWare IPX
8138	Novell
8139-813D	KTI
9000	Loopback (Conifguration Test Protocol)
9001	Bridge Communications XNS Systems Management
9002	Bridge Communications TCP/IP Systems Management
9003	Bridge Communications
FF00	BBN VITAL LANBridge cache wakeup

14 Index

?

? command 9-11

A

Active flows graph
- event analysis 5-22

alarms
- quality, overview 1-4
- quality, tab 1-4

Alarms
- configuring severity, frequency 8-28
- filtering results 4-30
- monitoring quality 4-28
- quality, reporting results 4-30
- quality, sorting results 4-30
- quality, types 4-29
- recent, dashboard 4-2

alerts
- system, tab 1-5
- system,overview 1-5

allow command 9-13

Analyzing an event
- event analysis 5-3

Application recognition
- upgrading 8-15

ATM PVC, FR PVC, Metro Ethernet, Leased Line deployment
- basic (GUI) 3-1
- basic, CLI 7-23
- basic, defining remote sites (GUI) 3-6
- basic, editing local site (GUI) 3-4
- basic, end-to-end map configuration (GUI) 3-2
- basic, policy-map configuration (GUI) 3-3
- defining monitor-queuing-maps (GUI) 3-16
- dual-homed (GUI) 3-16
- dual-homed, CLI 7-36
- dual-homed, defining end-to-end maps (GUI) 3-17
- dual-homed, defining policy-maps (GUI) 3-17
- dual-homed, defining remote sites (GUI) 3-20
- dual-homed, editing the local site (GUI) 3-18

attach command 9-14

attached-ports command 9-15

Attaching a traffic policy to an interface (CLI) 7-18

Average bit rate graph
- event analysis 5-20
- traffic insight 4-41

Average packet rate graph
- event analysis 5-21
- traffic insight 4-42

B

Backing up configuration files 8-14

Backing up packet capture files 8-14

backup command 9-16

bandwidth command 9-18

Bandwidth Quality Manager mode
- switching to System Administration 1-5

bandwidth sizing
- overview 1-4
- tab 1-4

Bandwidth sizing
- Corvil Bandwidth graph results 6-10
- defining custom report periods 6-5
- filtering results 6-6
- monitoring multi-class requirements 6-12
- monitoring single-class requirements 6-11
- overview 6-1
- recommendations 6-8
- reporting results 6-6
- selecting a report period 6-5
- sorting results 6-6
- viewing results 6-7

Byte-counts graph
- event analysis 5-20

C

capture command 9-20

Changing passwords 8-2

class command 9-22
class-adjust command 9-24
Class-map
defined.... 2-6
overview.... 2-6
class-map command 9-26
Class-maps
configuring (GUI).... 2-16
defing a match rule (GUI) 2-16
clear command 9-27
clock set command....9-28
clock timezone command....9-28
Command completion (CLI) 7-3
configuration
overview.... 1-4
tab 1-4
Configuration
default monitor-queuing-map 2-2
monitor-queuing-map 2-2
order of tasks 2-1
overview.... 2-1
status.... 8-11
Configuration file
defining a monitor-end-to-end-map (CLI).... 7-6
defining a monitor-queuing-map (CLI) 7-5
defining a traffic class (CLI) 7-7
Configuration files
attaching a traffic policy to an interface (CLI) 7-18
combining match-all and match-any statements.... 7-9
defining a remote site (CLI) 7-16
defining a router (CLI) 7-16
defining a traffic policy (CLI) 7-13
defining an interface (CLI).... 7-16
using nested class-maps (CLI).... 7-9
working with (CLI) 7-18
Configuring class-maps (GUI) 2-16
Configuring custom applications....2-32
Configuring LFI for an interface 2-48
Configuring monitor-end-to-end-maps 2-14
Configuring monitor-queuing-maps (GUI) 2-9
attributes.... 2-10
Corvil Bandwidth 2-12
expected delay and loss 2-11
microburst detection 2-13
Configuring network settings 8-5
Configuring NTP time server 8-8
Configuring policy-maps....2-21
Configuring QoS monitoring features (GUI)
configuring monitor-end-to-end-maps.... 2-14
monitor-queuing-maps 2-9
Configuring sites
editing the local site.... 2-36
local site router.... 2-37
local site router interface 2-39
remote site 2-41
remote site router.... 2-43
remote site router interface.... 2-44
Congeestion analysis
congestion indicator defined 4-10
Congestion
dashboard, top congested interfaces....4-3
monitoring....4-9
congestion analysis
overview 1-3
tab 1-3
Congestion analysis
congestion indicator results....4-23
defining custome report periods....4-14
delay Corvil Bandwidth results....4-24
expected delay results 4-20
expected loss results....4-21
expected priority drops results 4-27
filtering results....4-15
microburst detection....4-18
microburst results....4-21
overview 4-9
priority class Corvil Bandwidth results....4-26
queue length Corvil Bandwidth results 4-25
reporting results 4-15
selecting a report period....4-13
sorting results....4-14
viewing round-trip delay and loss 4-16
Congestion Indicator
defined 4-10
connects-to command 9-31
copy command.... 9-32
CPU utilization
status 8-11
custom applications
configuration (GUI) 2-32
Custom applications
overview 2-9
custom-application command.... 9-35

D

dashboard
overview 1-2
tab 1-2
Dashboard
introduction....4-1
navigation tree....4-5
recent alarms....4-2
top application results 4-7
top congested interfaces....4-3
viewing summary interface and class results 4-5
WAN application leaders....4-4
Default enabled features 2-3
Default monitor-queuing-map
enabled features 2-3
overview 2-3
Definig policy-maps (CLI) 7-13
Defining a monitor-end-to-end-map (CLI)..... 7-6
QoS commands....7-6
Defining a monitor-queuing-map (CLI) 7-5
QoS commands....7-5
Defining a remote site (CLI)..... 7-16

Defining a router (CLI.....7-16
Defining a traffic class
combining match-all and match-any statements..... 7-9
match commands (CLI)..... 7-8
nested class-maps (CLI)..... 7-9
Defining a traffic class (CLI).....7-7
Defining a traffic filter
event analysis..... 5-6
Defining a traffic policy
commands (CLI)..... 7-14
Defining a traffic policy (CLI).....7-13
Defining an interface CLI).....7-16
Defining class-maps (CLI).....7-7
Defining remote sites, routers and interfaces
commands (CLI)..... 7-16
Delay Corvil Bandwidth
event analysis..... 5-8
delete command.....9-37
Deleting
remote site..... 2-50
Deleting a configuration object or entry.....7-4
description command.....9-38
Diagnostics.....8-17
audit trail, viewing..... 8-21
storing system log messages..... 8-23
system log, review..... 8-22
technical support information..... 8-22
watchdog operation..... 8-23
dir command.....9-40
Disabling event detection packet capture.....5-24
Disabling features
overview..... 2-5
Disk utilization
status..... 8-11
domain command.....9-41
duration command.....9-42

E

Editing
remote site..... 2-49
Editing the local site.....2-36
Enabling bandwidth sizing.....2-3
Enabling Congestion Indicator.....2-3
Enabling Corvil Bandwidth.....2-3
Enabling Microburst event detection
overview..... 2-3
end2end-target command.....9-43
End-to-end measurement
overview..... 2-5
estimate-service-level command.....9-44
ethernet command.....9-45
Event analysis
active flows graph..... 5-22
analyzing an event..... 5-3
average bit rate graph..... 5-20
average packet rate graph..... 5-21
byte-counts graph.....5-20
defining a traffic filter.....5-6
delay Corvil Bandwidth.....5-8
disabling event detection packet capture.....5-24
expected delay.....5-9
expected loss.....5-11
expected priority drops.....5-12
expected queue-length.....5-10
identifying traffic leaders.....5-13
investigating events.....5-2
microburst results.....5-22
packet-counts graph.....5-21
priority class Corvil Bandwidth.....5-11
queue-length Corvil Bandwidth.....5-9
viewing delay and loss results.....5-8
viewing packet size distributions.....5-14
viewing top applications.....5-13
viewing top conversations.....5-17
viewing top listeners.....5-16
viewing top talkers.....5-15
zoom feature.....5-5
event-capture command..... 9-21
exit command..... 9-46
Expected delay
event analysis.....5-9
Expected loss
event analysis.....5-11
Expected priority drops
event analysis.....5-12
Expected queue-length
event analysis.....5-10

F

Fault notification
checking configuration status.....8-29
configuration.....8-23
overview.....8-23
Features
enabling bandwidth s XE "Enabling bandwidth sizing" XE "Enabling Corvil Bandwidth" XE "Enabling Congestion Indicator" izing.....2-3
enabling congestion indicator.....2-3
enabling Corvil Bandwidth.....2-3
enabling microburst event detection.....2-3
Filter classes
using (CLI).....7-22
filter-class command..... 9-47
Filtering results
alarms.....4-30
bandwidth sizing.....6-6
congestion analysis.....4-15
system alerts.....8-20
traffic insight.....4-35
Filtering traffic
event analysis.....5-6

G

GUI
overview ... 1-1

H

Help (CLI)
using ... 7-2
help command ... 9-49
Hybrid deployment
configuing, CLI ... 7-49
Hybrid deployment (GUI) ... 3-29

I

Identifying traffic leaders
traffic insight ... 4-44
Interface
defined ... 2-7
interface command ... 9-51
IP address access
restricting ... 8-6

L

License
installation ... 8-4
installation using ssh ... 8-4
status ... 8-4
license command ... 9-52
link-adjust command ... 9-53
local site
router interface configuration ... 2-39
Local site
defined ... 2-7
editing ... 2-36
router configuration ... 2-37
local-site command ... 9-55
log command ... 9-56
logging command ... 9-57
Logging Out (CLI) ... 7-5

M

manual packet capture
performing ... 5-24
match any command ... 9-60
match application command ... 9-61
match class-map command ... 9-63
match command ... 9-58
match ethertype command ... 9-64
match ether-type command ... 9-64
match ip command ... 9-66
match mpls command ... 9-69
match tcp command ... 9-71
match udp command ... 9-74
match vlan command ... 9-77
max-reserved-bandwidth command ... 9-80
measure-bandwidth command ... 9-81
measure-microburst command ... 9-83
measure-ping command ... 9-85
Memory utilization
status ... 8-11
Microburst detection
event analysis ... 5-22
Microburst event detection
enabling ... 2-3
Modes
switching ... 1-5
monitor-end2end-map command ... 9-89
Monitor-end-to-end-map
overview ... 2-5
Monitoring
congested interfaces ... 4-9
congestion analysis overview ... 4-9
traffic insight, overview ... 4-32
monitor-queuing command ... 9-87
Monitor-queuing-map
defined ... 2-2
overview ... 2-2
queuing targets overview ... 2-4
sizing policy overview ... 2-4
monitor-queuing-map command ... 9-90
Monitor-queuing-maps
attributes ... 2-11
more command ... 9-91
More prompt ... 7-4
MPLS VPN, Internet VPN, Private VPN
basic (GUI) ... 3-8
basic, CLI ... 7-27
basic, defining a remote site (GUI) ... 3-13
basic, defining class-maps (GUI) ... 3-10
basic, defining end-to-end maps (GUI) ... 3-9
basic, defining monitor-queuing-maps (GUI) ... 3-8
basic, defining policy-maps (GUI) ... 3-10
dual-homed (GUI) ... 3-22
dual-homed, CLI ... 7-42
dual-homed, defining class-maps (GUI) ... 3-23
dual-homed, defining end-to-end maps (GUI) ... 3-23
dual-homed, defining monitor-queuing-maps (GUI) ... 3-22
dual-homed, defining policy-maps (GUI) ... 3-24
dual-homed, defining remote sites (GUI) ... 3-27
dual-homed, editing the local site (GUI) ... 3-26

N

Network deployments
configuring (CLI) ... 7-23
Network model
ATM PVC, FR PVC, Metro Ethernet, Leased line ... 2-8
MPLS VPN, Internet VPN, Private VPN ... 2-9
overview ... 2-7
Network settings
configuration (CLI) ... 8-5

no command 9-93
ntp command 9-95
NTP time server
configuration 8-8

P

Packet capture
backing up files 8-14
manual, copying 5-28
manual, event analysis 5-31
manual, performing 5-24
manual, status 5-27
restoring files 8-15
setting disk space quota 5-30
setting password 5-30
Packet size distribution
traffic insight 4-43
Packet size distributions
viewing, event analysis 5-14
Packet-counts graph
event analysis 5-21
Password
set packet capture 5-30
password command 9-96
Passwords
recovery 8-2
users, changing 8-2
Pdf reports
creating 1-6
Peak-to-mean graph
traffic insight 4-42
Peer-interface
defined 2-7
peer-interface command 9-97
ping-address command 9-101
Policy-map
defined 2-6
overview 2-6
policy-map command 9-102
Policy-maps
configuring 2-21
low latency queuing configuration (GUI) 2-29
multi-class configuration (GUI) 2-23
single-class configuration (GUI) 2-22
strict priority queuing configuration (GUI) 2-23
weighted-fair queuing configuration (GUI) 2-26
port command 9-104
ppp command 9-105
Pre-queuing traffic
supported features 4-13
Priority class Corvil Bandwidth
event analysis 5-11
priority command 9-106
priority-level command 9-107

Q

quality alarms
overview 1-4
tab 1-4
Quality events timeline 4-10
Queue-length Corvil Bandwidth
event analysis 5-9
queue-limit command 9-110
Queuing targets
overview 2-4
queuing-targets command 9-109

R

Recovering passwords 8-2
reload command 9-111
Remote site
configuration 2-41
defined 2-7
editing 2-49
Remote site router
configuration 2-43
Remote site router interface
configuring 2-44
Remote sites
deleting 2-50
Reporting period
list of available 1-5
selecting 1-5
update frequencies 1-5
Reporting results
alarms 4-30
bandwidth sizing 6-5, 6-6
congestion analysis 4-15
system alerts 8-20
traffic insight 4-34, 4-36
Reports
generating 1-6
overview 1-6
restore command 9-113
Restoring configuration files 8-15
Restoring packet capture files 8-15
Restoring system software 8-12
Restricting IP access 8-6
Restricting SNMP access 8-6
Reviewing the system log 8-22
Router
defined 2-7
router command 9-114

S

Saving configuration changes (CLI) 7-4
Selecting a reporting period 1-5
service command 9-116
service-policy command 9-117

Setting packet capture disk space quota 5-30
Setting system time 8-7
Setting the time zone 8-8
setup command.....9-118
show command.....9-119
shutdown command.....9-128
Site
defined..... 2-7
site command.....9-129
Site subnet
defined..... 2-7
size command.....9-131
size-for command.....9-132
Sizing policy
busy period overview 2-5
overview..... 2-4
Sizing recommendations 6-8
snaplength command.....9-134
SNMP access
restricting..... 8-6
SNMP Traps
configuring fault notification.....8-23
snmp-server command 9-135
Sorting results
bandwidth sizing..... 6-6
congestion analysis..... 4-14
quality alarms 4-30
system alerts 8-20
traffic insight 4-35
start capture command.....9-141
start command 9-140
status command.....9-142
Storing system log messages.....8-23
subnet command.....9-146
Subnet filtering (CLI).....7-19
Supported features
interface direction..... 4-13
pre-queuing, post-queuing traffic 4-13
Switching modes 1-5
System Administration mode
switching to Bandwidth Quality Manager 1-5
system alerts
overview..... 1-5
tab 1-5
System alerts
clearing, reactivating, acknowledging 8-19
commenting..... 8-19
configuring severity, frequency 8-28
filtering results..... 8-20
reporting 8-20
sorting..... 8-20
types 8-18
viewing..... 8-17
System status and resources 8-9

T

terminal command..... 9-152
Time settings
configuration.....8-7
Time zone
configuration.....8-8
Top applications
viewing, event analysis 5-13
viewing, traffic insight 4-44
Top congested interfaces
dashboard.....4-3
Top conversations
viewing, event analysis 5-17
viewing, traffic insight 4-47
Top listeners
viewing, event analysis 5-16
viewing, traffic insight 4-46
Top talkers
viewing, event analysis 5-15
viewing, traffic insight 4-45
traffic insight
overview 1-3
tab 1-3
Traffic insight
average bit rate graph.....4-41
average packet rate graph.....4-42
class results overview 4-37
filtering results 4-35
identifying interface and class traffic patterns.....4-41
identifying traffic leaders 4-44
microburst results.....4-39
packet size distribution chart.....4-43
peak-to-mean graph 4-42
reporting results 4-36
sorting results.....4-35
viewing interface and class results.....4-37
viewing top applications 4-44
viewing top conversations.....4-47
viewing top listeners 4-46
viewing top talkers.....4-45
Traffic Insight
defining custom report periods.....4-34
selecting a reporting period.....4-34
Traffic Insight results
overview 4-32

U

Upgrading the application recognition module. 8-15
User sessions
viewing 8-3

V

Viewing round-trip delay and loss..... 4-16

W

WAN application leaders
dashboard 4-4

Z

Zoom feature
event analysis 5-5