



Cisco Bandwidth Quality Manager User Guide

Software Release 4.0

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-14118-01



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 © 2007 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, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, 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. (0708R)



PREFACE XI

ABOUT THIS GUIDE XI

AUDIENCE XI

PREREQUISITE KNOWLEDGE XI

RELATED DOCUMENTATION XI

CONVENTIONS USED IN THIS GUIDE XII

OBTAINING DOCUMENTATION, OBTAINING SUPPORT, AND SECURITY GUIDELINES XII

1 BANDWIDTH QUALITY MANAGER OVERVIEW 1-1

MONITORING AND CONFIGURATION INTERFACE FEATURES 1-2

Monitoring Network Service Quality 1-2

Analyzing Network Service Quality Events 1-4

Monitoring Network Traffic Statistics 1-4

Bandwidth Sizing 1-5

Using Live View and Related Links 1-6

Viewing Quality Event Alarms 1-7

SWITCHING BETWEEN MODES 1-7

BQM Configuration and Administration 1-8

SELECTING A REPORTING PERIOD 1-9

GENERATING REPORTS 1-9

2 CONFIGURING NETWORK SERVICE QUALITY MONITORING 2-1

OVERVIEW 2-1

CONFIGURING NETWORK SERVICE QUALITY MONITORING FEATURES 2-3

ENABLING END-TO-END MONITORING WITH NETWORK SERVICE OBJECTIVES 2-3

Default Network Service Objective 2-4

CONFIGURING A NETWORK SERVICE OBJECTIVE 2-6

Filtering the List of Network Service Objective 2-9

DEFINING A NETWORK SERVICE OBJECTIVE 2-9

Configuring Passive Network Quality Monitoring (PNQM) 2-11

Configuring ICMP Ping 2-11

Configuring Expected Queuing and Corvil Bandwidth 2-12

Configuring Microburst 2-13

CLASSIFYING TRAFFIC WITH CLASS MAPS 2-14

CONFIGURING CLASS MAPS 2-14

MODELING ROUTER QoS CONFIGURATION WITH POLICY MAPS 2-20

CONFIGURING POLICY MAPS 2-20

CONFIGURING A SINGLE-CLASS POLICY MAP 2-21

CONFIGURING A MULTI-CLASS POLICY MAP 2-22

Configuring a Strict Priority Queuing Policy Map 2-22

Configuring a Weighted Fair Queuing (WFQ) Policy Map 2-25

Configuring a Low Latency Queuing (LLQ) Policy Map 2-28

CONFIGURING CUSTOM APPLICATIONS 2-31

COMPLETING THE NETWORK MODEL WITH SITES, ROUTERS, AND INTERFACES 2-35

CONFIGURING SITES, ROUTERS, AND INTERFACES 2-38

EDITING THE LOCAL SITE 2-39

Configuring a Local Site Router 2-41

Configuring a Local Site Router Interface 2-43

CONFIGURING A NEW REMOTE SITE 2-45

Configuring a Remote Site Router 2-46

Configuring a Remote Site Router Interface – No PNQM Channel 2-48

Configuring a PNQM Channel 2-50

Configuring Advanced Interface Settings 2-52

EDITING A REMOTE SITE 2-54

DELETING A REMOTE SITE 2-54

CONFIGURING A CUSTOM DASHBOARD 2-55

3 CONFIGURING NETWORK DEPLOYMENTS 3-1

OVERVIEW 3-1

BASIC ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 3-2

DUAL-HOMED ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE

DEPLOYMENT 3-8

BASIC MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT 3-14

VPN DEPLOYMENT WITH REDUNDANT LOCAL SITE CONNECTIVITY 3-20

VPN DEPLOYMENT WITH REDUNDANT REMOTE SITE CONNECTIVITY 3-21

DUAL-HOMED MPLS VPN DEPLOYMENT 3-22

HYBRID DEPLOYMENT 3-29

4 MONITORING NETWORK SERVICE QUALITY 4-1

MONITORING DASHBOARD OVERVIEW 4-2

IDENTIFYING NETWORK SERVICE QUALITY ISSUES 4-3

Using Sparklines 4-4

IDENTIFYING TOP APPLICATIONS 4-5

IDENTIFYING RECENT QUALITY ALARMS 4-6

VIEWING SUMMARY INTERFACE AND CLASS RESULTS 4-7

Network Service Quality Results 4-9

Top Applications Results 4-11

MONITORING QUALITY ALARMS 4-12

- SORTING THE QUALITY ALARMS TABLE 4-14
- FILTERING THE QUALITY ALARMS TABLE 4-14
- GENERATING A QUALITY ALARMS REPORT 4-15
- MONITORING NETWORK SERVICE QUALITY 4-16**
- VIEWING NETWORK SERVICE QUALITY RESULTS 4-16
- SELECTING A REPORT PERIOD 4-21
- Defining a Custom Report Period 4-21
- SORTING THE NETWORK SERVICE QUALITY TABLE 4-21
- FILTERING THE NETWORK SERVICE QUALITY TABLE 4-22
- REPORTING NETWORK SERVICE QUALITY RESULTS 4-22
- VIEWING INTERFACE AND CLASS RESULTS 4-23
- Viewing Live View Results 4-23
- Viewing ICMP Round Trip and Packet Loss 4-26
- VIEWING CLASS MEASUREMENTS 4-29
- Viewing End-to-End Latency, Jitter and Loss Results 4-29
- Viewing Expected Queuing Latency, Loss and Delay Variation Results 4-32
- Viewing Priority Class Results 4-34
- IDENTIFYING NETWORK SERVICE QUALITY ISSUES 4-35**
- MONITORING CUSTOM DASHBOARD RESULTS 4-38**
- VIEWING CUSTOM DASHBOARD RESULTS 4-39
- VIEWING CLASS RESULTS 4-40

5 ANALYZING NETWORK EVENTS 5-1

OVERVIEW 5-1

- EVENT ANALYSIS OVERVIEW 5-2
- SELECTING A REPORT PERIOD 5-5
- Defining a Custom Report Period 5-5
- SORTING THE EVENT ANALYSIS TABLE 5-6
- FILTERING THE EVENT ANALYSIS TABLE 5-6
- REPORTING EVENT ANALYSIS RESULTS 5-6
- VIEWING INTERFACE AND CLASS EVENTS 5-7
- VIEWING ROUND TRIP TIME AND LOSS 5-7
- VIEWING INTERFACE MICROBURST AND NETWORK SERVICE INDEX MEASUREMENTS 5-9
- VIEWING CLASS MEASUREMENTS 5-12
- End-to-End Latency 5-12
- End-to-End Loss 5-14
- Expected Queuing Latency 5-15
- Expected Queuing Delay Variation 5-16
- Expected Queuing Loss 5-17
- Microburst Detection 5-18
- Corvil Bandwidth – Delay 5-19
- Corvil Bandwidth – Queue Length 5-20
- Network Service Index 5-21
- VIEWING PRIORITY CLASS RESULTS 5-22
- Corvil Bandwidth - Priority 5-22
- Expected Priority Drops 5-24
- INVESTIGATING NETWORK EVENTS 5-25**
- ANALYZING AN EVENT 5-26

- Defining and Applying Traffic Filters to Event Analysis Results 5-29
- VIEWING EVENT ANALYSIS RESULTS 5-31**
- IDENTIFYING EVENT TRAFFIC LEADERS 5-31**
- Viewing Top Applications 5-31
- Viewing Top Talkers 5-32
- Viewing Top Listeners 5-33
- Viewing Top Conversations 5-34
- IDENTIFYING EVENT MICROBURST MEASUREMENTS 5-35**
- IDENTIFYING EVENT TRAFFIC PATTERNS 5-35**
- Average Bit Rate and Byte-counts Graphs 5-36
- Average Packet Rate and Packet-counts Graphs 5-37
- Active Flows Graph 5-38
- Viewing Packet Size Distributions 5-38
- IDENTIFYING THE SOURCE OF APPLICATION PERFORMANCE PROBLEMS 5-39**
- DISABLING EVENT DETECTION ON SELECTED INTERFACES 5-40**
- WORKING WITH MANUAL PACKET CAPTURES 5-41**
- SETTING DISK SPACE QUOTA FOR MANUAL AND EVENT ANALYSIS PACKET CAPTURES 5-46**
- SETTING A PACKET CAPTURE PASSWORD 5-47**
- USING MANUAL PACKET CAPTURE TO IDENTIFY EVENTS 5-47**

6 MONITORING NETWORK TRAFFIC 6-1

MONITORING TRAFFIC INSIGHT RESULTS 6-1

- TRAFFIC INSIGHT OVERVIEW 6-2
- SELECTING A REPORT PERIOD 6-3
- Defining a Custom Report Period 6-4
- SORTING THE TRAFFIC INSIGHT TABLE 6-4**
- FILTERING THE TRAFFIC INSIGHT TABLE 6-4**
- REPORTING TRAFFIC STATISTIC RESULTS 6-5**
- VIEWING SUMMARY INTERFACE STATISTICS 6-5**
- VIEWING INTERFACE AND CLASS STATISTICS 6-6**
- CLASS STATISTICS OVERVIEW 6-7**
- IDENTIFYING MICROBURST MEASUREMENTS 6-8**
- IDENTIFYING INTERFACE AND CLASS TRAFFIC PATTERNS 6-10**
- Average Bit Rate Graph 6-10
- Average Packet Rate Graph 6-11
- Peak-to-Mean Ratio Graph 6-11
- Packet Size Distribution Chart 6-12
- IDENTIFYING TRAFFIC LEADERS 6-13**
- Viewing Top Applications 6-13
- Viewing Top Talkers 6-14
- Viewing Top Listeners 6-15
- Viewing Top Conversations 6-16

7 BANDWIDTH SIZING 7-1

OVERVIEW 7-1

- BANDWIDTH SIZING SUMMARY TABLE 7-2**

- SELECTING A REPORT PERIOD 7-4
- Defining a Custom Report Period 7-5
- SORTING THE BANDWIDTH SIZING TABLE 7-5
- FILTERING THE BANDWIDTH SIZING TABLE 7-5
- REPORTING BANDWIDTH SIZING RESULTS 7-6
- VIEWING SIZING RESULTS 7-7**
- BANDWIDTH SIZING RECOMMENDATIONS 7-7
- Single class Configuration Recommendations 7-8
- Multi-class Configuration Recommendations 7-8
- Priority Class in a Multi class Configuration Recommendations 7-9
- Viewing the Sizing Graph 7-9
- MONITORING SINGLE-CLASS SIZING REQUIREMENTS 7-11
- MONITORING MULTI-CLASS SIZING REQUIREMENTS 7-12
- IDENTIFYING NEW CLASS RESOURCE REQUIREMENTS 7-12

8 USING THE COMMAND LINE INTERFACE (CLI) 8-1

INTRODUCTION TO THE CLI 8-1

USING THE HELP FEATURE 8-2

COMPLETING A PARTIAL COMMAND NAME 8-3

USING THE SHOW COMMAND 8-3

USING THE STATUS COMMAND 8-4

CONTINUING OUTPUT AT THE --MORE-- PROMPT 8-4

DELETING CONFIGURATION OBJECTS AND ENTRIES 8-4

SAVING AND RESTORING CONFIGURATION CHANGES 8-5

LOGGING OUT OF THE BQM CLI 8-5

CONFIGURING BQM USING THE CLI 8-5

DEFINING A NETWORK SERVICE OBJECTIVE 8-5

DEFINING A CLASS MAP 8-7

USING NESTED CLASS-MAPS 8-9

Combining match-all and match-any Statements 8-9

Maintenance 8-10

Converting Network-Based Application Recognition (NBAR) Configurations 8-10

DEFINING A POLICY MAP 8-13

DEFINING A REMOTE SITE, ROUTER, AND INTERFACE 8-16

DEFINING A PASSIVE NETWORK QUALITY MONITORING (PNQM) CHANNEL 8-18

AUTOMATIC PNQM CONFIGURATION 8-19

MANUAL PNQM CONFIGURATION 8-21

Guidelines for Manual Configuration 8-21

Configuration Examples 8-24

Configuring Manual PNQM - Example Scenario 8-26

ATTACHING A POLICY MAP TO AN INTERFACE 8-30

WORKING WITH CONFIGURATION FILES 8-30

DEFAULT BQM CONFIGURATION 8-31

WORKING WITH SUBNET FILTERING 8-33

USING FILTER CLASSES 8-36

VIEWING CLI RESULTS 8-36

CONFIGURING NETWORK MODEL DEPLOYMENTS WITH THE CLI 8-39

BASIC ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 8-40

DUAL-HOMED ATM PVC, FRAME RELAY PVC, METRO ETHERNET, LEASED LINE DEPLOYMENT 8-45
BASIC MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT 8-49
MPLS VPN Deployment with Redundant Local Site Connectivity 8-55
MPLS VPN Deployment with Redundant Remote Site Connectivity 8-56
MPLS VPN Deployment with Any-to-Any Traffic 8-56
MPLS VPN Deployment with Remote Site Internet Traffic via Local Site 8-57
MPLS VPN Deployment with Local Site Connected to Remote Sites via Two WANs 8-58
DUAL-HOMED MPLS VPN, INTERNET VPN, PRIVATE VPN DEPLOYMENT 8-59
Dual Data Center Deployment 8-65
HYBRID DEPLOYMENT 8-67
POINT-TO-POINT FIREWALL DEPLOYMENT 8-74
CONFIGURING A CUSTOM DASHBOARD 8-75

9 SYSTEM ADMINISTRATION 9-1

USER ADMINISTRATION 9-1

CHANGING USER PASSWORDS 9-2

PASSWORD RECOVERY 9-3

VIEWING CURRENT USER SESSIONS 9-3

SYSTEM SETUP 9-4

INSTALLING A LICENSE 9-4

Installing a License Using SSH 9-5

CONFIGURING NETWORK SETTINGS 9-5

PASSIVE NETWORK QUALITY MONITORING (PNQM) COMMUNICATION PORT SETTINGS 9-6

RESTRICTING SNMP ACCESS 9-6

RESTRICTING IP ADDRESS ACCESS 9-7

SYSTEM TIME SETTINGS 9-8

Setting the System Time 9-8

Setting the Time Zone 9-9

Configuring an NTP Time Server 9-9

SYSTEM STATUS AND RESOURCES 9-10

PHYSICAL AND LOGICAL DISKS ON THE CISCO ADE 2130 AND 2140 9-13

BACKUP AND RESTORE 9-15

RESTORING SYSTEM SOFTWARE 9-15

BACKING UP AND RESTORING CONFIGURATION AND PACKET CAPTURE FILES 9-17

UPGRADING THE APPLICATION RECOGNITION MODULE (ARM) 9-19

DIAGNOSTICS 9-20

VIEWING SYSTEM ALERTS 9-20

System Alert Types 9-21

Viewing Active and Cleared Alerts Information 9-21

Adding a Comment to a System Alert 9-22

Sorting the System Alerts Table 9-22

Filtering the System Alerts Table 9-22

Using the CLI to View Alerts 9-23

VIEWING THE AUDIT TRAIL 9-23

GENERATING SYSTEM TECHNICAL SUPPORT DIAGNOSTICS INFORMATION 9-23

REVIEWING THE SYSTEM LOG 9-24

STORING SYSTEM LOG MESSAGES 9-24

WATCHDOG OPERATION 9-25
SYSTEM RECOVERY 9-25
CONFIGURING FAULT NOTIFICATION 9-26
OVERVIEW 9-26
CONFIGURING ALARM SEVERITY AND FREQUENCY SETTINGS 9-34
Checking Fault Configuration Status 9-34

10 CLI COMMAND REFERENCE 10-1

CONFIGURATION MODE 10-1
CLASS-MAP CONFIGURATION MODE 10-5
CUSTOM-DASHBOARD CONFIGURATION MODE 10-6
POLICY-MAP CONFIGURATION MODE 10-6
POLICY-MAP CLASS CONFIGURATION MODE 10-6
NETWORK SERVICE OBJECTIVE CONFIGURATION MODE 10-7
LOCAL SITE CONFIGURATION MODE 10-8
SITE CONFIGURATION MODE 10-8
SITE ROUTER CONFIGURATION MODE 10-8
INTERFACE CONFIGURATION MODE 10-9
PEER-INTERFACE CONFIGURATION MODE 10-10
PACKET CAPTURE CONFIGURATION MODE 10-10
COMMAND REFERENCE 10-11
? 10-11
ALLOW 10-13
ATTACH 10-14
ATTACHED-PORTS 10-15
BACKUP 10-16
BANDWIDTH 10-18
CAPTURE 10-20
CAPTURE-SETTINGS 10-21
CLASS 10-22
CLASS-ADJUST 10-24
CLASS-MAP 10-26
CLEAR 10-27
CLOCK 10-28
CONNECTS-TO 10-31
COPY 10-32
CUSTOM-APPLICATION 10-35
CUSTOM-DASHBOARD 10-37
DECAPSULATE 10-38
DELETE 10-40
DESCRIPTION 10-41
DIR 10-42
DISPLAY 10-43
DOMAIN 10-44
DOWN 10-45
DURATION 10-47
ETHERNET 10-48
EXIT 10-49

FILTER-CLASS 10-50
GPS 10-52
GRAPH 10-53
GRAPH-ORDER 10-55
HELP 10-57
INTERFACE 10-59
LICENSE 10-60
LINK-ADJUST 10-61
LOCAL-SITE 10-63
LOG 10-64
LOGGING 10-65
MATCH 10-66
MATCH ANY 10-68
MATCH APPLICATION 10-69
MATCH CLASS-MAP 10-71
MATCH ETHERTYPE 10-72
MATCH GRE 10-74
MATCH IP 10-75
MATCH MPLS 10-78
MATCH TCP 10-80
MATCH UDP 10-83
MATCH VLAN 10-86
MAX-RESERVED-BANDWIDTH 10-89
MEASURE-BANDWIDTH 10-90
MEASURE-EQ 10-92
MEASURE-ICMP 10-93
MEASURE-MICROBURST 10-95
MEASURE-PNQM 10-97
MEDIA 10-98
NSO 10-99
NSO-MAP 10-101
MORE 10-102
NO 10-104
NTP 10-106
ONE-WAY-LATENCY 10-107
PASSWORD 10-108
PEER-INTERFACE 10-109
PING 10-111
PING-ADDRESS 10-113
PING-ADDRESS-TEST 10-114
PNQM-SERVER 10-115
PNQM-SERVER-TEST 10-117
PNQM-SETTINGS 10-118
POLICY-MAP 10-119
PORT 10-120
PPP 10-121
PRIORITY 10-122
PRIORITY-LEVEL 10-123
PROTECT-PACKETS 10-125
QUEUEING-TARGETS 10-127

QUEUE-LIMIT 10-128
RELOAD 10-129
RENAME 10-130
RESTORE 10-131
ROUTER 10-132
SERVICE 10-133
SERVICE-POLICY 10-134
SETUP 10-135
SHOW 10-136
SHUTDOWN 10-146
SITE 10-147
SIZE 10-148
SNAPLENGTH 10-149
SNMP-SERVER 10-150
START 10-155
START CAPTURE 10-156
STATUS 10-157
SUBNET 10-160
SUBNET-FILTERING 10-163
TERMINAL 10-167
TRACE-EVENTS 10-168
TRACEROUTE 10-169
UP 10-170

11 APPENDIX A: CLASS-MAPS AND CLASSIFICATION 11-1

MATCHING CUSTOMER TRAFFIC 11-1
MATCHING PRIORITIZED TRAFFIC 11-1
MATCHING APPLICATION TRAFFIC 11-2
CLASS-MAP LOGIC 11-3

12 APPENDIX B: COMMON APPLICATION STATIC PORT ASSIGNMENTS 12-1

13 APPENDIX C: SUPPORTED PROTOCOLS 13-1

14 APPENDIX D: ETHERTYPE IDENTIFIERS 14-1

15 INDEX



Preface

About this Guide

This User Guide describes how to do the following:

- Identify the basic BQM GUI and CLI features
- Configure the BQM network model using either the GUI or CLI
- Monitor network traffic statistics
- Analyze network performance events
- Size links for bandwidth requirements
- 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 and Cisco router configuration, is assumed.

Related Documentation

For more information on installing and getting started with BQM, 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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



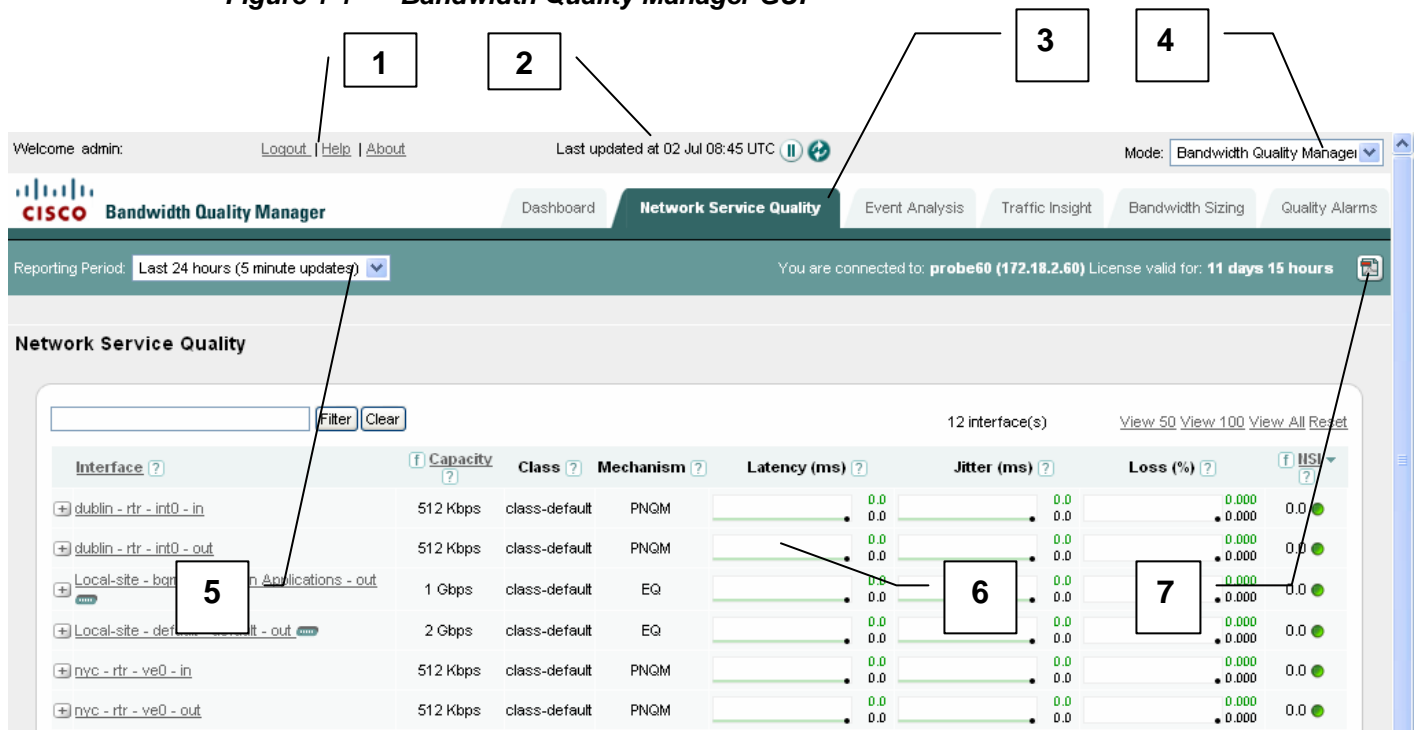
1 Bandwidth Quality Manager Overview

Cisco Bandwidth Quality Manager (BQM) provides end-to-end network service quality monitoring with unique visibility and analysis of traffic, bandwidth and service quality on IP access networks. You use BQM to monitor, troubleshoot and assure end-to-end network performance objectives for converged application traffic.

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

BQM runs on the Cisco ADE 1010, 2120, 2130, and 2140 series appliances. Each device attaches to a 10/100/1000 Ethernet network segment and performs the unique Corvil traffic measurement. The Cisco ADE supports a powerful filter classification engine that allows measurements to be carried out on specified traffic classes and/or application streams. BQM 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 Option to change the reporting period from the default view of the last 24 hours.
- 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 BQM: **Bandwidth Quality Manager** and **System Administration**. The monitoring user (monitor) has access to all the monitoring features of BQM, but does not have access to **System Administration** mode to perform configuration tasks.

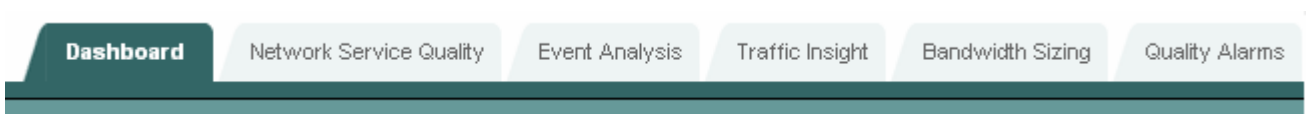
In general you use the dashboard or the **Network Service Quality** tab to monitor traffic. If a high Network Service Index value is displayed or if a quality alarm is triggered, you can view the end-to-end measured latency and loss results and the Expected Queuing calculations for the impacted interface.

To investigate an event further, you switch to the **Event Analysis** tab and drill in to the details.

Monitoring Network Service Quality

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

Figure 1-2 *Dashboard Tab*

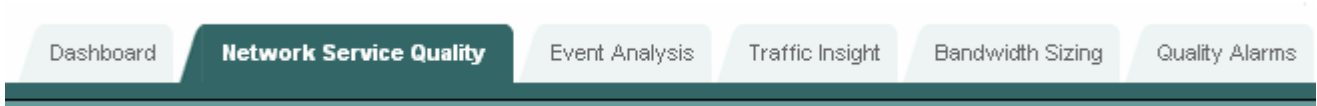


The information available from the dashboard includes:

- Network Service Quality – the top ten most impacted interfaces as calculated by BQM.
- Top Applications - the top ten applications with the highest traffic volume automatically discovered by BQM.
- Recent Alarms - the most recent alarms triggered by quality events in the network.

You use the **Network Service Quality** tab to focus on monitoring end-to-end packet latency and loss for all of the interfaces you have configured in the BQM network model.

Figure 1-3 Network Service Quality Tab



You can use the displayed Network Service Index values to identify the network service level on each interface. A Network Service Index value greater than 1 means that loss or latency is above an acceptable level, as specified in the BQM configuration. A Network Service Index of less than or equal to 1 means the loss or latency is better than that specified.

For each interface displayed you can view the following graph results per class, if configured:

- End-to-End Latency
- End-to-End Jitter
- End-to-End Loss
- Expected Queuing Latency
- Expected Queuing Delay Variation
- Expected Queuing Loss



Note For more information on monitoring network service quality with the **Dashboard** and **Network Service Quality** tabs, see the chapter “Monitoring Network Service Quality.”

BQM 4.0 introduces the ability to define and populate a custom dashboard. Once defined, the custom dashboard tab displays end-to-end network service quality monitoring results for a specified group of traffic classes.

Figure 1-4 Custom Dashboard Tab



The graph results displayed for each class are also specified in the configuration.



Note For more information on configuring the custom dashboard with the GUI, see the chapter “Configuring Network Service Quality Monitoring.”

For more information on viewing custom dashboard results, see the chapter “Monitoring Network Service Quality.”

Analyzing Network Service Quality Events

You use the **Event Analysis** tab to investigate network service quality events for all of the interfaces you have configured in the BQM network model.

Figure 1-5 *Event Analysis Tab*



As on the previous tab, Network Service Index values to identify the network service level on each interface. If network service quality events have occurred for any interface, they are displayed here. You can drill down to investigate individual events and review associated end-to-end measurements, expected queuing results, millisecond microburst results, and traffic data (for example, top applications and top talkers).



Note For more information on analyzing and investigating network service quality events using the **Event Analysis** tab, see the chapter “Analyzing Network Events.”

Monitoring Network Traffic Statistics

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

Figure 1-6 *Traffic Insight Tab*



The traffic statistic graphs available for each interface and its associated classes 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.

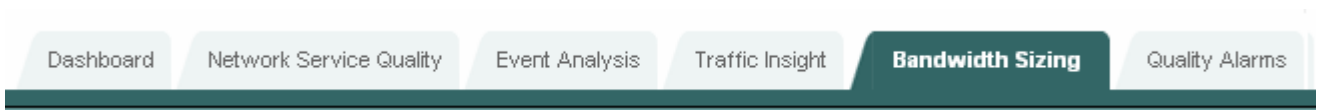


Note For more information on monitoring network traffic statistics using the **Traffic Insight** tab, see the chapter “Monitoring Network Traffic.”

Bandwidth Sizing

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 1-7 *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 least 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.



Note For more information on working with bandwidth sizing using the **Bandwidth Sizing** tab, see the chapter “Bandwidth Sizing.”

Using Live View and Related Links

When you view results for a particular interface on the **Network Service Quality**, **Event Analysis**, **Traffic Insight**, or **Bandwidth Sizing** tabs, you can move directly to live results with per-second updates for that same interface by clicking **Live View**.

Figure 1-8 *Related Links Between Tabs*

Related Links: **Network Service Quality** | [Event Analysis](#) | [Traffic Insight](#) | [Bandwidth Sizing](#) | [LIVE VIEW](#)

Live view results are displayed in a new window and comprise the following:

- Interface Microburst and average rate
- Class Microburst and average rate
- End-to-End Latency
- End-to-End Jitter
- End-to-End Loss
- Expected Queuing Latency
- Expected Queuing Delay Variation
- Expected Queuing Loss
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length



Note For more information on working with live view, see the chapter “Monitoring Network Service Quality.”

When you view results for a particular interface on the **Network Service Quality**, **Event Analysis**, **Traffic Insight**, or **Bandwidth Sizing** tabs, you can move directly to results for that same interface on one of the other tabs by clicking one of the available related links.



Note Not all interfaces are displayed on the **Bandwidth Sizing** tab. If you are viewing one of these interfaces on the other tabs, the **Bandwidth Sizing** link is not available. For more information on which interfaces are available for bandwidth sizing, see the section “Viewing Network Service Quality Results” in the chapter “Monitoring Network Service Quality.”

Viewing Quality Event Alarms

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

Figure 1-9 Quality Alarms Tab



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



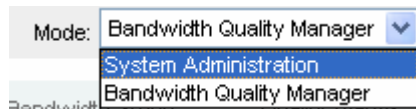
Note For more information on working with quality alarms, see the section “Monitoring Quality Alarms” in the chapter “Monitoring Network Service Quality.”

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 1-10 GUI Mode Options for Admin Users



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

BQM Configuration and Administration

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

Figure 1-11 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
- Network service objectives – enable and configure end-to-end BQM QoS monitoring features for class traffic
- Applications – configure custom applications to match those on your network and supplement the automatically discovered set supported by BQM
- Custom dashboard – define a tab to display a specified set of graph results for a specified set of traffic classes in **Bandwidth Quality Manager** mode.



Note For more information on configuring BQM using the GUI, see the chapter *Configuring Network Service Quality Monitoring*.”

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

Figure 1-12 System Alerts Tab

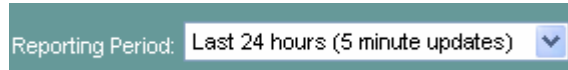


Note For more information on working with system alerts, see the section “Diagnostics” in the chapter *“System Administration.”*

Selecting a Reporting Period

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

Figure 1-13 *Selecting a Report Period*



You can choose different reporting periods by clicking the **Reporting Period** list. The following reporting periods (and associated data 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.

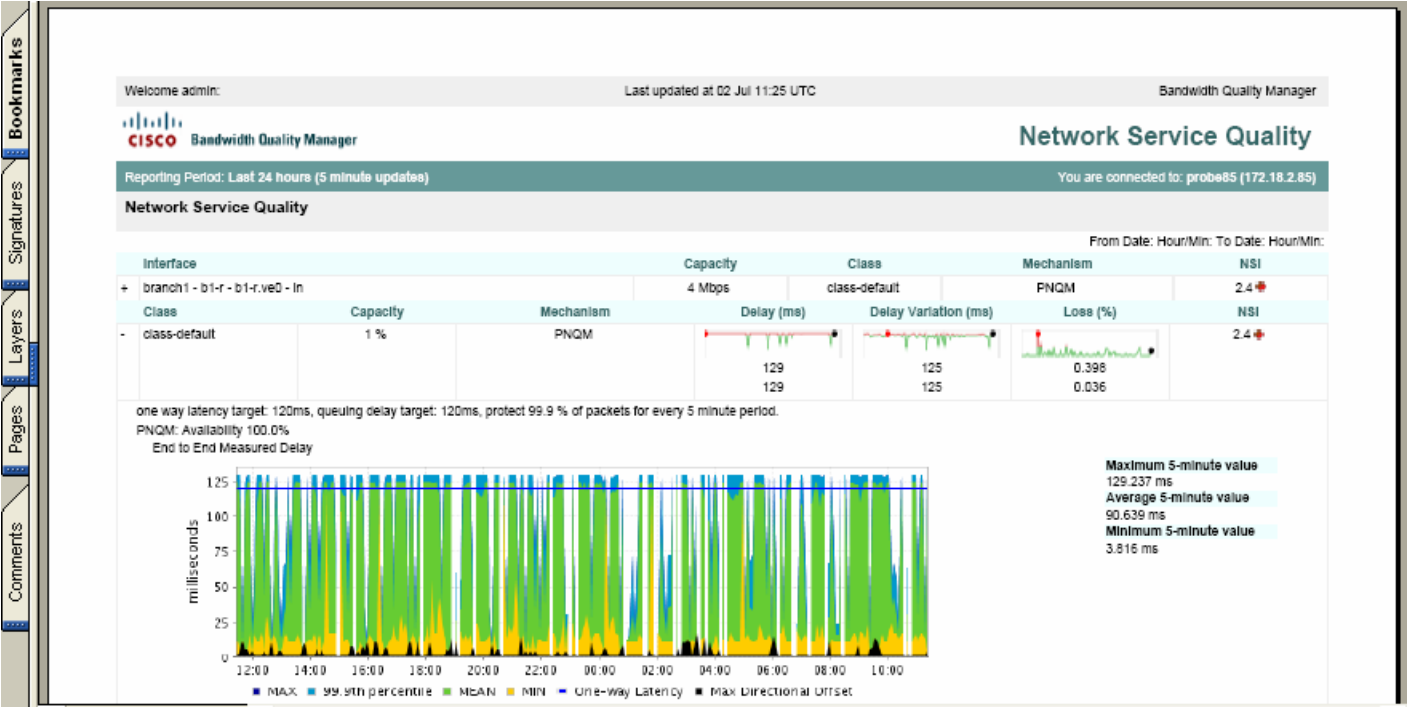
Generating Reports

You can generate a report in .pdf format at any point when viewing information on the **Network Service Quality**, **Event Analysis**, **Traffic Insight**, **Bandwidth Sizing**, or **Quality Alarms** tabs.

To generate a report, click .

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

Figure 1-14 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 Network Service Index 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 BQM time zone.



2 Configuring Network Service Quality Monitoring

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

- Overview
- Configuring Network Service Quality Monitoring Features
- Configuring Class Maps
- Configuring Policy Maps
- Configuring Custom Applications
- Configuring Sites, Routers, and Interfaces

Overview

With this release the BQM product line provides Network Service Objective Management (NSOM). The previous release focused on one of the primary areas impacting the delivery of NSOM – the service impact of traffic on QoS mechanisms at selected speed mismatch points in the network; essentially at WAN links. BQM 4.0 extends this capability with features which manage service quality across the entire network.

BQM 4.0 appliances provide the measurement and instrumentation, and the BQM 4.0 software provides the analysis and presentation functionality also required to manage end-to-end network service quality.

NSOM comprises the following features:

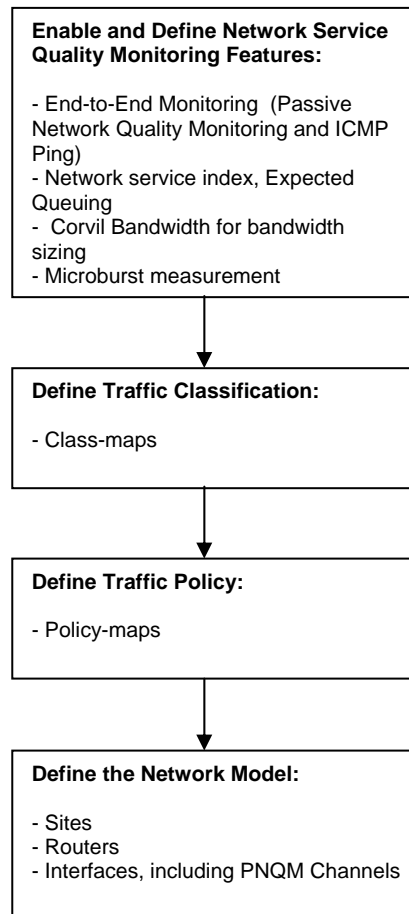
- Definition of appropriate network service objectives for each service.
- Continuous monitoring of the network and services to ensure the objectives are being met.
- Where the objectives are not being met, recommending the appropriate action to restore the delivery of the service objectives.

BQM 4.0 enables a combination of per-link and per-class service objective settings

BQM 4.0 offers both passive and active options for end-to-end monitoring. This allows you to choose your own trade-off between cost and visibility. Also, by offering Expected Queuing, BQM 4.0 enables you to determine how to make that trade-off.

By uniquely identifying what portion of the loss and latency are attributable to specific links and QoS policies, and which are service provider cloud issues, BQM 4.0 offers diagnostic information unavailable elsewhere, which should save money both in troubleshooting time and in useless upgrades.

Configuring BQM comprises the following tasks:



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

If you are performing a configuration using the CLI or GUI, you need to define network service objectives 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 network service objectives and class-maps are referenced during policy-map configuration, and policy-maps are in turn referenced during interface configuration.

Configuring Network Service Quality Monitoring Features

The BQM product provides network service objective monitoring results and alerting based on both end-to-end and per-hop measurements. To view these results you need to configure network service objectives. Network service objectives are not found on Cisco routers; they are specific to the BQM configuration. Network service objectives enable service quality monitoring features and define the quality thresholds used to report on traffic, for example, the maximum one-way latency and per-hop queuing latency that a class can tolerate.

Enabling End-to-End Monitoring with Network Service Objectives

User experience of network applications depends on many factors. These include user expectations, application design, server response and network response. Based on user expectations and the application design, both the servers and the network must behave in a manner to provide adequate performance under expected load conditions. For the network, this required performance is defined in terms of metrics like packet loss, latency, latency variation, throughput, and so on.

For some applications, establishing the relationship between these parameters and user experience is more straightforward than for others. For example, for IP telephony it is generally accepted that one-way latency of 150ms, jitter of approximately 20-30ms, and loss of about 1% is the threshold beyond which user experience starts to degrade significantly. However, for applications like SAP and Citrix, the relationship is more complex and can depend, for example, on the number of roundtrips required to complete a transaction. Since this can change from one version of an application to another, and since tens or hundreds of applications can co-exist on a network at any time, many of these developed in-house, it is virtually impossible to choose what metrics each application requires, and to design a network to meet them all. Thankfully, it is also not necessary.

BQM defines network service objectives in terms of a latency target in milliseconds, a latency variation target in milliseconds, and a percentage of packets that must not be lost and must meet these latency and latency variation targets. These targets can be specified per class.

Because BQM also measures with very high granularity and accuracy the latency, loss and latency variation that a class is receiving, over time you can fine-tune the appropriate objectives for the classes that it is measuring by base-lining against network users who are satisfied with performance. These ‘learned’ values can then form the basis for the service objectives for these classes in the rest of the network.

To enable end-to-end BQM Monitoring features and view results for these features, there must be a network service objective applied to each interface and class in the BQM configuration.

The network service objective defines the required network-wide QoS monitoring features, and associated event detection thresholds, for application to traffic classes. A network service objective comprises the following: a name, one-way latency target, packet protection target, expected queuing settings, queuing target, Corvil Bandwidth and microburst settings, and associated quality event detection thresholds. A network service objective establishes the set of end-to-end, QoS-aware monitoring features, and an associated event detection policy, enabled for the classified traffic.

When the network service objectives have been defined and assigned (via policy-maps) to interfaces and classes, BQM 4.0 monitors whether these objectives are being met by the network. The following technologies are used for this purpose:

Passive Network Quality Monitoring – passive measurement of one-way latency, latency variation and loss. Passive Network Quality Monitoring (PNQM) takes accurate timestamps of streams of packets as they pass two locations in the network where BQM appliances are installed. The timestamps are compared at the local BQM appliance, and highly accurate measurements of the latency, loss and latency variation experienced by the packet stream between the two locations are available. The feature can be configured to measure all

packets, or to measure a sample of packets. If all packets are measured, then all latency and loss violations of the network service objective will be observed. If sampling is used, then the visibility is somewhat reduced.

When you assign a policy-map to an interface, the monitoring mechanisms that have been defined in the network service objective are enabled for the interface, along with the mechanism-specific configurations that were defined for that network service objective.

Expected Queuing

Expected Queuing (EQ) estimates the loss and queuing latency that classes and applications can expect to incur when they interact with the queues and schedulers in the network. Although Expected Queuing focuses on the principal speed mismatch points in the network, rather than an end-to-end view, it is true to say that if the end-to-end target is violated in the EQ-modeled queue, then it will be violated end-to-end for the application traffic.

ICMP Ping – active measurement of roundtrip time and packet loss

Although ICMP pings will not catch all loss and latency violations that the application traffic may incur, it is highly likely that if the ICMP ping results violate the end-to-end network service objective, then it will be violated for the end-to-end application traffic.

Default Network Service Objective

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

The default network service objective comprises the following settings:

- One-way latency target of 500ms
- Packet protection target of 99.9% of packets in every 4-hour period
- Passive Network Quality Monitoring (PNQM) and associated event detection on latency and loss enabled
- ICMP Ping and associated event detection enabled on a roundtrip threshold of twice the one-way latency
- Expected Queuing (Expected Queuing Latency and Loss graphs) enabled, so if the calculated expected queuing latency value exceeds 500 ms (or if any loss is detected), an event is triggered.
- Corvil Bandwidth calculation enabled for bandwidth sizing using a queuing delay target of 500 milliseconds (as per the default one-way latency target), loss protection, and the packet protection target; event detection is enabled for Corvil Bandwidth values exceeding 100% of the interface capacity.
- Micro Burst enabled at 50ms resolution with shape detection

So using the default network service objective means that you can see the following **Network Service Quality** tab results:

- Network Service Index values
- End-to-end measured latency, loss, and jitter graphs
- Expected Queuing Latency, Loss, and Delay Variation graphs
- Roundtrip Delay and Loss graphs

The network service objective effectively establishes an end-to-end latency and loss-based event detection policy for traffic between sites.

Using the default network service objective means that you can see the following **Event Analysis** tab results:

- Network Service Index values
- End-to-end measured latency, loss, and jitter graphs
- Expected Queuing Loss and Latency graphs
- Corvil Bandwidth Delay graphs



Note The **Event 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. This bandwidth is an upper-bound on the bandwidth required to protect the packets against tail drop.

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.

Microburst measurement is enabled in the default network service objective. However, no microburst-related events will be displayed in the **Event Analysis** screen for interfaces or classes using the default map.

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

You can also view **Bandwidth Sizing** tab results for certain interfaces.

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 BQM features, for example Event Analysis or Bandwidth Sizing, you need to disable the relevant parameter(s) in any network service objective that is being applied to a given interface or class.

If you want to disable or edit settings for individual monitoring mechanisms for individual classes, you define a new network service objective (for example, by duplicating the current one, renaming it and editing the details) and assign it to the relevant class by editing the relevant policy-map.

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

To enable BQM microburst event detection without enabling any other features of the product, you configure only a microburst measurement resolution and event detection threshold in the network service objective.

Configuring a Network Service Objective

To configure a network service objective, you must be logged in as an administrative user. From **System Administration** mode, you click the **Configuration** tab (if it is not already open). To begin configuring network service objectives click **Network Service Objectives**.

The purpose of a network service objective is to define the required network-wide service quality monitoring features, and associated event detection thresholds, for application to traffic classes. A network service objective comprises the following: a name, one-way latency target, packet protection target, expected queuing, queuing target, Corvil Bandwidth and microburst settings, and associated quality event detection thresholds. A network service objective establishes the set of QoS-aware monitoring features, and an associated quality event detection policy, enabled for the classified traffic.

You can define network service objectives in the GUI from the **Network Service Objectives** page in the **Configuration** tab.

Figure 2-1 Configuring Network Service Objectives

The screenshot shows the Cisco Bandwidth Quality Manager GUI. The top navigation bar includes 'System Administration' and 'Bandwidth Quality Manager'. The 'Configuration' tab is active. The left sidebar shows 'NETWORK' and 'MONITORING' sections. Under 'MONITORING', 'Network Service Objectives' is selected. The main content area is titled 'Network Service Objectives' and contains a table of configured objectives.

Name	One Way Latency Target	One Way Maximum Latency Variation Target	Packet Protection Target	Actions
high-speed	500 ms	-	99.90000% of packets over a 5 minute period	edit duplicate delete
low-speed	500 ms	-	99.90000% of packets over a 5 minute period	edit duplicate delete
network-service-objective-default	500 ms	-	99.90000% of packets over a 4 hour period	edit duplicate delete
real-time	500 ms	-	99.90000% of packets over a 5 minute period	edit duplicate delete

4 Network Service Objective(s)

Copyright © Cisco 2007 All Rights Reserved

The **Network Service Objectives** page displays the current list of configured network service objectives in the system.

The following table describes the information displayed on the page:

Table 2-1 Network Service Objectives Page

Field	Description
Name	<p>Displays the name of the network service objective. The system has a number of pre-configured network service objectives:</p> <ul style="list-style-type: none"> • high-speed • low-latency • low-speed • network-service-objective-default • real-time
One Way Latency Target	<p>Displays the configured (or default) one-way latency target.</p> <p>The one-way latency target represents the maximum tolerable latency for packets traversing one direction of the path between two configured sites.</p>
One Way Maximum Latency Variation Target	<p>[Optional] Displays the maximum latency variation target, if configured. Otherwise, the value defaults to the one-way latency target.</p> <p>The one-way maximum latency variation target represents the maximum tolerable latency variation for packets traversing one direction of the path between two configured sites.</p>
Packet Protection Target	<p>Displays the configured percentage of packets in each busy period that must meet the configured quality targets.</p> <p>The packet protection targets enable you to permit a fraction of the packets during a defined timescale, or <i>busy period</i>, to violate the configured end-to-end and queuing targets. Permitting a certain fraction of the packets to violate the end-to-end latency and queuing targets allows a statistical softening of the required bandwidth down from that needed to guarantee no loss or latency 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 end-to-end latency no greater than the configured latency target (or a per-hop queuing latency no greater than the configured queuing latency value).</p> <p>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</p>

	sizing calculation takes every 30-minute period of traffic into account. The resulting sizing calculation is sufficient to ensure that the configured 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 target.
Actions	edit – click to edit network service objective details duplicate – click to duplicate the details of the selected network service objective in a new map delete – click to delete the network service objective.

Click  to view the advanced configuration details for a given listed network service objective.

Table 2-2 Network Service Objectives – Advanced Configuration Details

Field	Description
Description	[Optional] Displays the description text for the network service objective, if configured.
Passive Network Quality Monitoring (PNQM)	Displays whether PNQM is enabled or disabled and lists the PNQM sample rate, and related event detection configuration status.
ICMP Ping	Displays whether ICMP Ping is enabled or disabled and lists the ping interval, roundtrip latency target, ping packet size, and related event detection configuration status.
Expected Queuing	Displays whether Expected Queuing is enabled or disabled, and related event detection configuration status.
Corvil Bandwidth	Displays whether Corvil Bandwidth measurement is enabled or disabled and related event detection configuration status.
Queuing Target	Displays whether queuing and loss targets are enabled or disabled, and lists the details of queuing latency and loss target configuration.
User Micro-burst	Displays whether microburst measurement is enabled or disabled and lists the configured minimum microburst duration, event detection configuration status, and whether the shape detection algorithm is enabled or disabled.

Filtering the List of Network Service Objective

You can filter the displayed list of network service objectives. To filter the displayed list based on filter text you do the following:

-
- Step 1** Enter the name or part of a name in the filter field.
- Step 2** Click **Filter**.
-

The new filtered list of network service objectives is displayed. To return to the default display of all network service objectives, click **Clear**.

Defining a Network Service Objective

When you define a network service objective and then assign it to a class, you are effectively enabling BQM features such as End-to-End Latency and Loss, Expected Queuing Latency and Loss and Network Service Index calculation, Corvil Bandwidth, and Microburst detection. For more information on the relationship between the configurable parameters and the BQM features, see the section “Enabling End-to-End Monitoring with Network Service Objectives.”

To open the **Add Network Service Objective** page and define a new network service objective, you do the following:

-
- Step 1** Click **Add Network Service Objective**.

Figure 2-2 Basic Network Service Objective Settings

Add Network Service Objective

* Name:

Description:

Latency and Loss Targets

* One-way Latency: ms

One-way Maximum Latency Variation: ms

* Packet Protection: % of packets over a

Advanced Settings *(Passive Network Quality Monitoring, ICMP Ping, Queuing Target, Expected Queuing, Corvil Bandwidth, User Micro-burst)*

- Step 2** Enter a unique name for the network service objective in the **Name** field.
- Step 3** Enter a brief text description for the network service objective in the **Description** field.
- Step 4** Enter a one-way latency target in milliseconds in the **One-way Latency** field. [Range: 1 - 10000ms]
- The value configured here is used by default as the basis for advanced settings, including the ICMP roundtrip target (2x the one-way latency value) and the queuing delay target (same as one-way latency) used for bandwidth sizing.
- Step 5** Enter a maximum value for the tolerable latency target variation in milliseconds in the **One-way Maximum Latency Variation** field. [Range: 1 - 10000] This step is optional. If you do not configure a value here, the system uses the one-way latency target as a default value.
- Step 6** Enter a packet protection target specifying a percentage of packets [Range: 0 - 99.99999%] and a busy period from the available list. The percentage value determines the percentage of traffic (for example 99.9999%) that must meet the configured targets. The busy period is the timescale that has historically seen the greatest volumes of traffic.
- The packet protection target is used to calculate the Network Service Index and also for bandwidth sizing calculations.

If you name a new network service objective and click **Save** without configuring any details, the network service objective will contain the default settings. The default settings are as follows:

- One-way Latency: 500ms
- Passive Network Quality Monitoring (PNQM): enabled with a 4 packets per second sampling rate and event detection on latency and loss enabled
- ICMP Ping: enabled with a ping packet size of 36 bytes, inter-packet interval of 10 seconds, and event detection enabled on a roundtrip threshold of twice the one-way latency
- Bandwidth Sizing policy: protect 99.9% of packets in every 4-hour period
- Expected Queuing (Expected Queuing Latency and Loss graphs): enabled
- Queuing Targets: delay 500 milliseconds (as per the one-way latency target) and loss protection enabled
- Corvil Bandwidth Monitoring: enabled
- Micro Burst: enabled (50 ms with shape detection)


To configure advanced settings, or review the defaults, click .

Figure 2-3 PNQM Configuration

☒ **Passive Network Quality Monitoring**

* Sample: ☒ All Packets ☐ packets per second

☐ Generate events when latency exceeds threshold

☐ Generate events when delay variation exceeds threshold

☐ Generate events when loss occurs

Configuring Passive Network Quality Monitoring (PNQM)

To enable PNQM, you do the following:

-
- Step 1** Check the **Passive Network Quality Monitoring** check box and set a sample rate. You can choose to sample all packets or specify a sample rate in packets per second.
- Step 2** To trigger event detection based on latency or latency variation exceeding the values configured previously, or when loss occurs, check the relevant check box.
-

Figure 2-4 ICMP Configuration

☒ **ICMP Ping**

* Interval: ms (500-1000000)

* Roundtrip delay target: ☒ Use twice the one-way latency target ☐ ms

* Packet Size: bytes (36-1500)

☐ Generate events when roundtrip delay exceeds threshold

☐ Generate events when loss occurs

Configuring ICMP Ping

To enable ICMP Ping, you do the following:

-
- Step 1** Check the **ICMP Ping** check box and set the following:
- an inter-packet interval in the **Interval** field [Range: 500 - 1000000ms]
 - a roundtrip latency target by choosing either the previously configured one-way latency target or specifying a value in milliseconds [Range: 1 - 10000ms]
 - a ping packet size in the **Packet Size** field [Range: 36 - 1500 bytes]
- Step 2** To trigger event detection when roundtrip delay exceeds the values configured previously, or when loss occurs, check the relevant check box.
-

Figure 2-5 Expected Queuing and Corvil Bandwidth Configuration

☒ **Expected Queuing** ?

☐ Generate events when delay exceeds threshold

☐ Generate events when loss occurs

☒ **Corvil Bandwidth** ?

☒ Generate events when Corvil Bandwidth exceeds % of interface capacity (1-1000)

Queuing Target

* Queuing Delay: ☒ Use one way latency ms ?

* Queuing Loss: ☒ Use packet protection % of packets

Configuring Expected Queuing and Corvil Bandwidth

To enable the calculation and display of expected queuing latency and loss results and Corvil Bandwidth calculation for bandwidth sizing, you do the following:

-
- Step 1** Check the **Expected Queuing** check box.
 - Step 2** To enable event detection when the calculated queuing latency exceeds the configured delay target, check the **Generate events when delay exceeds threshold** check box. The queuing delay target you configure, which may be based on the one-way latency target, 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.
 - Step 3** To enable calculation of Corvil Bandwidth values for bandwidth sizing, check the **Corvil Bandwidth** check box.
 - Step 4** To set a Corvil Bandwidth threshold, at which event detection is triggered, enter a value in the **Generate Events when Corvil Bandwidth Exceeds** field as a percentage of the link bandwidth [Range: 1 - 1000%] or in kbps [Range: 1 - 10000000 kbps].
 - Step 5** To configure queuing QoS targets for expected loss and latency and Corvil Bandwidth calculations, choose the previously configured one-way latency value or enter a queuing delay target in milliseconds in the **Queuing Delay** field. [Range: 1 - 10000 ms]
 - Step 6** For queuing loss you choose either a value derived from the previously configured packet protection target or you enter a percentage of packets that must not be lost in the **Queuing Loss** field. [Range: 0 - 99.99999%]

For example, specifying 99% here means that packet loss must not exceed 1%.



Note .. Corvil Bandwidth calculations also use the previously configured packet protection target. Only one set of queuing targets and packet protection target values are specified in a single network service objective.



Note .If you want to disable Expected Queuing calculation you must disable EQ in all classes and also at the interface level. The interface level usually has the default network service object applied.

When you attempt to disable EQ you should use the **show policy-map**, or **show detailed-config CLI** commands to check and ensure that both network service objectives used by the class and interface have EQ disabled.

Figure 2-6 Microburst Configuration

☒ **User Micro-burst** ?

* Minimum Duration: (5ms - 10000ms) ?

☐ Generate Events on micro-bursts % of interface capacity (1-1000) ?

☐ Use shaping detection algorithm ?

Configuring Microburst

The default BQM microburst measurement resolution is five milliseconds. You can override this default setting by enabling user microburst measurement and setting your own minimum duration in milliseconds. To configure the user microburst value and associated event detection, you do the following:

- Step 1** Check the **User Micro-burst** check box.
- Step 2** Enter a minimum millisecond resolution for peak measurements in the **Minimum Duration** field (Range: 1 - 10000 ms).

- Step 3** To configure a threshold value at which to trigger event detection, enter a value in the **Generate events on micro-bursts** field as either a percentage of the link bandwidth (Range: 1 - 1000) or in kbps (Range: 1 - 10000000).
- Step 4** 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.

To save the network service objective, click **Save**. The new network service objective is saved and displayed on the **Network Service Objectives** page. The network service objective is available to select when defining policy maps.

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.

Configuring Class Maps

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

Figure 2-7 Class Map Configuration

Class Maps						
<input type="text"/>		<input type="button" value="Filter"/>	<input type="button" value="Clear"/>	<input type="button" value="Add New Class Map"/>		
Name ▲	TCP/UDP Rule(s)	TOS Rule(s)	Application Rule(s)	Class Map Rule(s)	Advanced Rule(s)	Actions
<input type="checkbox"/> class-default	-	-	-	-	ANY	duplicate
<input type="checkbox"/> unknown-applications	-	-	Application: Unknown	-	-	edit duplicate delete
2 class map(s)						

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 2-3 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. If there are multiple match rules of this type defined, the number of this type of match rule defined in the class-map is displayed.
TOS Rules	Displays a summary if a single Type of Service (ToS) match rule (IP Precedence, ToS, DSCP) is defined. If there are multiple match rules of this type defined, the number of this type of match rule defined in the class-map is displayed.
Application Rule(s)	Displays a summary if a single application match rule is defined. If there are multiple match rules of this type defined, the number of this type of match rule defined in the class-map is displayed.
Class map Rule(s)	Displays a summary if a single match rule referencing other class-maps is defined. If there are multiple match rules of this type defined, the number of this type of match rule defined in the class-map is displayed.
Advanced Rule(s)	Displays a summary if a single advanced match rule (IP Protocol, MPLS, vLAN, Ethertype) is defined. If there are multiple match rules of this type defined, the number of this type of match rule defined in the class-map is displayed.
Actions	edit – click the link to edit the class-map configuration. Not available for class-default. duplicate – click the link to duplicate the class-map configuration. delete – click the link to delete the class-map. Not available for class-default.



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 2-8 Class Map Configuration

Add Class Map

Add Class Map

* Name:

Description:

Match Rules

☒ Traffic can match ANY of the rules ☐ Traffic must match ALL the rules

Define Rule for Class Map...

Save Cancel

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

-
- Step 1** Click **Add New 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.



Note We recommend that if you define class-map match rules in the GUI, you edit them using the GUI. If you define match rules using the CLI, edit them using the CLI.

Figure 2-9 *Defining a Match Rule*

Match Rule

* Class Map: low_speed

TCP/UDP

☐ Match all traffic except the following IP addresses and ports.

Protocol	Source Address	Source Port	Destination Address	Destination Port
Both TCP and UDP	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
	Example: 192.168.1.0/24	Example: 118,200-210	Example: 192.168.1.0/24	Example: 118,200-210

Save Cancel

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 IP addresses and ports**.

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

Figure 2-10 *Defining a Match Rule - Applications*

Match Rule

* Class Map: voice

Application

☐ Match all traffic except traffic matching the selected application.

Application: Any

URL: ?

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



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 2-11 Defining a Match Rule - TOS

Match Rule

* Class Map: voice

TOS ▼

☐ Match all traffic except the following.

IP Precedence: Any ▼

TOS: Any ▼

DSCP: Any ▼ (When set, IP Precedence and TOS values will be ignored.)

To match all traffic except the IP Precedence, TOS, or DSCP 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 2-12 Defining a Match Rule – Class Map

Match Rule

* Class Map: voice

Class Map ▼

☐ Match all traffic except traffic matching the selected class map.

Class Map: class-default ▼

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

- 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 2-13 Defining a Match Rule – Advanced

Match Rule

* Class Map video

Advanced ▾

☐ Match all traffic except the following.

IP Protocol

☐ Protocol Any ▾

☐ Source Address

☐ Source Port

☐ Destination Address

☐ Destination Port

VLAN

☐ VLAN Id (0 - 4094)

☐ VLAN Priority (0 - 7)

MPLS

☐ Label (1-4) from top of stack ▾

☐ Experimental Value 1-7

☐ Label Value 0 - 1,048,575

☐ Stack Size 1 - 4 labels in the stack

Ethertype

☐ Any ▾ (0x0000-0xFFFFE)

Any

☐ Match All Packets

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

- Step 11** Click **Save**.
- 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.

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 event detection thresholds (previously defined by network service objectives). 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.

Configuring Policy Maps

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

Figure 2-14 Policy Maps

NAME	CLASSES	NETWORK SERVICE OBJECTIVES	INTERFACES USING POLICY MAP	ACTIONS
default	1	network-service-objective-default	12	duplicate

1 policy map(s)

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 2-4 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.
Network Service Objectives	Displays the name of the network service objective 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. Not available for the default policy-map. duplicate – click the link to duplicate the policy-map configuration in a new policy-map. delete – click the link to delete the policy-map. Not available for the default 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 2-15 Policy Map Configuration

Add Policy Map

Policy Map General Properties

Name:
Enter a unique name for the policy map.

Description:

Network Service Objectives:
?

Queuing Configuration:
☒ Cisco Modular QoS CLI
☐ Strict Priority Queuing
?

Define Class...

Class Map	Network Service Objectives	Queue Type	Reserve Bandwidth
class-default			

1 classes

Save Cancel

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 network service objective to the policy-map, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.

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 network service objective to the policy-map, that is, at interface level, select a network service objective from the list. If you have not configured any network service objectives, the list contains only preconfigured network service objectives and the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.
- Step 5** Select **Strict Priority Queuing**.
- Step 6** Click **Define Class**.
- The **Add Class** page is displayed.

Figure 2-16 **Configuring a Strict Priority Queuing Class****Add Strict Priority Class**

* Policy Map:	strict
* Class Map:	unknown-applications ▼
Network Service Objectives:	high-speed ▼ ?
Priority Level:	High ▼
Queue Limit:	<input type="text"/> leave blank to let system assign default
+ Packet Size Adjustment	

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 preconfigured class-map named unknown-applications. See the section “Configuring a Class Map” for more information on defining class-maps.

Step 8 If you are applying a network service objective to the class, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the preconfigured network service objectives and the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.



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 setting a priority level:

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 (Range: 16 – 100000 packets). If you leave the field blank, the system uses the default value of 64 packets.



Note The **Event 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 - corresponds to a byte adjustment value of -36.
no-udp-checksum - corresponds to a byte adjustment value of -38. This is the default.

- 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.



Note You cannot change the queuing configuration (Cisco Modular QoS CLI or Strict Priority Queuing) by editing a defined policy-map. To change the queuing configuration you must delete the policy-map and redefine it.

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 network service objective to the policy-map, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.
- Step 5** Select **Cisco Modular QoS CLI**.
- Step 6** Click **Define Class**.

Figure 2-17 Configuring a Cisco Modular QoS CLI Class

Add Class

* Policy Map:	test	
* Class Map:	<input type="button" value="v"/>	
Network Service Objectives:	network-service-objective-default <input type="button" value="v"/> <input type="button" value="?"/>	
Queue Type	<input checked="" type="radio"/> Bandwidth <input type="radio"/> Priority <input type="button" value="?"/>	
* Bandwidth	<input type="text" value="0"/>	kbps <input type="button" value="v"/>
Queue Limit:	<input type="text"/>	leave blank to let system assign default
<input type="button" value="+"/> Packet Size Adjustment		

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 or assigned classes to policy-maps, the list will contain only the preconfigured unknown-applications class and the default class-map. Once you have assigned these two classes, the list will be empty until you have configured other class-maps. See the section “Configuring a Class Map” for more information on defining class-maps.

Step 8 If you are applying a network service objective to the class, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the preconfigured network service objectives and the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.



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

Step 9 Select queue type **Bandwidth**.



Note You cannot change the queue type (Bandwidth or Priority) by editing a defined policy-map. To change the queue type for a class you must delete the policy-map and redefine it.

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 – 20,000,000 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. If you leave the field blank, the system uses the default of 64 packets.

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.



Note You cannot change the queuing configuration (Cisco Modular QoS CLI or Strict Priority Queuing) by editing a defined policy-map. To change the queuing configuration you must delete the policy-map and redefine it.

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 network service objective to the policy-map, that is, at the interface level, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the preconfigured network service objectives and the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.
- 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 network service objective to the class, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the preconfigured network service objectives and the default network service objective. See the section “Defining a Network Service Objective” for more information on defining network service objectives.



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.



Note You cannot change the queue type (Bandwidth or Priority) by editing a defined policy-map. To change the queue type for a class you must delete the policy-map and redefine it.

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 – 20,000,000 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 2,000,000 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 - corresponds to a byte adjustment value of -36.
no-udp-checksum - corresponds to a byte adjustment value of -38. This is the default.

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.



Note You cannot change the queuing configuration (Cisco Modular QoS CLI or Strict Priority Queuing) by editing a defined policy-map. To change the queuing configuration you must delete the policy-map and redefine it.

Configuring 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.

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

Figure 2-18 Custom Applications

Applications

	Precedence	Name ▲	Type	Description	Actions
+	255	AARP	Protocols		edit duplicate delete
1		Abacast	Auto-Discovered	[Entertainment/Streaming Media/Video/Abacast] Proprietary media streaming protocol using P2P technology (control session)	
1		Abacast transfer	Auto-Discovered	[Entertainment/Streaming Media/Video/Abacast] Proprietary media streaming protocol using P2P technology (transfer session)	
1		Agresso	Auto-Discovered	[Business Systems/Enterprise] Integrated Business information management	

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 2-5 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. Range: 1 – 255.
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 2-19 Defining a Custom Application

Add Custom Application

Add Custom Application

Name:

Description:

Precedence:

Match All:

☐

Define Rule for Application...

Application Rules

Save

Cancel

To define a custom application, you do the following:

Step 1 Click **Add Custom Applications**.

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 2-20: Defining a Custom Application Match Rule

Add Application Rule

Application: MyTransact

Source Address ☒

Destination Address ☒

Protocol Both TCP and UDP

Ports

Match Source Port: ☒

Match Destination Port: ☒

Match Either Direction: ☒

Advanced Settings

TOS Any

Protocol Any

Applications Any

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, select and fill out the source and destination address, protocol, and port 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.



Note If more than one type of advanced match rule is configured, then two match rules will be created for the custom application. For example, let's say TOS and application fields are both specified. In this case one IP match rule (for the TOS values) and one Application type match rule are created.

- 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.

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 2-6 Network Model Components

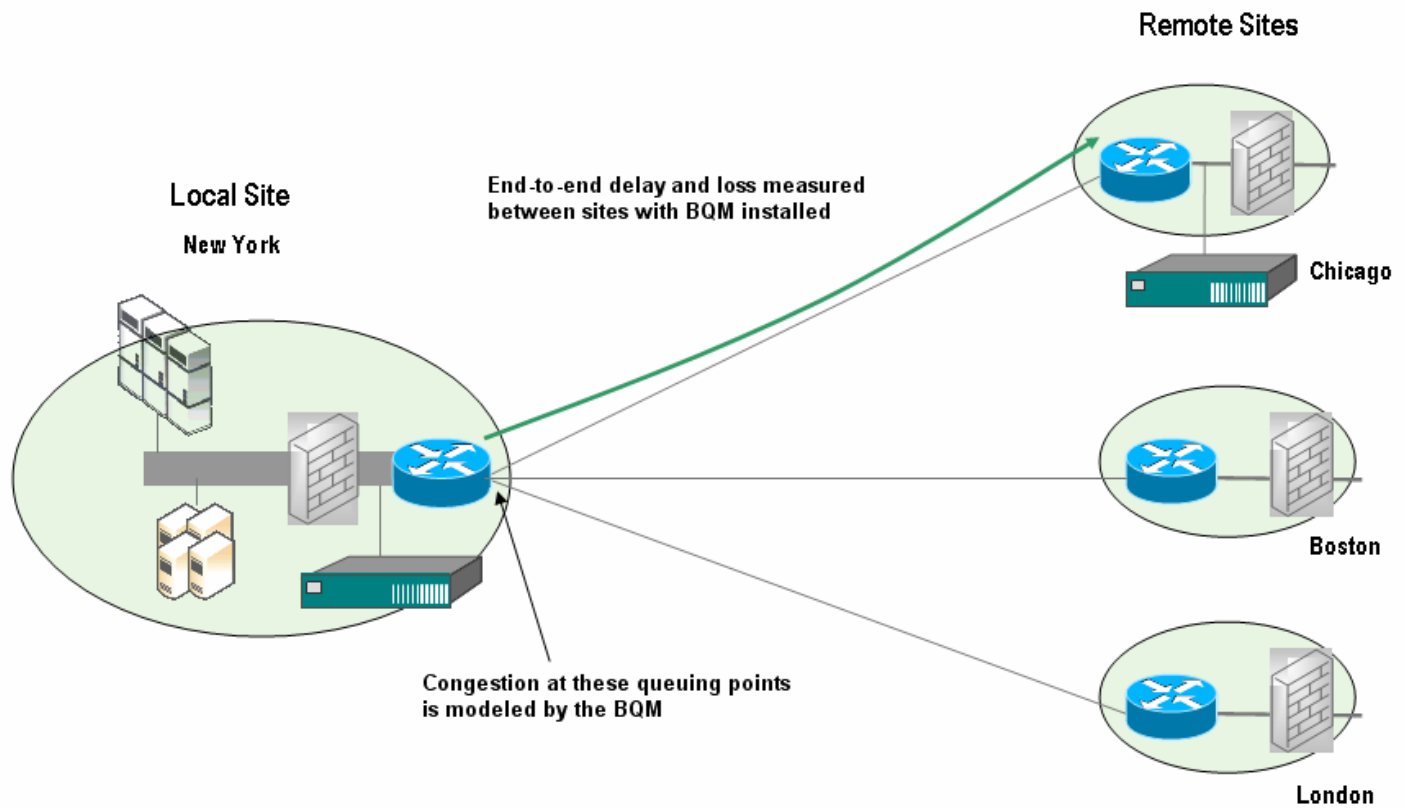
Component	Description
Local Site	A representation of a physical site where the Cisco ADE is installed in the network of interest. A local site is usually defined in the network model by specifying network subnets.
Remote Site	A representation of a physical site that is connected to, but remote from, the local site in the network of interest. A remote site is usually defined 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	<p>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.</p> <p>An end-to-end PNQM measurement channel can be configured between the local site and a particular remote site interface.</p>
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 Cisco ADE is installed in the network of interest. A local site is usually defined in the network model 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 usually defined by specifying network subnets.

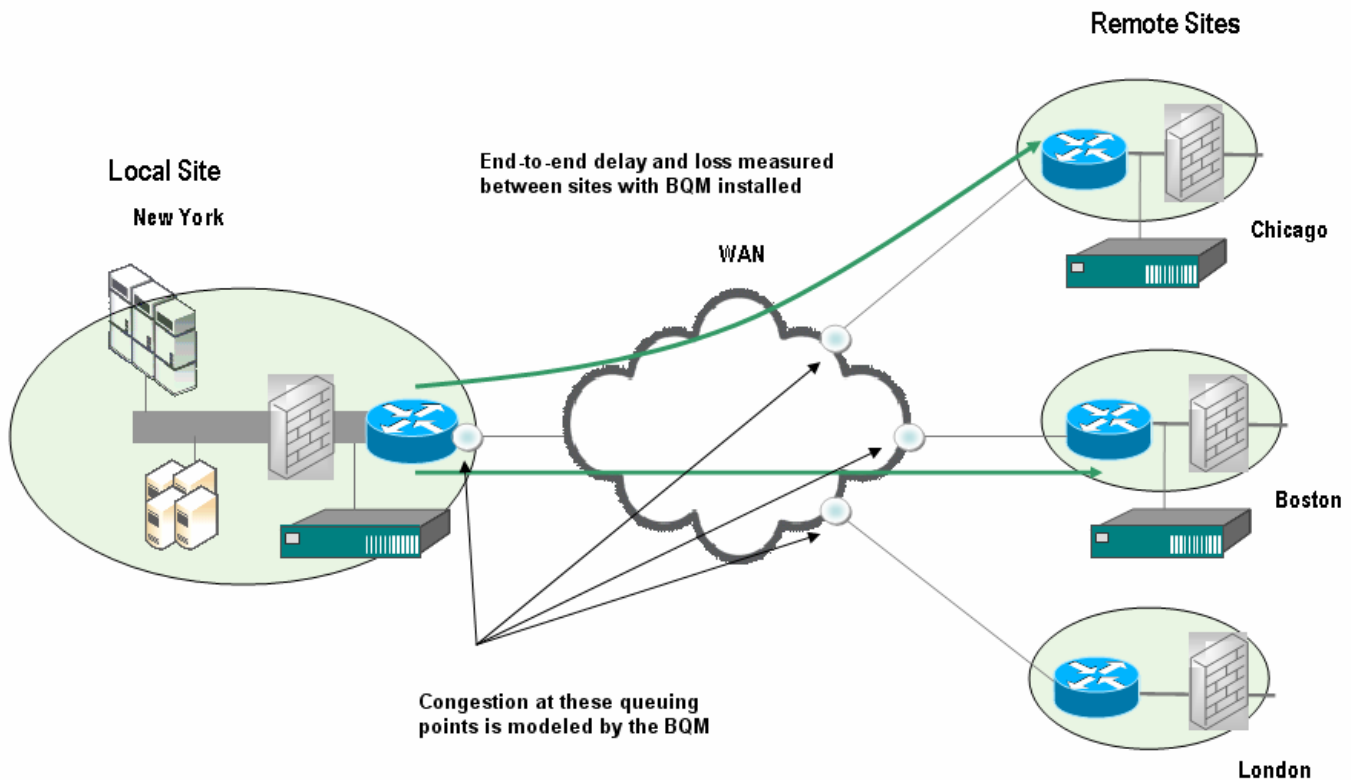
Each site comprises at least one router and its associated interfaces, configured to match the details of the network devices being modeled.

Figure 2-21 *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 2-22 *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 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.

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

Sites / Interfaces					
Local Site Name	Router(s)	Interface(s)	Policy Map(s)	Subnet(s)	Actions
Local-site	2	5	default	0	edit

Remote Sites					
Remote Site Name ▲	Router(s)	Interface(s)	Policy Map(s)	Subnet(s)	Actions
Unmatched Traffic	default	default	default	Unmatched Remote	edit duplicate delete

1 remote site(s)

Table 2-7 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)	<p>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.</p> <p>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).”</p>
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.
Actions	<p>edit – click to display the site details for editing.</p> <p>delete – click to delete a site (Remote sites only.)</p> <p>duplicate – click to copy site details to a new site (Remote sites only.)</p>

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

Local Site Properties

Site Name: Local-site

Site Description: site in which BQM is deployed

Local IP Address / Subnet: Add additional subnet (example: 192.168.1.0/24) ?

Add Router

Routers

Router Name	Port	Interface(s)	Policy Map(s)	Actions
bgm	A B	4	1	edit duplicate delete
default	A B	1	1	edit duplicate delete

Save Cancel

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 new name for the local site, if required.
- Step 4** Enter a brief description of the site in the **Site Description** field.
- Step 5** 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 6 To configure a router for the local site, click **Add Router**. Alternatively, to save the site without configuring a router, click **Save**.

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 2-8 *Edit Local Site - Routers Page*

Column	Description
Router Name	Displays the name of the configured router(s).
Port	Displays the physical Cisco ADE 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.

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 Router** page.

Figure 2-25 Defining a Local Site Router

Edit Router

Site: Local-site

Local Router Properties

* Router Name:

Router Description:

Ports Monitoring this Router: ☒ Port A ☒ Port B

[Add Interface](#)

Interfaces

Interface Name	Port	WAN Connectivity	Bandwidth	Policy Map	Actions
Save Cancel					

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

- Step 1** From the **Edit Sites/Interfaces** screen, click **Add 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 Cisco ADE physical ports from the **Ports monitoring this router** field that are being used to measure traffic for this router. Depending on the hardware platform you are using, there will be one (Cisco ADE 1010 or single-port 2120), two (certain Cisco ADE 2120, 2140 models), or four ports (certain Cisco ADE 2120, 2130 models) available here.
- Step 5** To configure an interface for the router, click **Add Interface**. Alternatively, to save the router without configuring an interface, click **Save**.

The **Edit Router** 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 2-9 **Local Site – Edit Router Page**

Column	Description
Interface Name	Displays the name of the interface.
Port	Displays the physical Cisco ADE ports that are configured to measure traffic from the interface being represented in the model.
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.
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.

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 **Add Router** page.

Figure 2-26 Defining a Local Router Interface

Add Interface

Site:	Local-site
Router:	local-rtr

WAN Interface Properties

* Interface Name: Enter a name for the site router interface

Interface Description:

* Bandwidth: Kbps

Policy Map:

Advanced Options


WAN Connectivity ☒ MPLS VPN, Internet VPN, Private VPN, etc. ☐ ATM PVC, FR PVC Metro Ethernet, Leased Line, etc.

☐ **Local Site WAN Interface**

Bandwidth:
Kbps

Policy Map:
default

Advanced Options



Local Site Service Provider

☐ **Service Provider WAN Interface** [EDIT](#)

Bandwidth:
Kbps

Policy Map:
default

Advanced Options

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

- Step 1** Click **Add Interface**.
- Step 2** Enter a name in the **Interface Name** field.
- Step 3** Enter a brief description in the **Description** field.
- Step 4** Enter a link bandwidth for the interface in kbps, Mbps, or Gbps in the **Bandwidth** field.
- Step 5** 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 6 Select the **Connectivity** type relevant to the deployment.



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

Step 7 If you have selected a WAN Connectivity type of **MPLS VPN, Internet VPN, Private VPN** click **Edit** and check that the displayed Service Provide WAN interface (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, select the policy-map from the list.

If you have selected **ATM PVC...** as the **Connectivity** type, the Local Site WAN Interface details are updated to reflect the configuration you have made. You configure the Remote Site WAN Interface properties when you configure the remote site. Note that a given local interface can only be connected to one remote interface.

Step 8 Click **Save**.

The **Edit Router** page is displayed.

Step 9 Click **Save**.

The **Edit Local Site** 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 and subnet address.
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.

If you require end-to-end PNQM measurements, then configuring a remote site also involves defining a channel between the local and remote sites.

Figure 2-27 Remote Site Configuration

Add Remote Site

Remote Site Properties

* Site Name: Enter a unique name for the site.

Site Description:

Local IP Address / Subnet: [Add additional subnet](#) (example: 192.168.1.0/24) [?](#)

Routers

[Add Router](#) [Save](#) [Cancel](#)

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 **Add 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 the **Local IP Address/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 5 To configure a router for the site, click **Add Router**. Alternatively, to save the site without configuring a router, click **Save**.

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 2-10 Remote Site - Router Information

Column	Description
Router Name	Displays the name of the configured router(s).
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

Add Router

Site: sanfran

Remote Router Properties

* Router Name: Enter a unique name for the site router.

Router Description: 

Interfaces

[Add Interface](#)

[Save](#) [Cancel](#)

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

-
- Step 1** From the **Add Site** screen, click **Add 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 **Add Interface**. Alternatively, to save the router without configuring an interface, click **Save**.
-

The **Add Router** 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 2-11 Remote Site – Add Router Page

Column	Description
Name	Displays the name of the interface.
Port	Displays the physical port(s) on the appliance measuring traffic for this 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.
ICMP ping IP	Displays the ICMP responder IP address configured for the interface to facilitate end-to-end ICMP ping measurement.
BQM IP	Displays the IP address configured for the interface to facilitate PNQM measurement. Click Test to check the viability of the PNQM channel to the specified IP address. The outcome of the test is displayed in a pop-up window. For more information on testing the PNQM channel, see the section “Defining a Passive Network Quality Monitoring (PNQM) Channel” in the chapter “Using the Command Line Interface (CLI)”
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.

Configuring a Remote Site Router Interface – No PNQM Channel

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.

Figure 2-29 Remote Site Interface Configuration

Add Interface

Site: sanfran

Router: rtr

WAN Interface Properties

* Interface Name:

Enter a name for the site router interface

Interface Description:

* Bandwidth

Kbps

Policy Map:

default

+ Advanced Options

WAN Connectivity

☒ MPLS VPN, Internet VPN, Private VPN, etc.

☐ ATM PVC, FR PVC Metro Ethernet, Leased Line, etc. ?

☐ Service Provider WAN Interface

EDIT

Bandwidth:

Kbps

Policy Map:

default

+ Advanced Options

☐ Remote Site WAN Interface

Bandwidth:

Kbps

Policy Map:

default

+ Advanced Options

Cisco Bandwidth Quality Manager User Guide

2-48

OL-14118-01

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

Step 1 Click **Add Interface**.

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

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

Step 4 Enter a link bandwidth for the interface in kbps, Mbps or Gbps in the **Bandwidth** field.

Step 5 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 6 Select the **Connectivity** type relevant to the deployment.

Step 7 If you have selected **ATM PVC...** as the **Connectivity** type, first select the local router. 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 the 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, click **Edit** and check the bandwidth value and select a policy-map for the Service Provider WAN Interface (peer-interface) to which this remote site interface connects.



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

- Step 8** If you want to enable end-to-end ICMP measurements, enter an IP address of an available device at the remote site that is pinged for end-to-end roundtrip measurements. Click **Test** to send a few packets to confirm the availability and accessibility of the specified IP address. The outcome of the test is displayed in a pop-up window.
- Step 9** Click **Save**.
- The **Router** page is displayed.
- Step 10** Click **Save**.
- The **Edit Remote Site** page is displayed.
- Step 11** Click **Save**.

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

Configuring a PNQM Channel

BQM offers two modes of PNQM channel configuration: automatic and manual.

Choose automatic configuration initially to see if issues are being caused by congestion in the downstream direction (that is from the local site to the remote site) without having to perform any BQM configuration on the physical appliance at the remote site. If instead you want to access complete results for both directions of traffic and therefore require EQ results for traffic coming from the remote site, choose manual configuration. In this case, you will need to perform BQM configuration on the appliance installed at the remote site.

Figure 2-30: End-to-End ICMP and PNQM Configuration

End-to-end Settings

End-to-end Settings

ICMP Ping Address

Passive Network Quality Management Settings

Remote BQM address:

PNQM Mode

☐ manual (requires configuration of Remote BQM) ☒ automatic (no retrieval of Remote EQ)

Sample:

☐ Use class sample rate from NSO map (single class only)

☐ All packets

☒ One in packets

☐ ignoring rerouted/missing flows

Each direction of a PNQM channel may have a different policy-map (for example, FIFO in one direction, multi-class in the reverse). Such configurations are legal and PNQM may be configured.

Automatic PNQM Configuration

To specify automatic configuration of a PNQM channel, you do the following:

-
- Step 1** To enable end-to-end PNQM measurements, enter the IP address of the BQM appliance at the remote site.



Note When you have saved the PNQM configuration, you can test the configured PNQM channel. On the **Add/Edit Router** page, click **Test** to check the viability of the PNQM channel to the specified IP address. The outcome of the test is displayed in a pop-up window.

- Step 2** Select the PNQM configuration mode: automatic.



Note The system disallows automatic configurations when no subnets have been configured for the site. The system also issues a warning message when the site configuration uses filter classes or attached ports, as these will be ignored if an automatic configuration is attempted.

- Step 3** Choose a sample rate for PNQM measurement. If you are configuring for a multi-class network, you must set the sampling rate to **All packets** or **One in**.

- Step 4** Click **Save**.
-

Manual PNQM Configuration

To specify manual configuration of the remote BQM when defining a PNQM channel, you do the following:

-
- Step 1** To enable end-to-end PNQM measurements, enter the IP address of the BQM appliance at the remote site.

- Step 2** Select the PNQM configuration mode: manual.

- Step 3** Choose a sample rate for PNQM measurement. If you are configuring for a multi-class network, you must set the sampling rate to **All packets** or **One in**. Setting a sampling rate to override the network service objective enables traffic misclassification detection. Enabling traffic misclassification detection can help troubleshoot any potential issues with ensuring that the remote configuration matches that of the local.

- Step 4** You can also flag traffic that has been classified by the system as re-routed or missing. If there is no possibility of re-routing in the network deployment and you do not need an indication of re-routed packets, you can choose **strict**.



Note Rerouting/misclassification detection - routing and classification policies typically treat all packets in a flow in the same way, they all take the same route and end up in the same class. We take advantage of this by assuming that continuous loss for a flow indicates that the flow is not being seen at both ends of the PNQM channel and can be discounted from the PNQM results.

You can specify here that you do not expect any re-routing to occur, so that re-routing is disabled.

Step 5 Click **Save**.



Note For more information on testing the PNQM channel, see the section “Defining a Passive Network Quality Monitoring (PNQM) Channel” in the chapter “Using the Command Line Interface (CLI).”

See the section “Manual PNQM Configuration” in the chapter “Using the Command Line Interface (CLI)” for additional guidelines on performing manual configuration and achieving a matching configuration between the local and remote BQM appliances.

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 latency 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 latency and jitter.

The configured LFI value represents the maximum tolerable latency 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 latency on a per-hop basis is 10 ms and should not exceed 20 ms.

Layer 2 or Tunneling Overhead

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 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 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, Event 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 re-included, 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.

Configuring a Custom Dashboard

You can configure a custom dashboard to monitor the network service level being achieved by a defined set of classes. The newly defined custom dashboard is displayed as a new tab in **Bandwidth Quality Manager** mode. One custom dashboard can be configured at any one time.

You define a custom dashboard in the GUI from the **Custom Dashboard** page in the **Configuration** tab.

Figure 2-31 Custom Dashboard Configuration Page

Custom Dashboard

^{*} Name:

^{*} Show Tab: ☐ (check to display the custom dashboard tab in the monitoring tabs)

Available Classes:

- class-default
- unknown-applications
- ssh
- http

Selected Classes:

Available Graphs:

- Microburst-detection
- Average Rate
- Packet Rate
- Peak-to-mean
- Packet Size distribution (by bytes)
- Packet Size distribution (by packets)
- Top 10 Applications
- Top 10 Talkers
- Top 10 Listeners
- Top 10 Conversations

Selected Graphs:

Save Cancel

To define a custom dashboard, you do the following:

Step 1 Enter a unique name for the custom application in the **Name** field.



Note The name you specify here will be displayed as the name of the new tab in **Bandwidth Quality Manager** mode. In this case there will be seven tabs displayed in the GUI, so we recommend that you use a concise name for the tab. The maximum allowable length is 15 characters.

Step 2 Check the **Show Tab** check box to enable display of the new tab. Clearing the check box suppresses display of the custom dashboard tab in **Bandwidth Quality Manager** mode.

Step 3 Specify the classes to be monitored using the custom dashboard by clicking each chosen class from the **Available Classes** list box and clicking >>.

Step 4 Specify the graph and chart results to be displayed for each selected class by clicking each chosen graph or chart from the **Available Graphs** list box and clicking >>.

Step 5 Click **Save**.

The new custom dashboard is displayed as a new tab in **Bandwidth Quality Manager** mode to the right of the **Network Service Quality** tab. When the next data summarization period elapses (as per the selected reporting period), results are available for each monitored class.



3 Configuring Network Deployments

Overview

This chapter describes how to take knowledge of the existing network design, which BQM is used to monitor and troubleshoot, and configure the appropriate deployment of the product network model using the GUI. 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

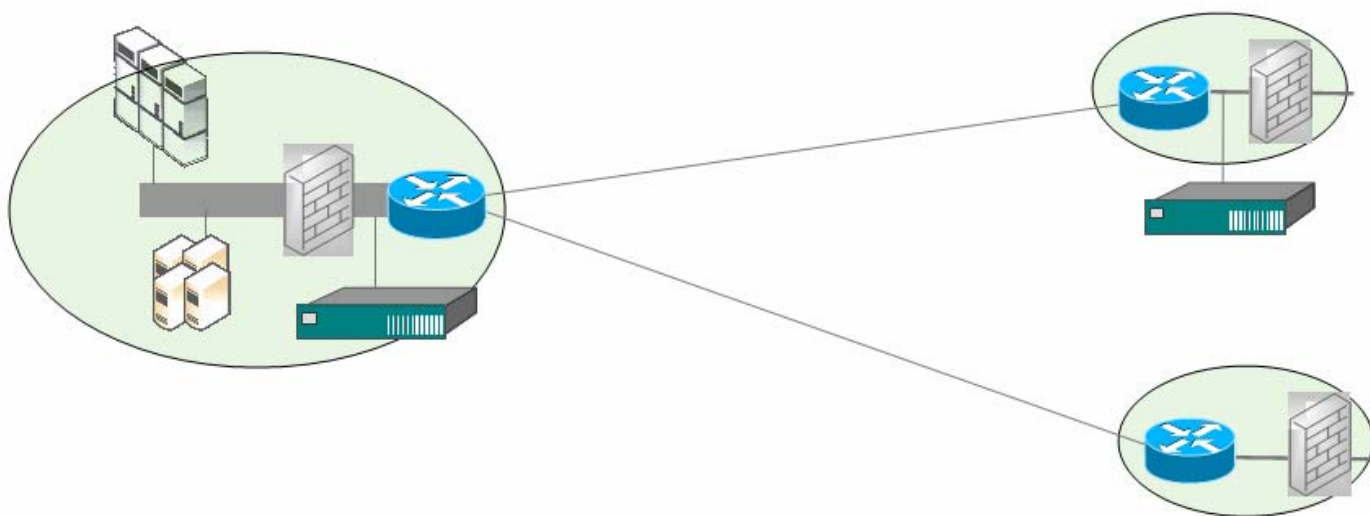


Note For additional information on supported network deployments, see the section “Configuring Network Model Deployments with the CLI” in the chapter ‘Using the Command Line Interface (CLI).’

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

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' represents the Cisco ADE physical installation site.

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:

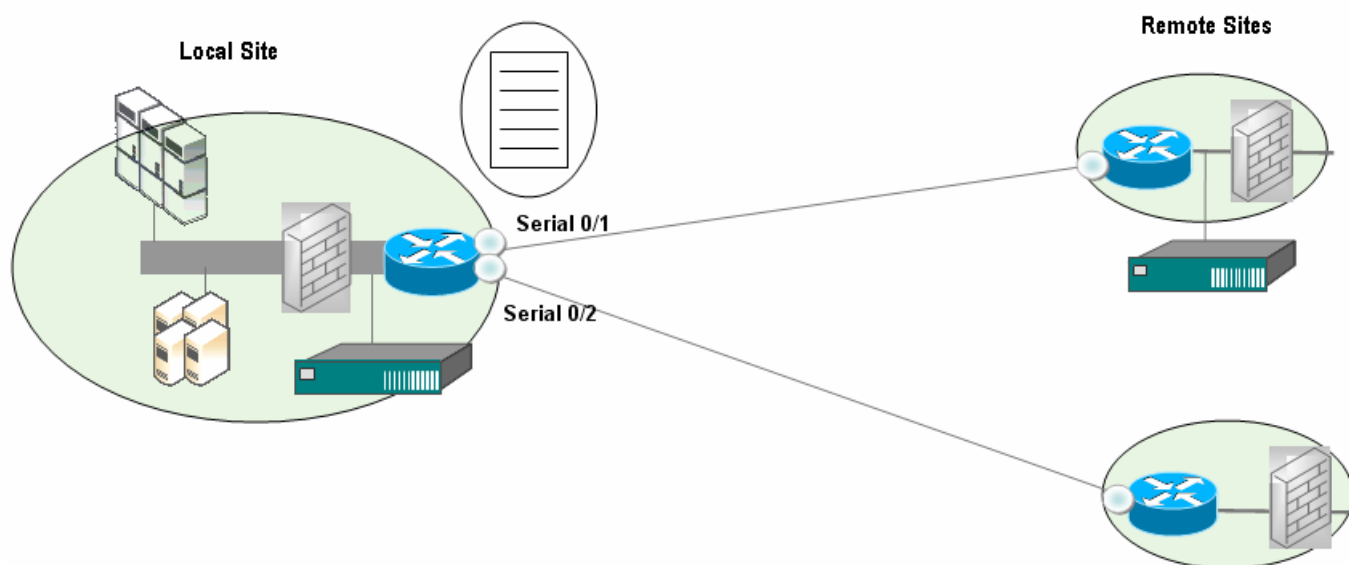
- Local site
 - Default site in model that contains a Cisco ADE; the name is editable
 - Subnet
 - Router
 - Interfaces specifying bandwidth configuration and policy-maps
- Remote Site with Cisco ADE installed for PNQM measurement
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map, address of Cisco ADE for PNQM measurement
- Remote Site (no Cisco ADE installed, no PNQM measurement)
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map

In this example single-class configuration, we do not explicitly configure class-maps, policy-maps, or network service objectives. The system then uses the default class-map, policy-map and network service objective. Also we do not configure a BQM IP address for remote site interfaces for which PNQM measurement is not required.

When you define interfaces without explicitly defining a policy-map or network service objective, the default policy-map and therefore the default network service objective are automatically assigned to the interface. You can also define a policy-map and an associated (non-default) network service objective, and apply them to a configured interface.

The first 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 default policy-map:

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



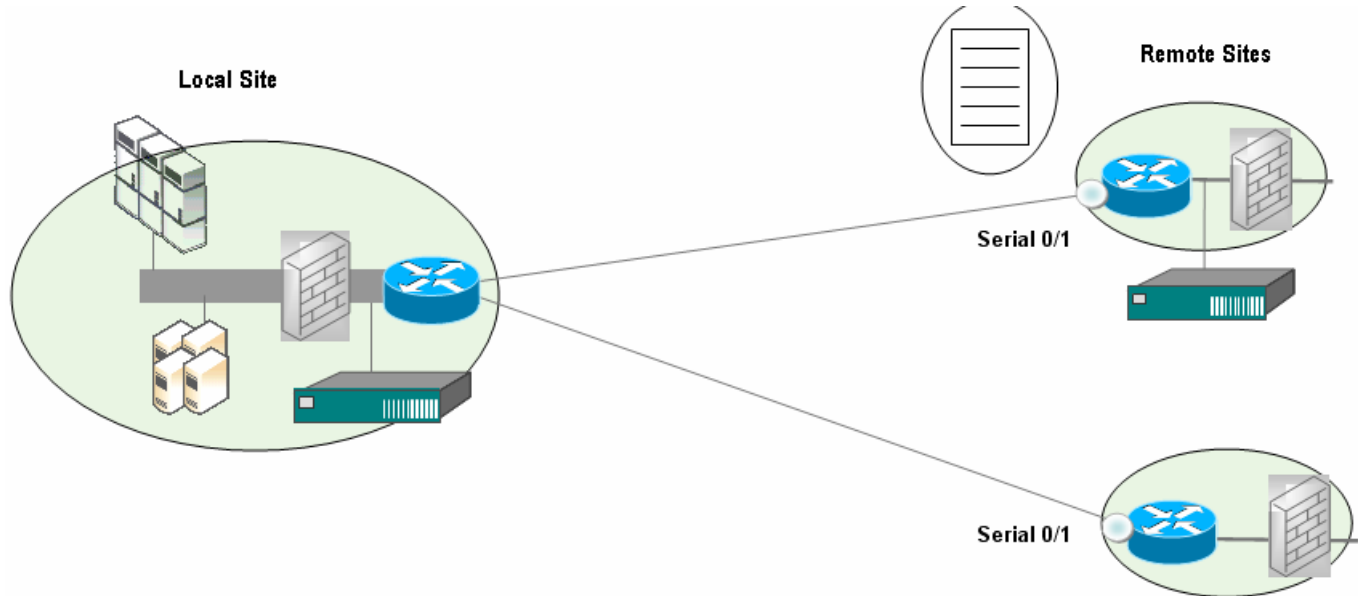
-
- Step 1** Click the named local site link or the **edit** link.
 - Step 2** The **Edit Local Site** page is displayed.
 - Step 3** Enter a brief description of the site in the **Site Description** field.
 - Step 4** Enter the site subnet address and prefix in the **Subnet** field.
 - Step 6** To configure a router for the local site, click **Add 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 Cisco ADE physical ports from the **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 **Add Interface**.
- 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 default policy-map for the interface from the **Policy Map** list.
- Step 15** Select **ATM PVC...** as the **WAN Connectivity** type.
- Step 16** Click **Save**.
- The **Edit 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 Local Sites** 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** Click **Add Router**.
- The **Add Router** page is displayed.
- Step 6** Enter a name in the **Router Name** field, in this example remote1.
- Step 7** Enter a brief description in the **Router Description** field.
- Step 8** To configure an interface for the router, click **Add Interface**.
- Step 9** Enter a name in the **Interface Name** field, in this example Serial0/1.
- Step 10** Enter a brief description in the **Interface Description** field.
- Step 11** Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.
- Step 12** Select the default 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 13** 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 14** Enter an IP address of an available device at the remote site that is pinged for end-to-end roundtrip measurements. Click **Test** to send a few packets to confirm the availability and accessibility of the specified IP address. The outcome of the test is displayed in a pop-up window.
- Step 15** Enter the IP address of the BQM appliance at the remote site to facilitate PNQM measurement.
- Step 16** Set the PNQM measurement mode to **automatic**.



Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” in the chapter “Using the Command Line Interface (CLI) for guidelines on how to define a BQM configuration to enable PNQM measurement on a remote Cisco ADE to match a given configuration on the local Cisco ADE.

In this single class example, the sample rate is left at the default setting.



Note If you are configuring for a multiclass network, you must choose a different sample rate, using either the **All packets** or **One in** options.

- Step 17** Click **Save**.
- The **Edit Router** page is displayed.
- Step 18** Click **Test** to check the viability of the PNQM channel with the specified IP address. The outcome of the test is displayed in a pop-up window.



Note For more information on testing the PNQM channel, see the section “Defining a Passive Network Quality Monitoring (PNQM) Channel” in the chapter “Using the Command Line Interface (CLI).”

Step 19 Click **Save**

The **Edit Remote Sites** page is displayed.

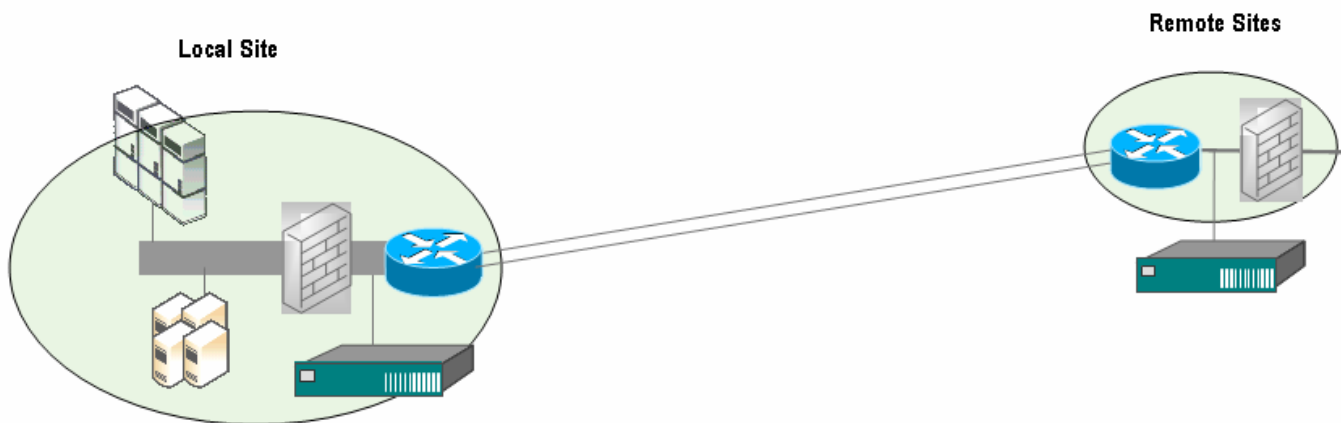
Step 20 Click **Save**.

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

Step 21 Repeat this task from Step 1 to Step 14 and then Step 17 to Step 20 to add the remote site for which no BQM appliance is installed or PNQM measurement is not required. 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.

If there are two interface connections between the local site and a remote site, you must use the CLI to model the separate remote site interfaces using filter classes and disable subnet filtering with the **no subnet-filtering** command.

Figure 3-4 Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Two Directly Connected Interfaces

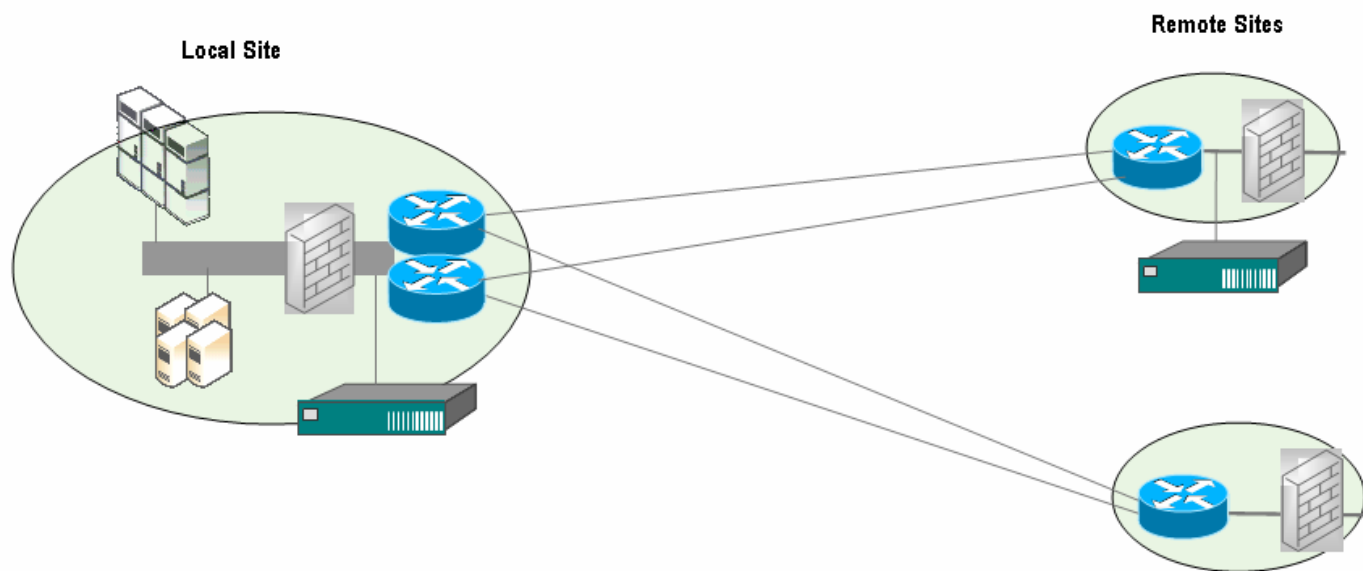


For more information on subnet filtering and filter classes, see the sections “Working with Subnet Filtering”, “Using Filter Classes”, and the section “Basic ATM PVC, Frame Relay PVC, Metro Ethernet, and Leased Line Deployment” in the chapter “Using the Command Line Interface (CLI).”

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

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

Figure 3-5 *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 Cisco ADE; the name is editable
 - Subnet
 - Router
 - Two interfaces specifying bandwidth configuration and policy-maps
 - Mapping of Cisco ADE physical measurement ports to routers
- Remote Site with Cisco ADE installed for PNQM measurement
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map, address of Cisco ADE for PNQM measurement

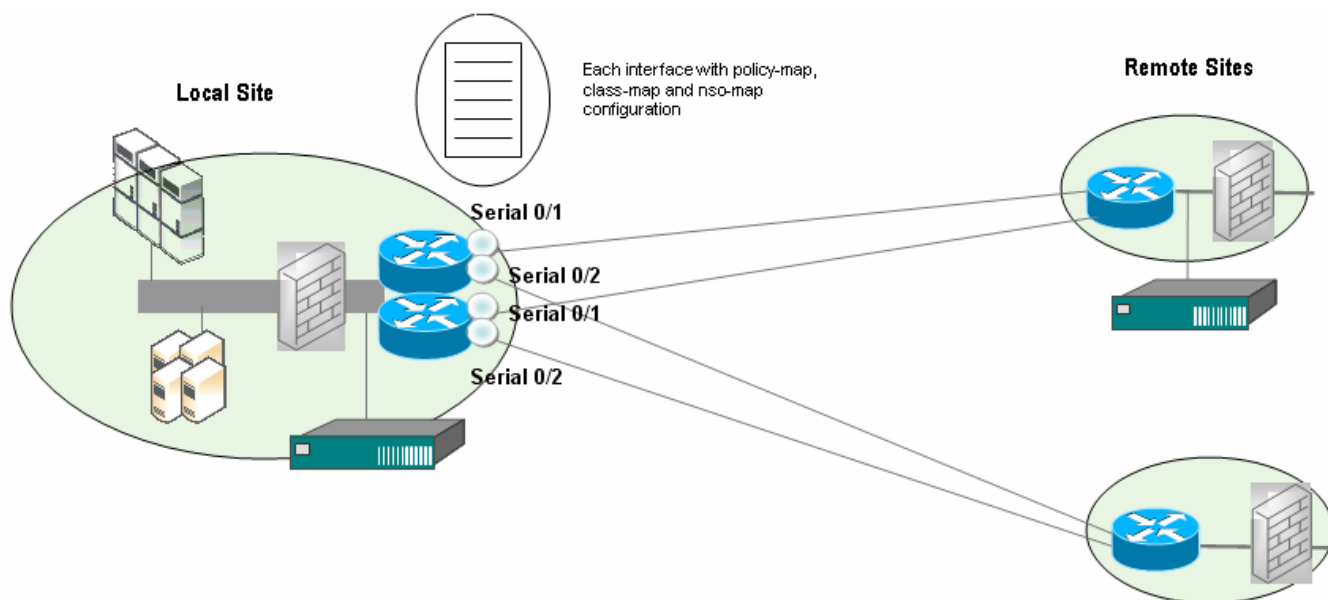
- Remote Site (no Cisco ADE installed, no PNQM measurement)
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map

In this example single-class configuration, we do not explicitly configure class-maps, policy-maps, or network service objectives. The system then uses the default class-map, policy-map and network service objective. Also we do not configure a BQM IP address for remote site interfaces for which PNQM measurement is not required.

When you define interfaces without explicitly defining a policy-map or network service objective, the default policy-map and therefore the default network service objective are automatically assigned to the interface. You can also define a policy-map and an associated (non-default) network service objective, and apply them to a configured interface.

The first 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 3-6 *Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Local Site Configuration*



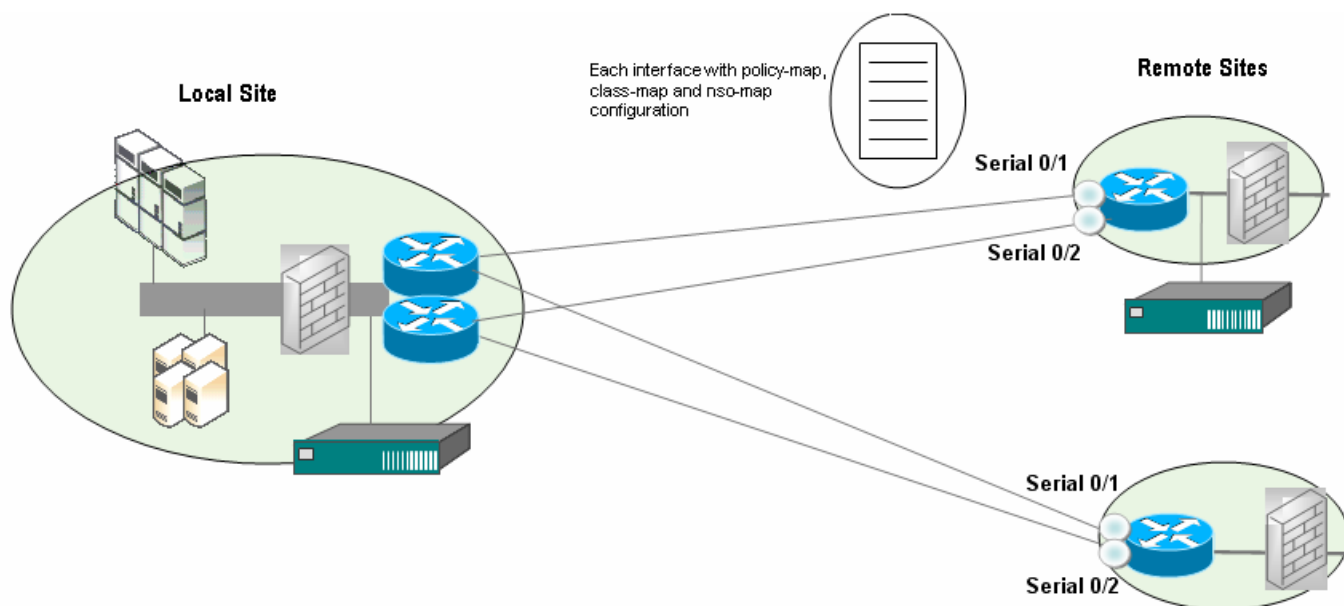
-
- Step 1** Click the named local site link or the **edit** link.
- Step 2** The **Edit Local Site** page is displayed.
- Step 3** Enter a brief description of the site in the **Site Description** field.

- 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 Cisco ADE physical ports from the **Ports Monitoring this Router** field that are being used to measure traffic for this router. In this example, there are two physical ports available for monitoring this router (PortA and PortB).
- Step 9** To configure an interface for the router, click Add Interface.
- Step 10** Enter a name in the **Interface Name** field, in this example Serial0/1.
- Step 11** Enter a brief description in the **Interface Description** field.
- Step 12** Enter the link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.
- Step 13** Select the default policy-map for the interface from the **Policy Map** list.
- Step 14** Select **ATM PVC...** as the **WAN Connectivity** type.
- Step 15** Click **Save**.
- The **Edit 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 Local Site** 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 3-7 *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** Click **Add Router**.
- The **Add Router** page is displayed.
- Step 6** Enter a name in the **Router Name** field, in this example remote1.
- Step 7** Enter a brief description in the **Router Description** field.
- Step 8** To configure an interface for the router, click **Add Interface**.
- Step 9** Enter a name in the **Interface Name** field, in this example Serial0/1.
- Step 10** Enter a brief description in the **Interface Description** field.
- Step 11** Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.
- Step 12** Select the default 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 13** 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 14** Enter an IP address of an available device at the remote site that is pinged for end-to-end roundtrip measurements. Click **Test** to send a few packets to confirm the availability and accessibility of the specified IP address. The outcome of the test is displayed in a pop-up window.
- Step 15** Enter the IP address of the BQM appliance at the remote site to facilitate PNQM measurement.
- Step 16** Set the PNQM measurement mode to **automatic**.



Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” in the chapter “Using the Command Line Interface (CLI) for guidelines on how to define a BQM configuration to enable PNQM measurement on a remote Cisco ADE to match a given configuration on the local Cisco ADE.

In this single class example, the sample rate is left at the default setting.



Note If you are configuring for a multiclass network, you must choose a different sample rate, using either the **All packets** or **One in** options.

- Step 17** Click **Save**.
- The **Edit Router** page is displayed. Click **Test** to check the viability of the PNQM channel with the specified IP address. The outcome of the test is displayed in a pop-up window.



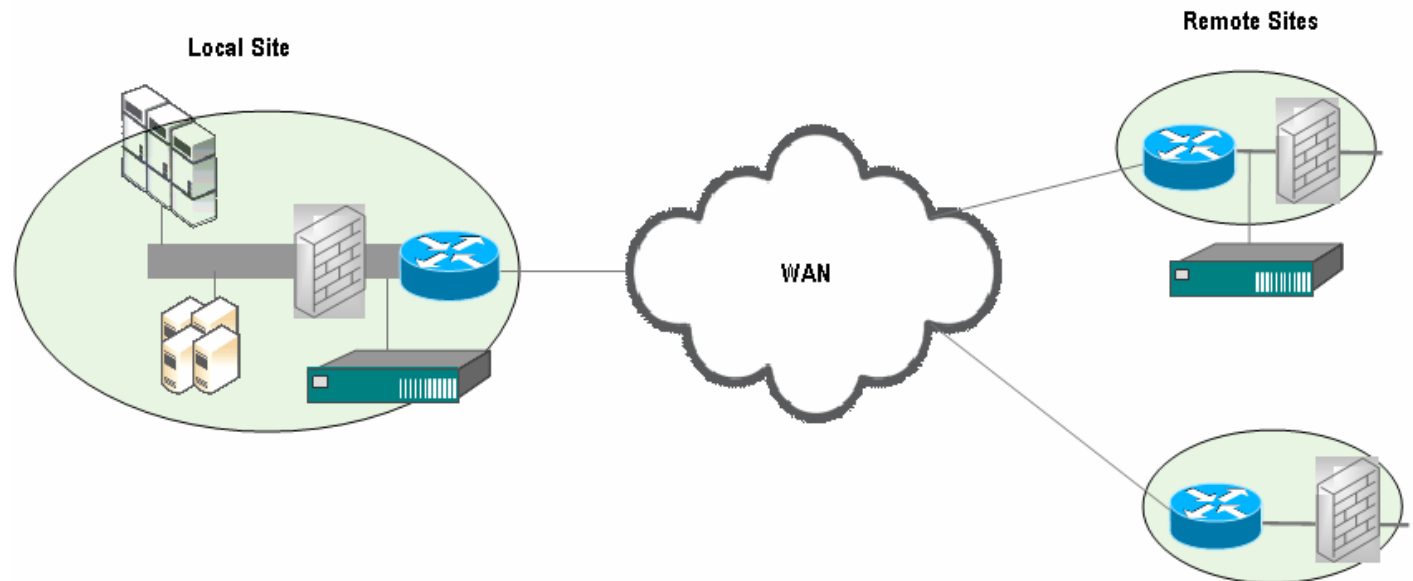
Note For more information on testing the PNQM channel, see the section “Defining a Passive Network Quality Monitoring (PNQM) Channel” in the chapter “Using the Command Line Interface (CLI).”

- Step 18** Repeat Step 10 to Step 17 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 19** Click **Save**.
- The **Edit Remote Site** page is displayed.
- Step 20** Click **Save**.
- The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.
- Step 21** Repeat this task from Step 1 to Step 15 and then Step 17 to Step 20 to add the remote site for which there is no installed BQM appliance and PNQM measurement is not required. 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.
-

Basic MPLS VPN, Internet VPN, Private VPN Deployment

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' represents the Cisco ADE physical installation site 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.

Figure 3-8 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 Cisco ADE; the name is editable
 - Subnet
 - Router
 - Two interfaces specifying bandwidth configuration and policy-maps
 - Mapping of Cisco ADE physical measurement ports to routers
- Remote Site with Cisco ADE installed for PNQM measurement
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map, address of Cisco ADE for PNQM measurement
- Remote Site (no Cisco ADE installed, no PNQM measurement)
 - 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 network service objectives for each class of traffic in the configuration:

-
- Step 1** In **System Administration** mode, click the **Configuration** tab, and then click **Network Service Objectives**.
 - Step 2** Click **Define Network Service Objective**.
 - Step 3** Enable and configure the required features and thresholds for each class.
-

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**.

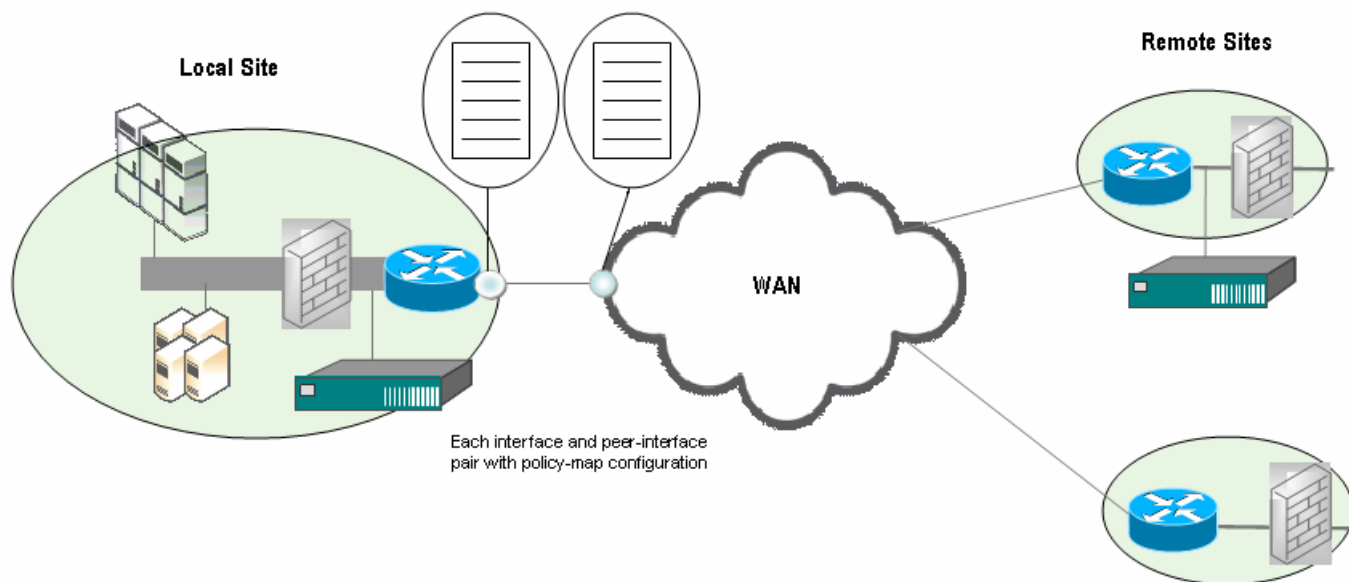
The next task is to define the policy-map for the configuration. In this example, a multi-class WFQ policy-map is configured, comprising the class-maps and the network service objective defined in the previous tasks:

- 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 network service objective to the policy-map, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the default network service objective. See the section “Configuring a Network service objective” for more information on defining network service objectives.
- 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 network service objective to the class, select a network service objective 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. If you leave the field blank, the system uses the default value of 64 packets.
- 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 3-9 Basic MPLS VPN, Internet VPN, Private VPN Deployment – Local Site Configuration

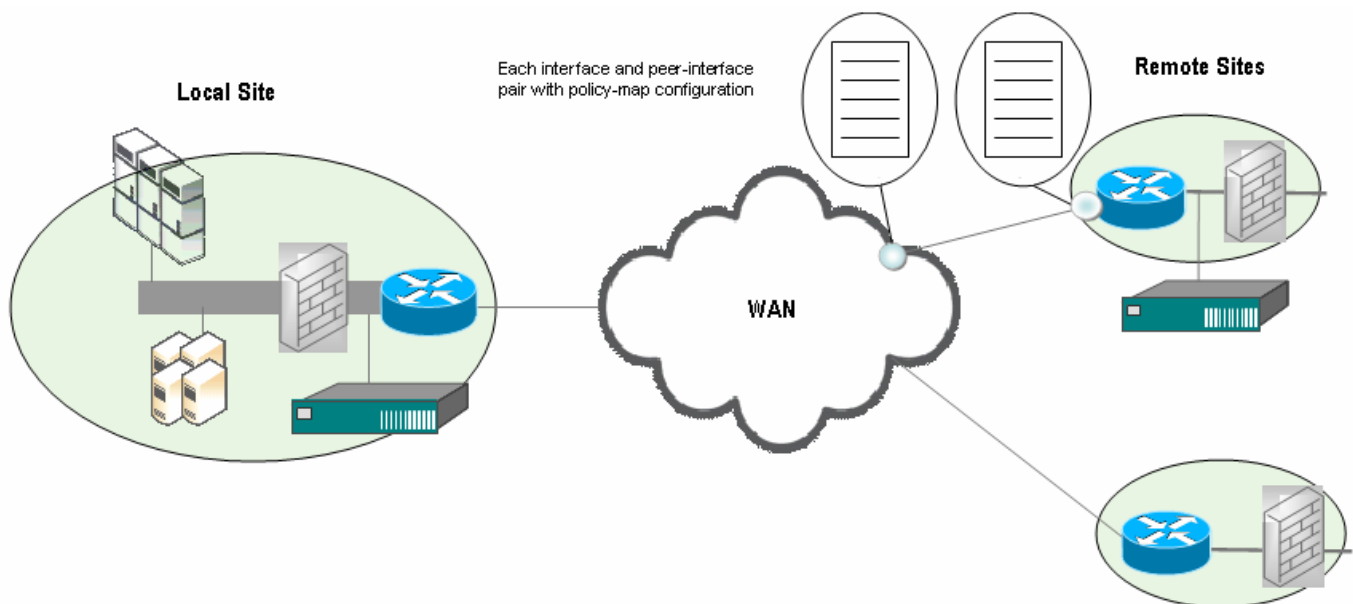


- Step 1** Click the named local site link or the **edit** link.
- Step 2** The **Edit Local Site** page is displayed.
- Step 3** Enter a brief description of the site in the **Site Description** field.
- Step 4** Enter the site subnet address and prefix in the **Subnet** field, in this example 192.168.5.0/24.
- Step 5** To configure a router for the local site, click 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 Cisco ADE physical ports from the **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 Add Interface.
- Step 10** Enter a name in the **Interface Name** field, in this example FastEthernet0.
- Step 11** Enter a brief description in the **Interface Description** field.

- Step 12** Enter the link bandwidth for the interface, in this example 100 Mbps, in the **Bandwidth** field.
- Step 13** Select the policy-map for the interface from the **Policy Map** list.
- Step 14** Select **MPLS VPN...** as the **WAN Connectivity** type.
- Step 15** Click **Edit** and check that the peer-interface details in the Service Provider panel are correct.
- Step 16** Click **Save**.
- The **Edit Router** page is displayed.
- Step 17** Click **Save**.
- The **Edit Local Site** page is displayed.
- Step 18** Click **Save**.

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

Figure 3-10 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** Click **Add Router**.
- The **Add Router** page is displayed.
- Step 6** Enter a name in the **Router Name** field, in this example remote1.
- Step 7** Enter a brief description in the **Router Description** field.
- Step 8** To configure an interface for the router, click **Add Interface**.
- Step 9** Enter a name in the **Interface Name** field, in this example Serial0/1.
- Step 10** Enter a brief description in the **Interface Description** field.
- Step 11** Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.
- Step 12** 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 13** 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 14** Check that the peer-interface details in the Service Provider panel are correct.
- Step 15** Enter an IP address of an available device at the remote site that is pinged for end-to-end roundtrip measurements. Click **Test** to send a few packets to confirm the availability and accessibility of the specified IP address. The outcome of the test is displayed in a pop-up window.
- Step 16** Enter the IP address of the BQM appliance at the remote site to facilitate PNQM measurement.



Note You need only configure PNQM for the remote site interface of interest. You do not need to configure PNQM details for the associated peer-interface.

- Step 17** Click **Save**.

The **Edit Router** page is displayed. Click **Test** to check the viability of the PNQM channel with the specified IP address. The outcome of the test is displayed in a pop-up window.



Note For more information on testing the PNQM channel, see the section “Defining a Passive Network Quality Monitoring (PNQM) Channel” in the chapter “Using the Command Line Interface (CLI).”

Step 18 Click **Save**.

The **Edit Remote Site** page is displayed.

Step 19 Click **Save**.

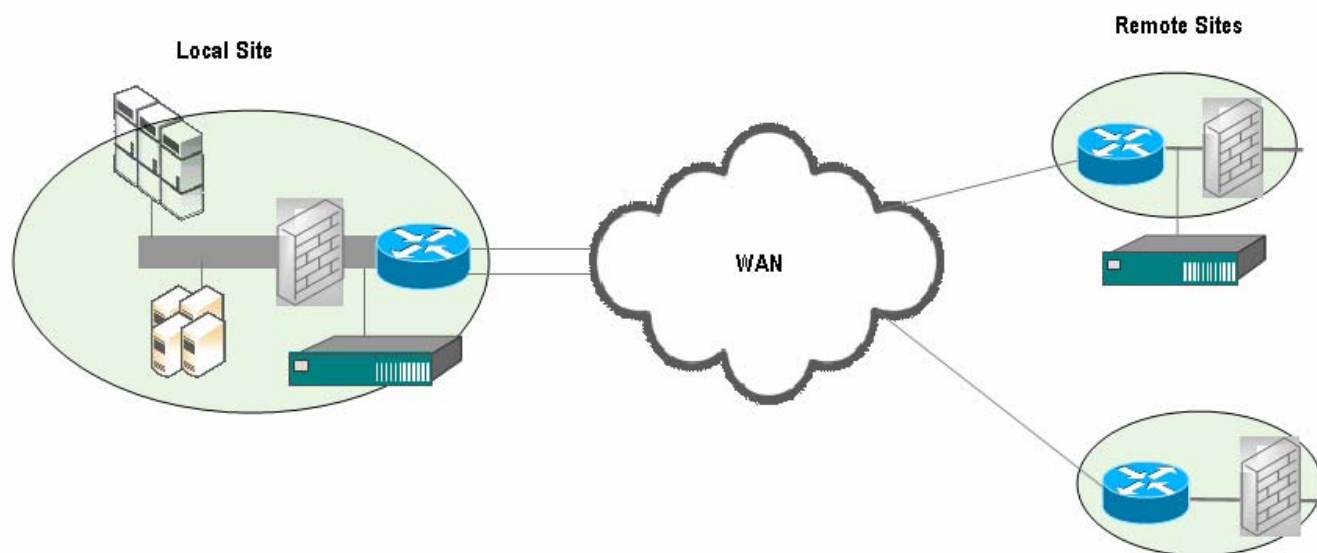
The new remote site configuration is saved and the **Sites/Interfaces** page is displayed.

Step 20 Repeat this task from Step 1 to Step 15 and Step 17 to Step 19 to add the remote site for which there is no installed BQM appliance and PNQM measurement is not required.

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.

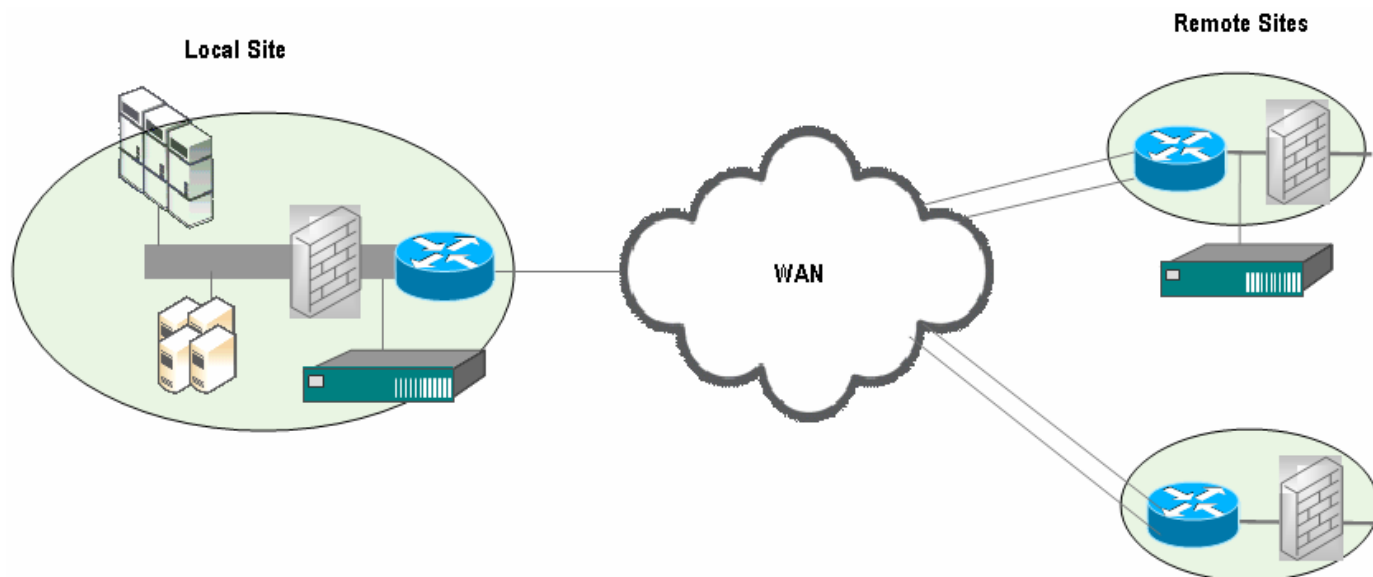
Figure 3-11 Network Model –VPN Deployment with Redundant Remote Site Connectivity



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, BQM does not present accurate traffic statistic results for the remote site interfaces in this case.

Figure 3-12 Network Model –VPN Deployment with Redundant Remote Site Connectivity



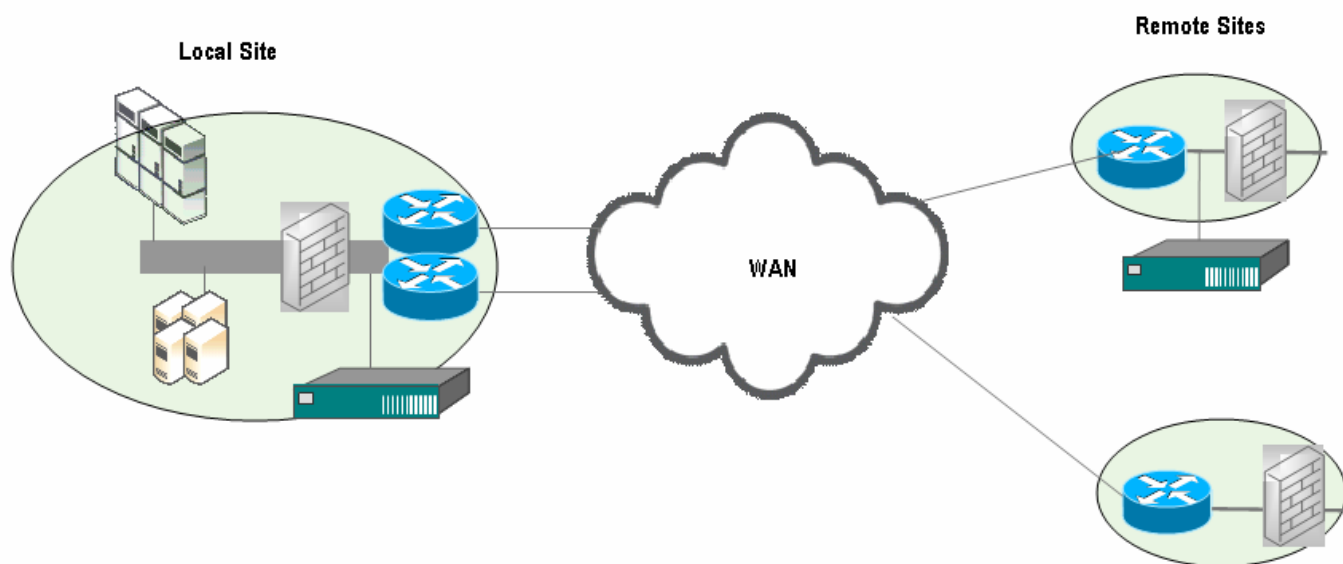
Note For more information on deployments for which certain caveats on BQM results apply, see the following sections in the chapter “Using the Command Line Interface (CLI)”:

- MPLS VPN deployment with any-to-any traffic
- MPLS VPN deployment with remote site internet traffic via local site
- MPLS VPN deployment with local site connected to remote site via two WANs
- Dual data center deployment

Dual-homed MPLS VPN Deployment

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' represents the Cisco ADE physical installation site 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 3-13 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 Cisco ADE; the name is editable
 - Subnet
 - Router
 - Two interfaces specifying bandwidth configuration and policy-maps
 - Mapping of Cisco ADE physical measurement ports to routers
- Remote Site with Cisco ADE installed for PNQM measurement
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map, address of Cisco ADE for PNQM measurement
- Remote Site (no Cisco ADE installed, no PNQM measurement)
 - 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 network service objectives for the traffic classes in the configuration:

-
- Step 1** In **System Administration** mode, click the **Configuration** tab, and then click **Network Service Objectives**.
 - Step 2** Click **Define Network Service Objective**.
 - Step 3** Enable and configure the required features and thresholds for each class.
-

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**.

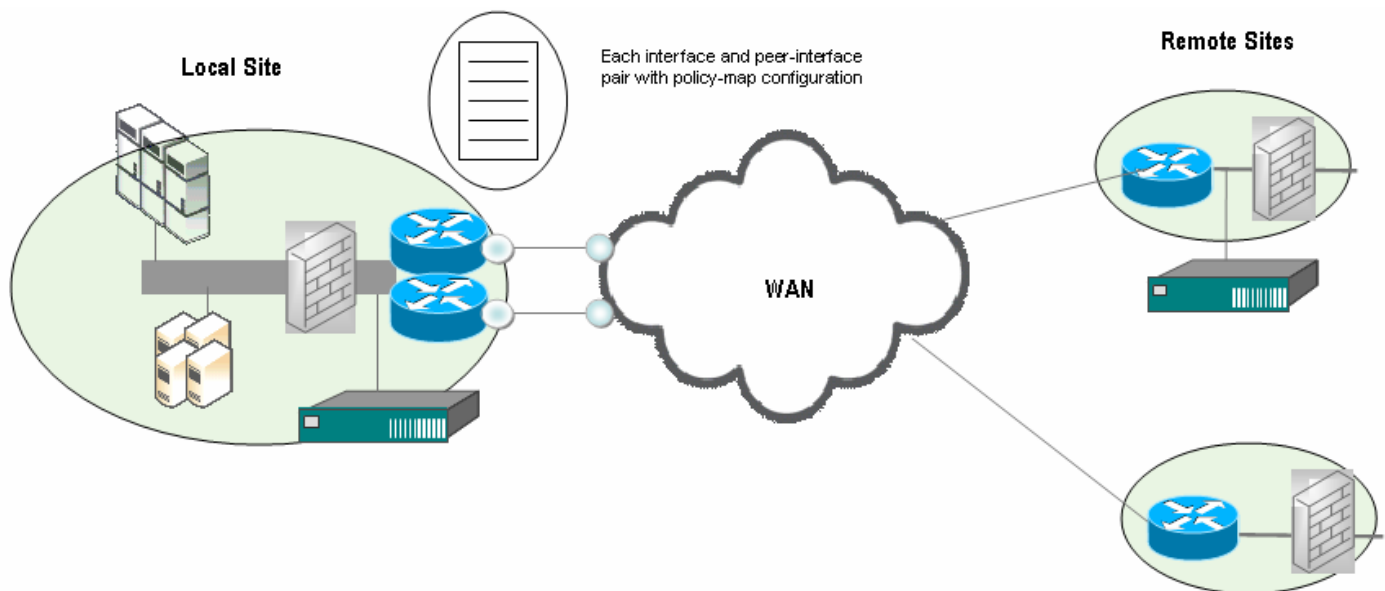
The next task is to define the policy-map for the configuration. In this example, a multi-class WFQ policy-map is configured, comprising the class-maps and the network service objective defined in the previous tasks:

- 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 network service objective to the policy-map, select a network service objective from the list. If you have not configured any network service objectives, the list will contain only the default network service objective. See the section “Configuring a Network service objective” for more information on defining network service objectives
- 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 network service objective to the class, select one 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. If you leave the field blank, the system uses the default value of 64 packets.
- 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 3-14 *Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment – Local Site Configuration*



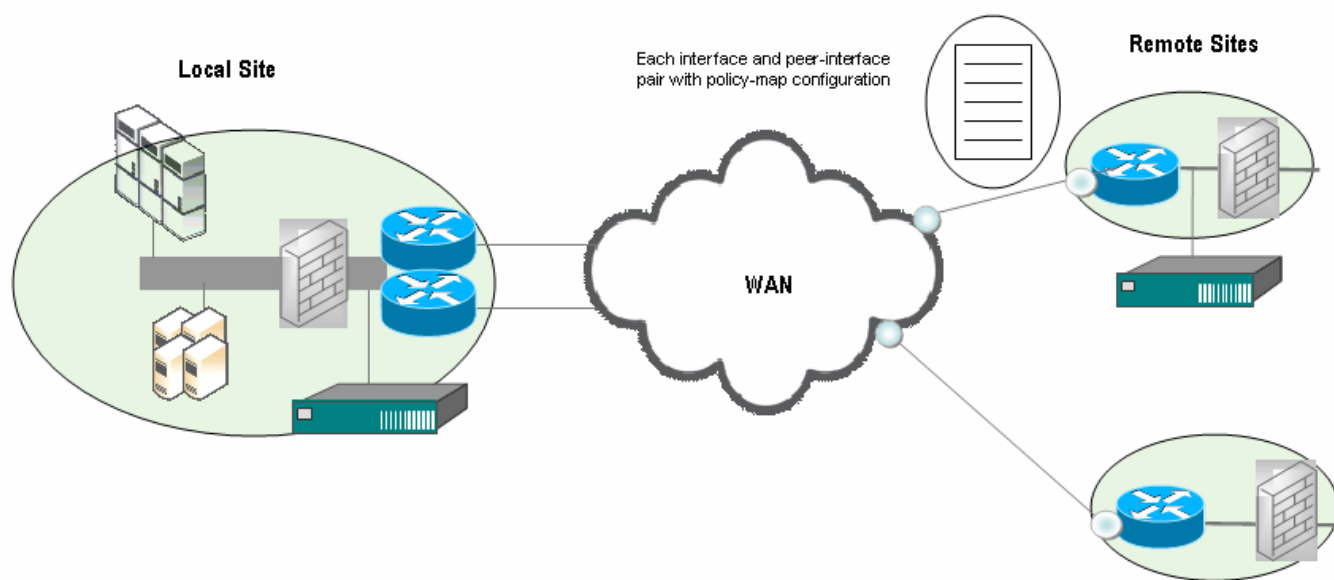
-
- Step 1** Click the named local site link or the **edit** link.
 - Step 2** The **Edit Local Site** page is displayed.
 - Step 3** Enter a brief description of the site in the **Site Description** field.
 - Step 4** Enter the site subnet address and prefix in the **Subnet** field, in this example 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 Cisco ADE physical ports from the **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 **Add Interface**.

- Step 10** Enter a name in the **Interface Name** field, in this example FastEthernet0.
- Step 11** Enter a brief description in the **Description** field.
- Step 12** Enter the link bandwidth for the interface, in this example 100 Mbps, in the **Bandwidth** field.
- Step 13** Select the policy-map for the interface from the **Policy Map** list.
- Step 14** Select **MPLS VPN...** as the **WAN Connectivity** type.
- Step 15** Click **Edit** and check that the peer-interface details in the Service Provider panel are correct.
- Step 16** Click **Save**.
- The **Edit Router** page is displayed.
- Step 17** Click **Save**.
- The **Edit Local Site** 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 3-15 *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** Click **Add Router**.
- The **Add Router** page is displayed.
- Step 6** Enter a name in the **Router Name** field, in this example remote1.
- Step 7** Enter a brief description in the **Router Description** field.
- Step 8** To configure an interface for the router, click **Add Interface**.
- Step 9** Enter a name in the **Interface Name** field, in this example Serial0/1.
- Step 10** Enter a brief description in the **Description** field.
- Step 11** Enter a link bandwidth for the interface, in this example 512 kbps, in the **Bandwidth** field.
- Step 12** 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 13** 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 14** Enter an IP address of an available device at the remote site that is pinged for end-to-end roundtrip measurements. Click **Test** to send a few packets to confirm the availability and accessibility of the specified IP address. The outcome of the test is displayed in a pop-up window.
- Step 15** Enter the IP address of the BQM appliance at the remote site to facilitate PNQM measurement.
- Step 16** Check that the peer-interface details in the Service Provider panel are correct.



Note You need only configure PNQM for the remote site interface of interest. You do not need to configure PNQM details for the associated peer-interface.

- Step 17** Click **Save**.
- The **Edit Router** page is displayed. Click **Test** to check the viability of the PNQM channel with the specified IP address. The outcome of the test is displayed in a pop-up window.



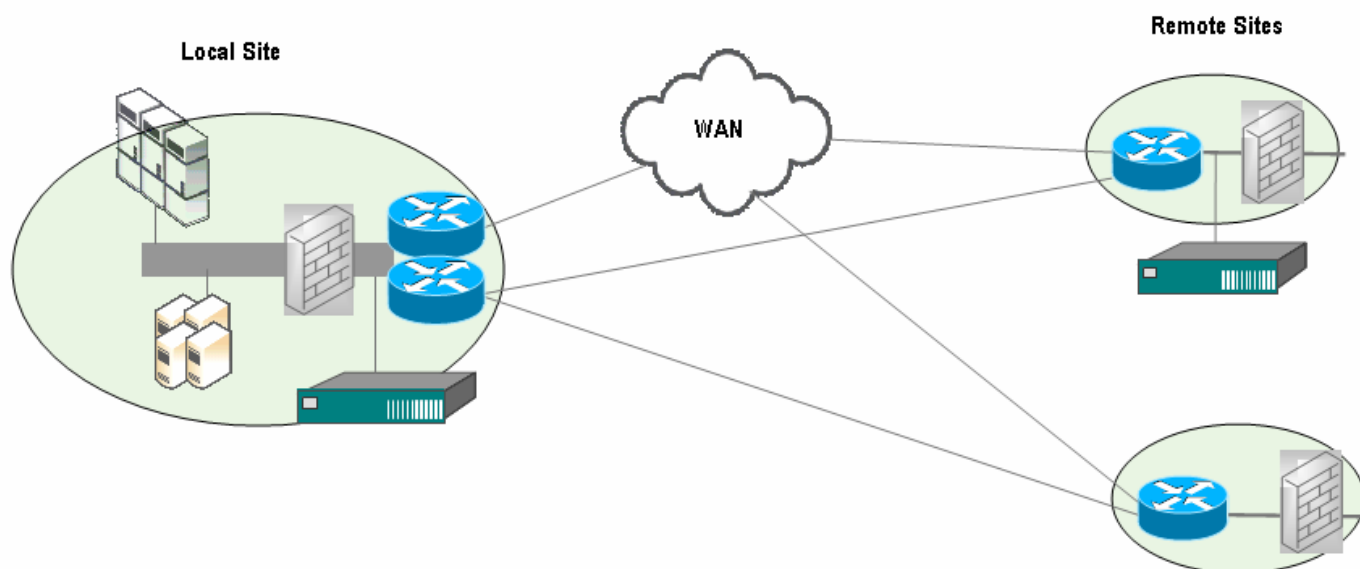
Note For more information on testing the PNQM channel, see the section “Defining a Passive Network Quality Monitoring (PNQM) Channel” in the chapter “Using the Command Line Interface (CLI).”

- Step 18** Click **Save**.
- The **Edit Remote Site** 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 15 and Step 17 to Step 19 to add the remote site for which there is no BQM appliance installed and no PNQM measurement is required.
-

Hybrid Deployment

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

Figure 3-16 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 Service Quality

This chapter describes the end-to-end BQM network service objective management feature. The displayed information enables you to identify network-wide issues and serves as a launching point for further investigation of issues with event analysis, network traffic statistics and bandwidth sizing measurements.

When the network service objectives have been defined and assigned (via policy-maps) to interfaces and classes, BQM 4.0 monitors whether these objectives are being met by the network. The following technologies are used for this purpose:

Passive Network Quality Monitoring – passive measurement of one-way latency, jitter, and loss.

Passive Network Quality Monitoring (PNQM) takes accurate timestamps of streams of packets as they pass two locations in the network. The timestamps are compared at a central location, and highly accurate measurements of the latency, loss and latency variation experienced by the packet stream between the two locations are available. The feature can be configured to measure all packets, or to measure a sample of packets. If all packets are measured, then all latency and loss violations of the network service objective will be observed.

By uniquely identifying what portion of the loss and latency are attributable to specific links and QoS policies, and which are service provider cloud issues, BQM 4.0 offers diagnostic information unavailable elsewhere, which should save money both in troubleshooting time and in useless upgrades.

Expected Queuing

Expected Queuing (EQ) estimates the loss and queuing latency that classes and applications can expect to incur when they interact with the queues and schedulers in the network. Although Expected Queuing focuses on the principal speed mismatch points in the network, rather than an end-to-end view, it is true to say that if the end-to-end target is violated in the EQ-modeled queue, then it will be violated end-to-end for the application traffic.

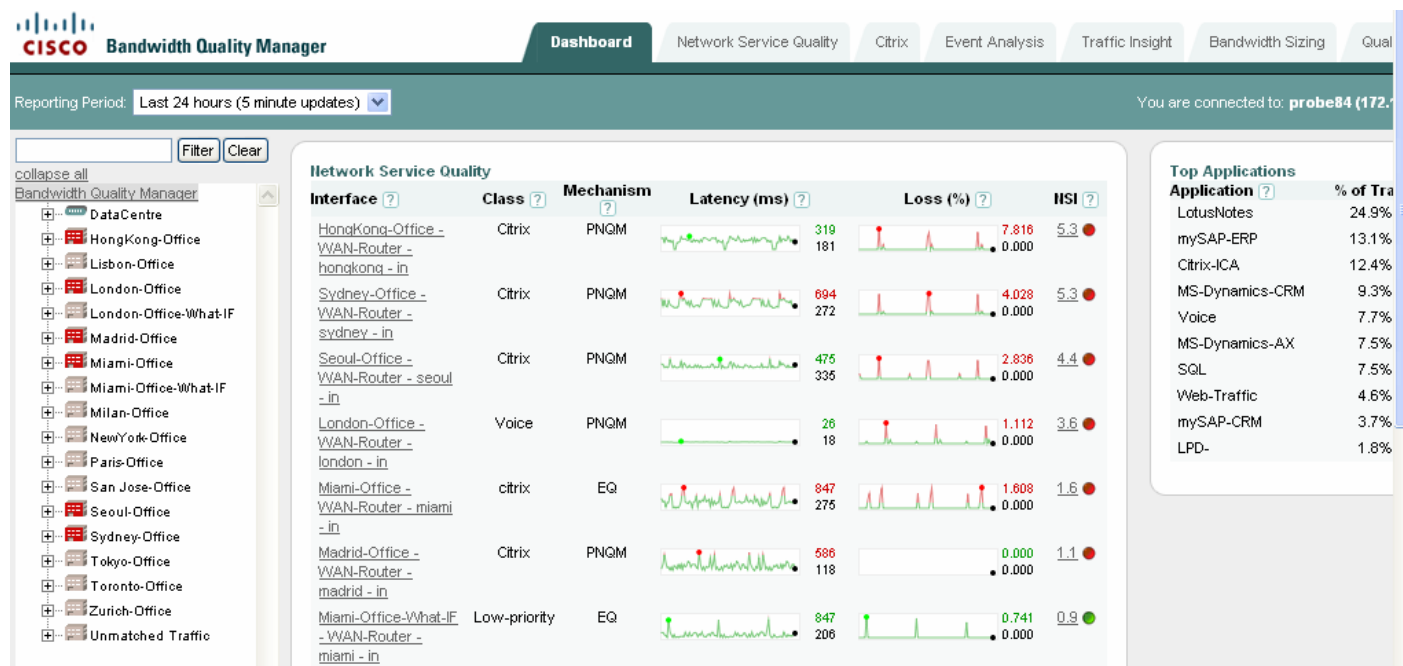
ICMP Ping – active measurement of roundtrip latency and loss

Although ICMP pings will not catch all loss and latency violations that the application traffic may incur, it is highly likely that if the ICMP ping results violate the end-to-end network service objective, then it will be violated for the end-to-end application traffic.

Monitoring Dashboard Overview

This section introduces the use of 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 use BQM to investigate the problem. The detailed analysis of traffic is done using the **Network Service Quality**, **Event 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:

- **Network Service Quality** - a list of the top ten interfaces most frequently experiencing network service quality issues and a chart of the total number of interfaces meeting service objectives.
- **Top Applications**- the list of the top ten applications using most resources on the network.
- **Recent Alarms** - a list of most recent network quality alarms.


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 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 Network Service Quality Issues

The **Network Service Quality** section of the dashboard displays the top ten interfaces experiencing network service quality issues on the network. Local site interfaces are indicated by the  icon.

The following describes the congestion information displayed on the dashboard:

Interface - displays the full name of the interface: 'site name - router name - interface name - direction'.

Class - displays the name of the class experiencing the network service quality issue.

Mechanism - displays which technology is being used to provide the displayed measurements: PNQM, EQ, or ICMP, depending on which mechanism is configured.

Latency - displays a sparkline chart of the one-way latency measurements for this class (PNQM or EQ) or interface (ICMP) during the chosen reporting period.

Loss - displays a sparkline chart of the packet loss for this class (PNQM or EQ) or interface (ICMP) during the chosen reporting period.

NSI - displays a number reflecting the network service quality level for an interface. The number represents the worst Network Service Index (NSI) value seen on any class on that interface. A Network Service Index value greater than 1 means the loss and/or latency are greater than that specified. A Network Service Index of less than 1 means the loss and latency are better than that specified.

If you click on an interface name in the list, the **Network Service Quality** tab is displayed, showing the details of the congestion events associated with that interface.

Using Sparklines

BQM uses ‘sparklines’ to give intuitive representations of time-varying network conditions in a compact form. Sparklines in BQM provide clear visual indication of which measurements are violating thresholds, and of the magnitude and timing of violations. You can easily identify service level violations above configured thresholds by a change in sparkline color. For example, sparklines are green when measurements are below the configured threshold, and red when the threshold is broken.

Figure 4-2 Sparklines



Loss, latency and microburst sparklines show two numbers to the right of the sparkline, one above the other. The upper number represents the largest value in the time-series and is colored red/green according to whether it is above or below the threshold. The lower number is the most recent value and is colored black. The corresponding points on the sparkline have red/green and black visible dots accordingly.

Each point in the sparkline represents the maximum value of the series of five-minute values over the time period covered by that point. For example, for a 1-hour sparkline, there is one point for each of the 12 five-minute measurements. For a 60-day sparkline, each point represents the largest five-minute value measured during the 15 hours summarized by that point.



Note Latency and jitter sparkline values displayed on the **Dashboard** and the **Network Service Quality** tab are based on the xxth percentile of measured values, as configured in the network service objective (default 99.9%).

So in these cases each point in the sparkline represents the configured xxth percentile of the series of five-minute values over the time period covered by that point. For example, for a 1-hour sparkline, there is one point for each of the 12 five-minute measurements. For a 60-day sparkline, each point represents the largest xxth percentile five-minute value measured during the 15 hours summarized by that point.

As a consequence, the upper number will not necessarily match the maximum value displayed beside the corresponding class graphs.

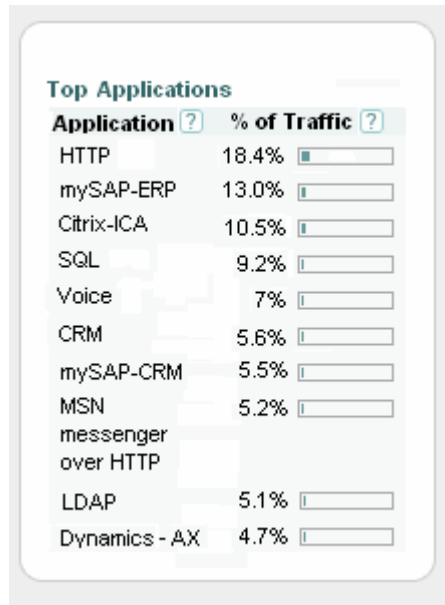
Sparklines enable you to

- Identify service level threshold violations in the network at a glance.
- Identify whether latency, latency variation or loss targets are being exceeded.
- Identify the magnitude and timing of violations before further investigation.

Identifying Top Applications

The **Top Applications** list displays the applications that have the top ten highest average volumes over the selected reporting period for all traffic.

Figure 4-3 Top Applications



The following describes the top application information displayed:

Application - displays the name of the application; 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.'



Note The list of automatically-discovered applications includes the Corvil Signature Streaming Protocol (SSP) used to facilitate system traffic between local and remote BQM devices.

% 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.

Identifying Recent Quality Alarms

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

Figure 4-4 Recent Quality Alarms

Recent Alarms					
Interface/Class	Type	Time	Count	Severity	

Interface/Class - 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 events that were coalesced into this alarm.

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.

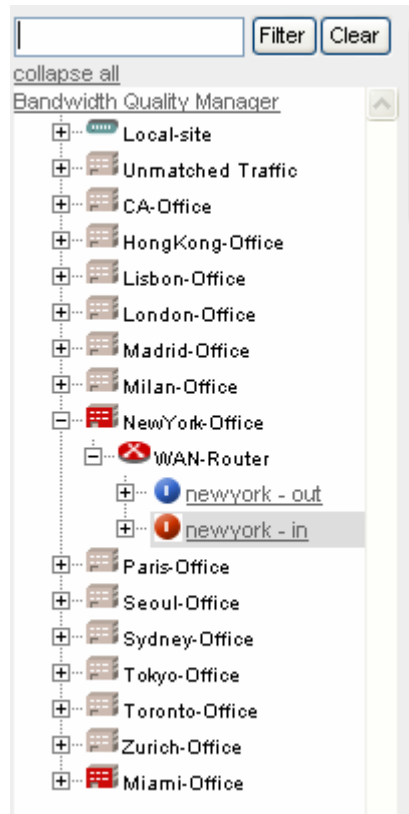
Quality alarms are generated whenever an event is generated. An alarm of a particular type persists until the system detects an interval with no events of that type. To avoid floods of alarms, the system also applies a configurable coalescing period to alarms. For example, if you have configured a delay 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 recently raised alarms are shown.

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:

- Network Service Quality results
- Top Applications results

For local site outbound and remote site inbound interfaces, the summary results include Network Service Index, Corvil Bandwidth and End-to-End Latency and Loss graphs. For local site inbound and remote site outbound interfaces, the summary results include Microburst graphs.

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

Figure 4-6 Network Service Quality 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 network service objective 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 network service objective applied to the interface.

NSI - indicates quality issues in the network. The Network Service Index uses PNQM measurements and EQ, when configured, to detect events impacting end-to-end network quality based on the specified quality of service targets. Use the **Network Service Objectives** menu in **System Administration** mode to set the quality targets that are used to calculate the Network Service Index. If you have not enabled Network Service Index calculation in the network service objective being applied to an interface or class, a dash is displayed.

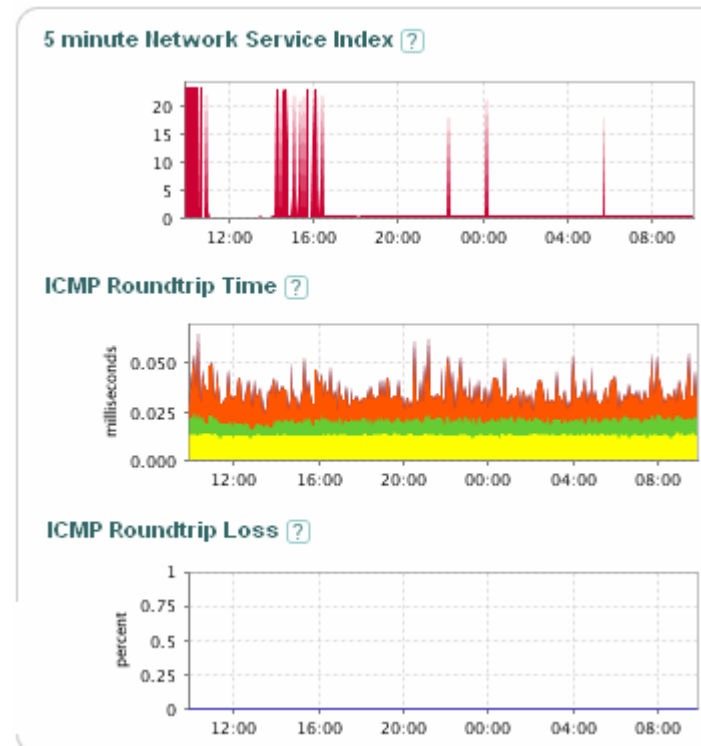
Network Service Quality Results

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. In the absence of a configured value, the default resolution for microburst measurements is 50 milliseconds.

For local site outbound interfaces and remote site inbound interfaces, the 5 minute Network Service Index graph displays the calculated NSI values during the selected reporting period.

In both cases, the interface level graphs include ICMP roundtrip and loss results, if configured.

Figure 4-7 Local Site Outbound and Remote Site Inbound Interface Graph Results



Click the 5 minute Network Service Index graph to view more detailed results for the class on the **Event Analysis** tab.

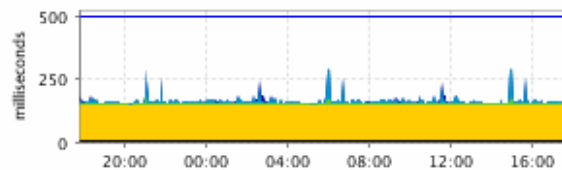
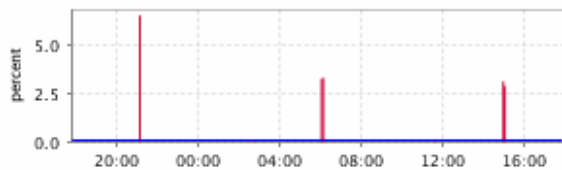
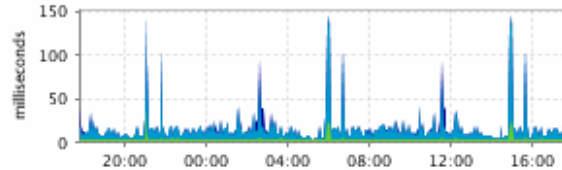
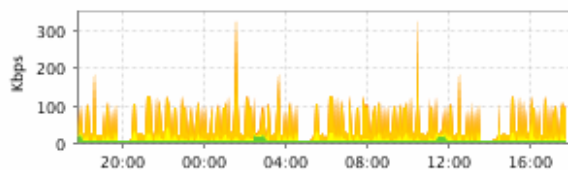
Click the Microburst graph to view more detailed results for the class on the **Traffic Insight** tab.

Click any of the other graphs to view more detailed results for the class on the **Network Service Quality** tab.

Class results include the following graphs, if configured:

- 5 minute Network Service Index
- End-to-End Latency
- End-to-End Jitter
- End-to-End Loss
- Corvil Bandwidth - Delay

For classes on local site inbound and remote site outbound interfaces, the Corvil Bandwidth results are retrieved from the remote BQM appliance, if the remote device is configured appropriately.

Figure 4-8 Class Graph Results**5 minute Network Service Index ?****End to End Latency ?****End to End Loss ?****End to End Measured Jitter ?****Corvil Bandwidth Delay ?**

Click the 5 minute Network Service Index graph to view more detailed results for the class on the **Event Analysis** tab.

Click any of the other graphs to view more detailed results for the class on the **Network Service Quality** tab.

Top Applications Results

The top applications summary for interfaces and classes include the following:

Figure 4-9 Top Applications Results



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.

Monitoring Quality Alarms

By default the **Quality Alarms** tab lists all active or cleared alarms triggered due to quality events in the network. 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 4-10 Quality Alarms

Alarms

Dropped Packets: mgmt: 0 PortA: 44687228 PortB: 48015868 PortC: 44687249 PortD: 44687245 packets dropped during capture: 188294204

No alarm(s) found.

Source Name Time Severity Status Count




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 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.

The following table describes the information displayed in the quality alarms table:

Table 4-1 Quality Alarms Table

Column	Description
Source	Displays the full, qualified name identifying the interface or class for which the alarm was triggered: <i>site name – router name – interface name – direction – class name</i> .
Name	Displays the type of quality alarm that has been triggered.
Time	Displays the time at which the active alarm triggered, or at which a cleared alarm was cleared.
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

Status	Indicates whether the alarm is active or cleared. You can use the filter  to display only active or only cleared alarms.
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.

The following table describes the alarm types that may be displayed on the **Quality Alarms** tab:

Table 4-2 Alarm Types

Alarm Type	Description
Corvil Bandwidth Threshold Exceeded	The Corvil Bandwidth measurement indicates the class bandwidth threshold has been exceeded.
E2E Availability Issue	An issue with completing ICMP measurements has been detected.
E2E Delay Threshold Exceeded	The ICMP roundtrip latency exceeded the configured threshold.
ICMP Loss Detected	Packets have been lost during ICMP roundtrip measurement.
Expected Policing Threshold Exceeded	The expected policing value crossed the configured threshold.
Expected Queuing Delay Threshold Exceeded	The expected queuing delay crossed the configured threshold.
Expected Queuing Loss Threshold Exceeded	The expected queuing loss crossed the configured threshold.
ICMP Failure Detected	ICMP end-to-end measurement is not operating.
Microburst Detected	Microbursts exceeding the configured bandwidth threshold have been detected.
Network Service Threshold Exceeded	The Network Service Index has crossed the configured threshold.
PNQM Failure Detected	PNQM end-to-end measurement is not operating possibly due to network, version, license or configuration problems - see logs for details.
PNQM Latency Threshold Exceeded	PNQM latency measurements have exceeded the configured threshold.
PNQM Latency Variation Threshold Exceeded	PNQM latency variation measurements are exceeding the configured threshold.
PNQM Loss Threshold Exceeded	PNQM loss measurements are exceeding the configured threshold.

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  beside the **Name**, **Severity**, or **Status** 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 appliance.

Figure 4-11 Quality Alarms Report

Bookmarks

Signatures

Layers


Pages

Comments

Welcome admin:

Last updated at 04 Jul 10:30 UTC

Bandwidth Quality Manager



Bandwidth Quality Manager

Quality Alarms

Reporting Period: Last 24 hours (5 minute updates)

You are connected to: probe85 (172.18.2.85)

Alarms

Dropped Packets: mgmt: 0 PortA: 0 PortB: 0 PortC: 0 PortD: 0 packets dropped during capture: 0

Filter: "Server"

1 to 15 of 137 alarm(s)

Source	Name	Time	Severity	Status	Count
+ server-1 - c72c - serial3/0 - out	Expected Queuing Delay Threshold Exceeded	2007-07-04 10:31	Major	Cleared	403
+ server-1 - cloudtr - cloudtr.v60 - out	PNQM Latency Threshold Exceeded	2007-07-04 10:28	Warning	Cleared	92
+ server-1 - c72c - serial3/0 - af11.cmap - out	PNQM Latency Threshold Exceeded	2007-07-04 10:26	Warning	Active	172
+ server-1 - c72c - serial3/0 - af11.cmap - out	PNQM Loss Detected	2007-07-04 10:26	Warning	Active	201
+ server-1 - c72c - serial3/0 - af13.cmap - out	PNQM Latency Threshold Exceeded	2007-07-04 10:26	Warning	Active	194
+ server-1 - c72c - serial3/0 - af13.cmap - out	PNQM Loss Detected	2007-07-04 10:26	Warning	Active	211
+ server-1 - c72c - serial3/0 - af21.cmap - out	PNQM Latency Threshold Exceeded	2007-07-04 10:26	Warning	Active	193
+ server-1 - c72c - serial3/0 - af21.cmap - out	PNQM Loss Detected	2007-07-04 10:26	Warning	Active	215
+ server-1 - c72c - serial3/0 - af23.cmap - out	PNQM Latency Threshold Exceeded	2007-07-04 10:26	Warning	Active	192
+ server-1 - c72c - serial3/0 - af23.cmap - out	PNQM Loss Detected	2007-07-04 10:26	Warning	Active	208
+ server-1 - c72c - serial3/0 - af31.cmap - out	PNQM Latency Threshold Exceeded	2007-07-04 10:26	Warning	Active	194

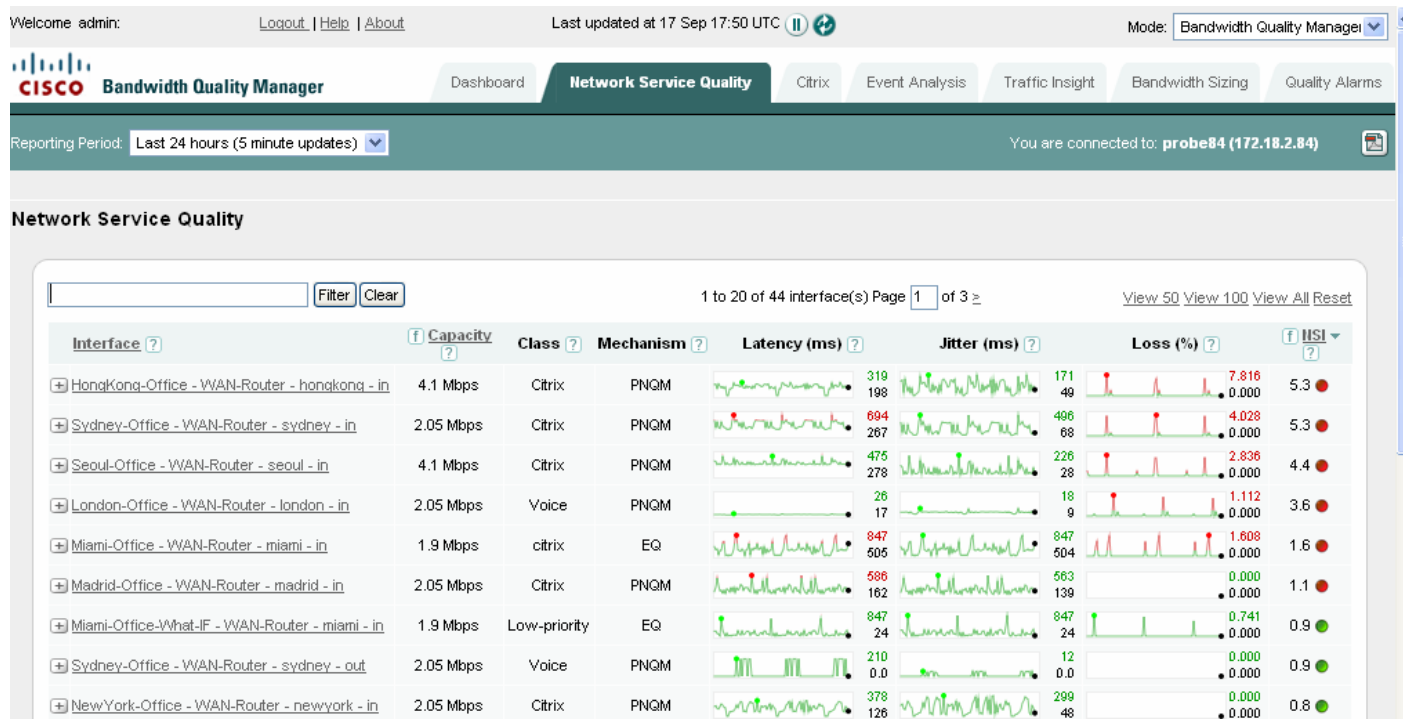
The generated report reflects all configured sorting or filtering of displayed data at the time the report is generated. For example you can set a reporting period, sort and filter the onscreen data to show all cleared major alarms sorted by time over the last hour. The report presents the results displayed on the current screen only.

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

Monitoring Network Service Quality

BQM enables you to identify end-to-end packet latency and loss measurements and assess the subsequent impact on the network. The **Network Service Quality** tab lists all of the interfaces you have configured in the BQM network model.

Figure 4-12 Network Service Quality Tab




The summary table information is sorted by Network Service Index value and provides a visual guide to service quality 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 for individual interfaces. You can also sort the summary information by certain columns and you can drill into each interface to view more details (such as class service quality).

Viewing Network Service Quality Results


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. 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 describes the information displayed in the network service quality summary table:

Table 4-3 Network Service Quality Summary

Field	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 ATM PVC, FR PVC and Metro Ethernet deployments, the directly connected interface is shown in italics below a given interface. 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). Local site interfaces are indicated by the  icon.
Capacity	This is the bandwidth configured for the interface or class; for example, modeling a T1 line means configuring a capacity of 1.54 Mbps.
Class	Displays the name of the class with the highest Network Service Index value. Internally, each class has an NSI value calculated using PNQM and EQ, and the interface has an NSI calculated using ICMP. If PNQM is enabled, the name of the class with the highest PNQM-based NSI is displayed. This value is also then used as the NSI for the interface. Otherwise, the higher of the EQ and ICMP-based NSI values is used. If EQ contributes the highest NSI value then the name of the class with the highest EQ-based NSI value is displayed. If ICMP contributes the highest NSI value, this field is blank.
Mechanism	Displays the end-to-end monitoring mechanism that has produced the Network Service Index value.
Latency (ms)	Displays a chart of the one-way latency measurements for this class (PNQM or EQ) or interface (ICMP) during the chosen reporting period.
Jitter	Displays a chart of the one-way jitter measurements for this class (PNQM or EQ) or interface (ICMP) during the chosen reporting period.
Loss (%)	Displays a chart of the packet loss for this class (PNQM or EQ) or interface (ICMP) during the chosen reporting period.

Network Service Index	<p>Displays a unitless number which reflects the congestion level on an interface or class. For a class, it reflects the extent by which the loss and/or latency experienced by the class exceed the user-specified targets. For an interface, it represents the worst Network Service Index value seen on any class on that interface.</p> <p>If you have not enabled Network Service Index calculation in the network service objective being applied to an interface, a dash (-) is displayed</p>
-----------------------	--

Each interface entry in the Network Service Quality table can be expanded to display information for configured classes. Click  beside the interface name to expand an interface.



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 five minutes 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.

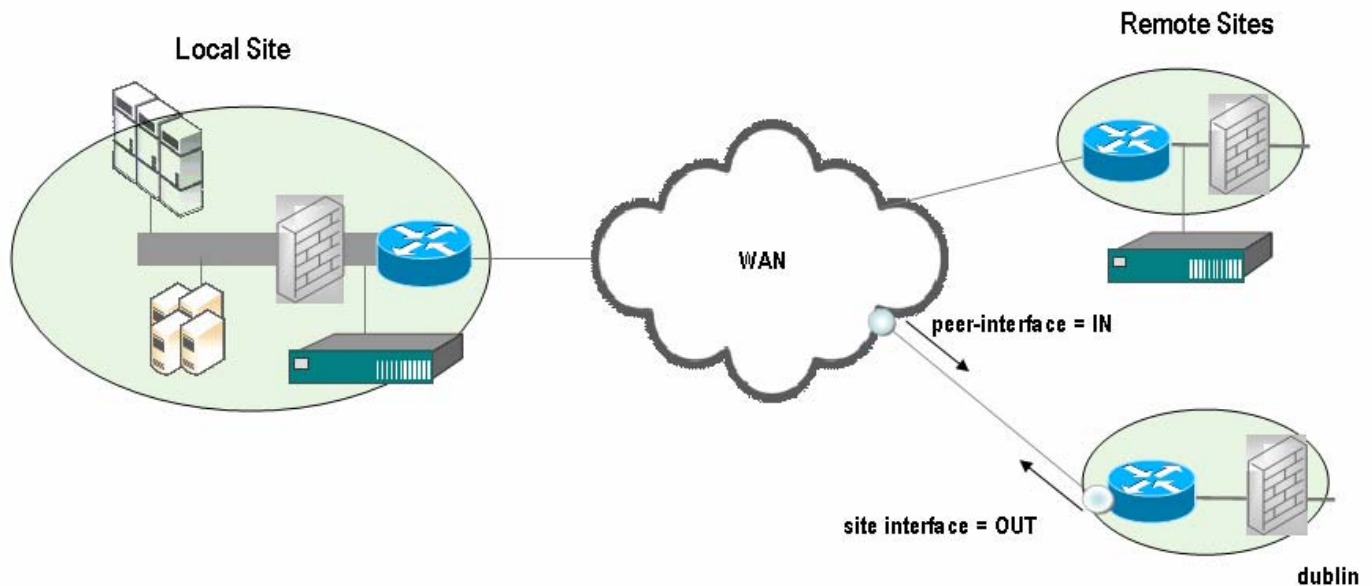
You should wait about ten minutes (that is, after a couple of data updates) following a configuration change before viewing graphs.

In general, 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.

The sparkline charts displayed on the summary screen use data generated by either PNQM, ICMP or EQ, depending on which of the mechanisms is configured:

Table 4-4 Mechanisms Used to Graph Results

PNQM Active?	ICMP Active?	EQ Active?	Graphs Use
Yes	No	No	PNQM
No	Yes	No	ICMP
No	Yes	Yes	ICMP or EQ (Whichever produces greatest NSI value.)
No	No	No	No Results

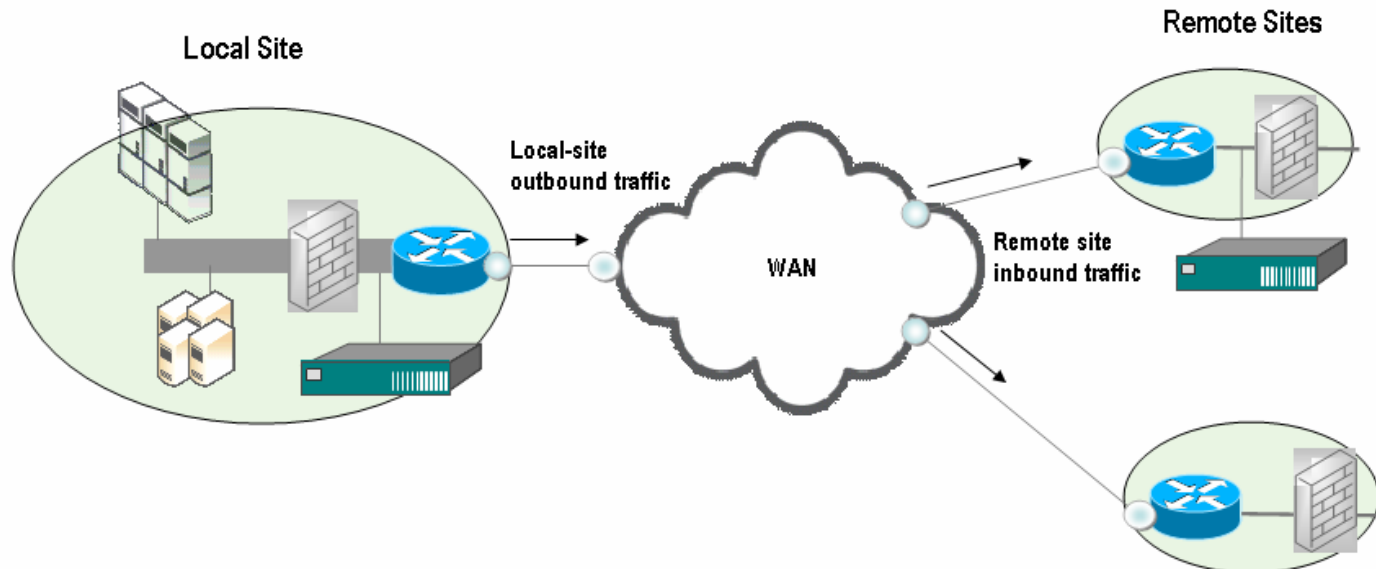
Figure 4-13 MPLS VPN, Internet VPN, Private VPN Network Model

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 4-14 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 monitoring features are otherwise enabled in the current configuration, the following information is available only for the outbound direction of local site interfaces and the inbound direction of remote site interfaces:

- Expected Queuing Latency, Expected Queuing Delay Variation and Expected Queuing Loss graphs on the **Network Service Quality** tabs, unless a manual BQM configuration has been performed at the remote site.
- Corvil Bandwidth, Expected Queuing Delay, and Expected Queuing Loss graphs on the **Event Analysis** tab
- Bandwidth Sizing – post-queuing interfaces are not displayed on the **Bandwidth Sizing** tab

If both the local and remote sites have matching BQM configurations, then EQ results will be retrieved from the remote BQM for display on the local BQM when viewing EQ graph results for post-queuing interfaces.

All other graphs, charts and results on the **Traffic Insight** tab are available for both directions of traffic. When you click on an interface name, the traffic statistic graphs displayed for the interface are as follows:



Note For more information on performing manual configuration of remote BQM appliances to support the display of EQ results for both directions of traffic, see the section “Manual PNQM Configuration” in the chapter “Using the Command Line Interface (CLI).”

Selecting a Report Period

By default, the **Network Service Quality** 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 - 30 minute updates
- Last 30 days - 2 hour updates
- Last 60 days - 6 hour updates

The text above the summary table 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 | Select Custom Period from the Select Reporting Period list. |
| Step 2 | Click select beside the From Date field and choose a date from the calendar. |
| Step 3 | Choose a time from the list of half-hour intervals. |
| Step 4 | Click select beside the To Date fields and choose a date from the calendar. |
| Step 5 | Choose a time from the list of half-hour intervals. |
| Step 6 | 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. If you click the **Related Links** for the interface, the defined custom period is used to display the related interface information.

The global **Select Reporting Period** field is set to Custom Period.

Sorting the Network Service Quality Table


The **Network Service Quality** table is sorted by the **NSI** column by default, but you can sort this table by either the **Interface** or **Capacity** columns. 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 Network Service Index values, you click the **NSI** column heading to sort. The summary is rearranged according to the maximum Network Service Index values per interface, with the highest value first. Click the **NSI** column heading again to sort the summary screen again, this time with the lowest measured Network Service Index value first.

Filtering the Network Service Quality Table

You can use the search facility on the Network Service Quality table to display a particular interface or set of interfaces of interest. Enter the name of the required interface or use a wildcard (*) 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) that contain the word Serial. Interfaces containing the word 'serial' will not be returned.

The **Network Service Quality** tab also provides the option to filter results based on the configured interface capacity or NSI values. Click  beside the **Capacity** or **NSI** column headings and select an option from the list. The screen will refresh, displaying only the results relevant to the filtering option you selected.

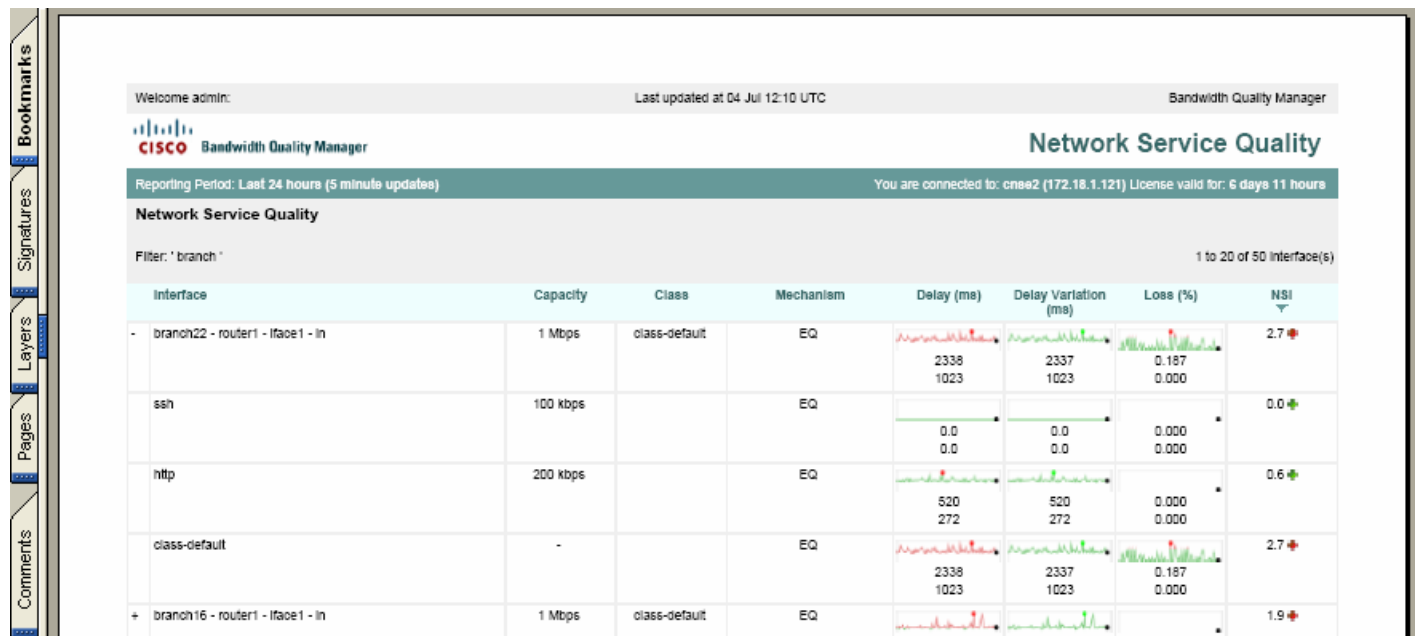
Reporting Network Service Quality Results

You can generate a report in .pdf format at any point when viewing results.

To generate a report, click .

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

Figure 4-15 Network Service Quality 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 Network Service Index 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 Results

Click the linked interface name in the Network Service Quality table to get access to graph results for interfaces and classes. 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 outbound interface information.

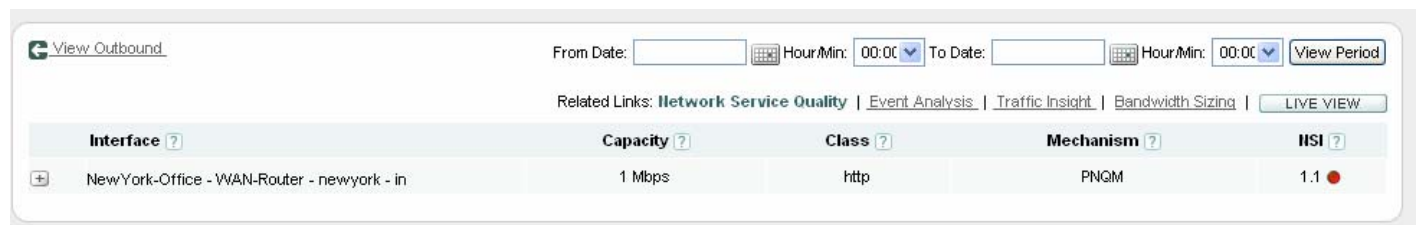
You can switch to the event analysis, traffic statistics and bandwidth sizing results for the interface by clicking the relevant link from **Related Links**.

You can also define a custom reporting period for viewing interface results. See the topic “Defining a Custom Report Period” for more information.

Viewing Live View Results

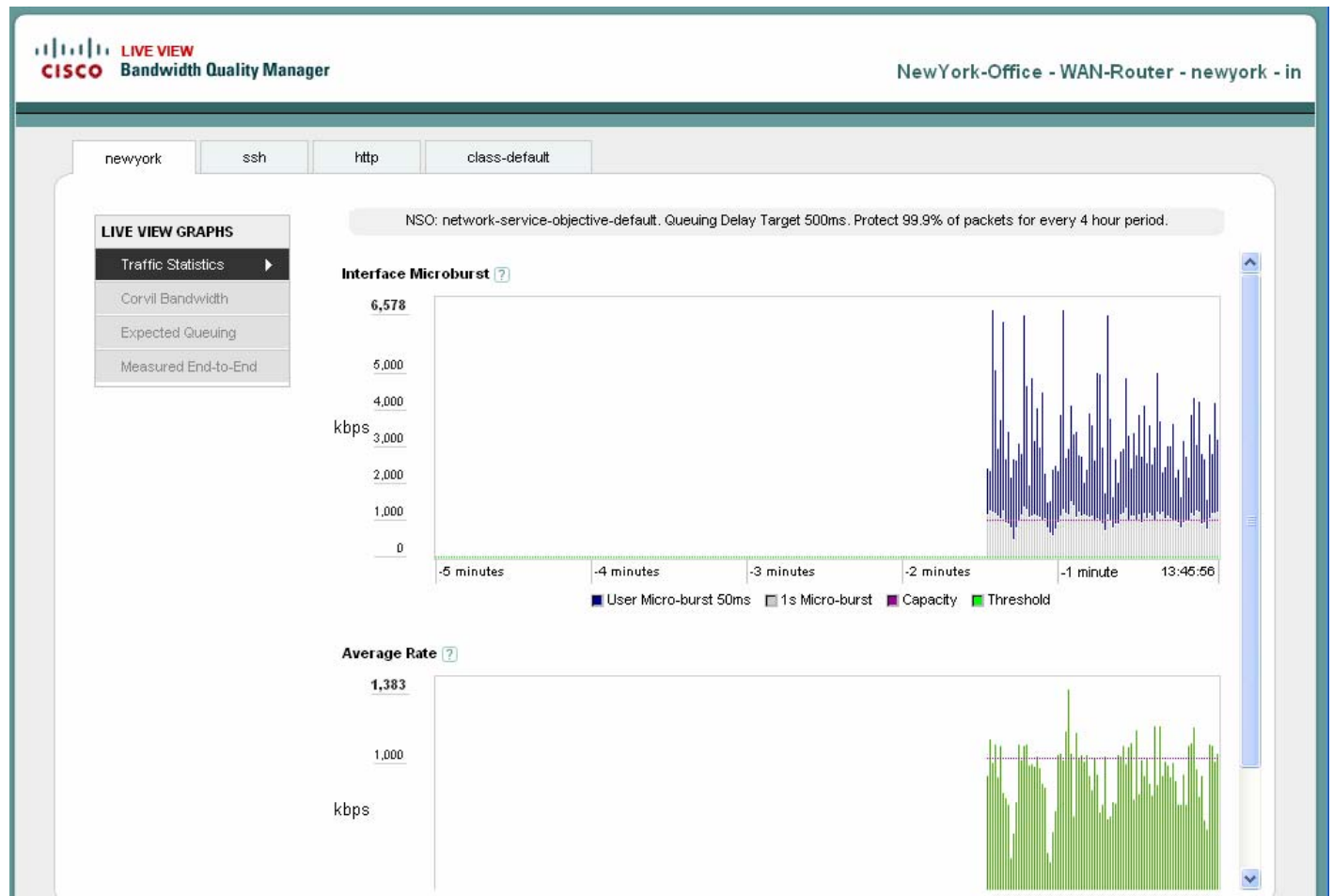
The purpose of the live monitoring view is to enable you to troubleshoot current performance issues on the network. When you launch the live monitoring view a new window is opened displaying graphs for the interface and classes under separate tabs. All graphs update every second giving you a unique insight into the traffic currently being measured.

Figure 4-16 Live View Button



To view live results for an interface and its classes, you click **Live View**.

Figure 4-17 Live View – Interface Results

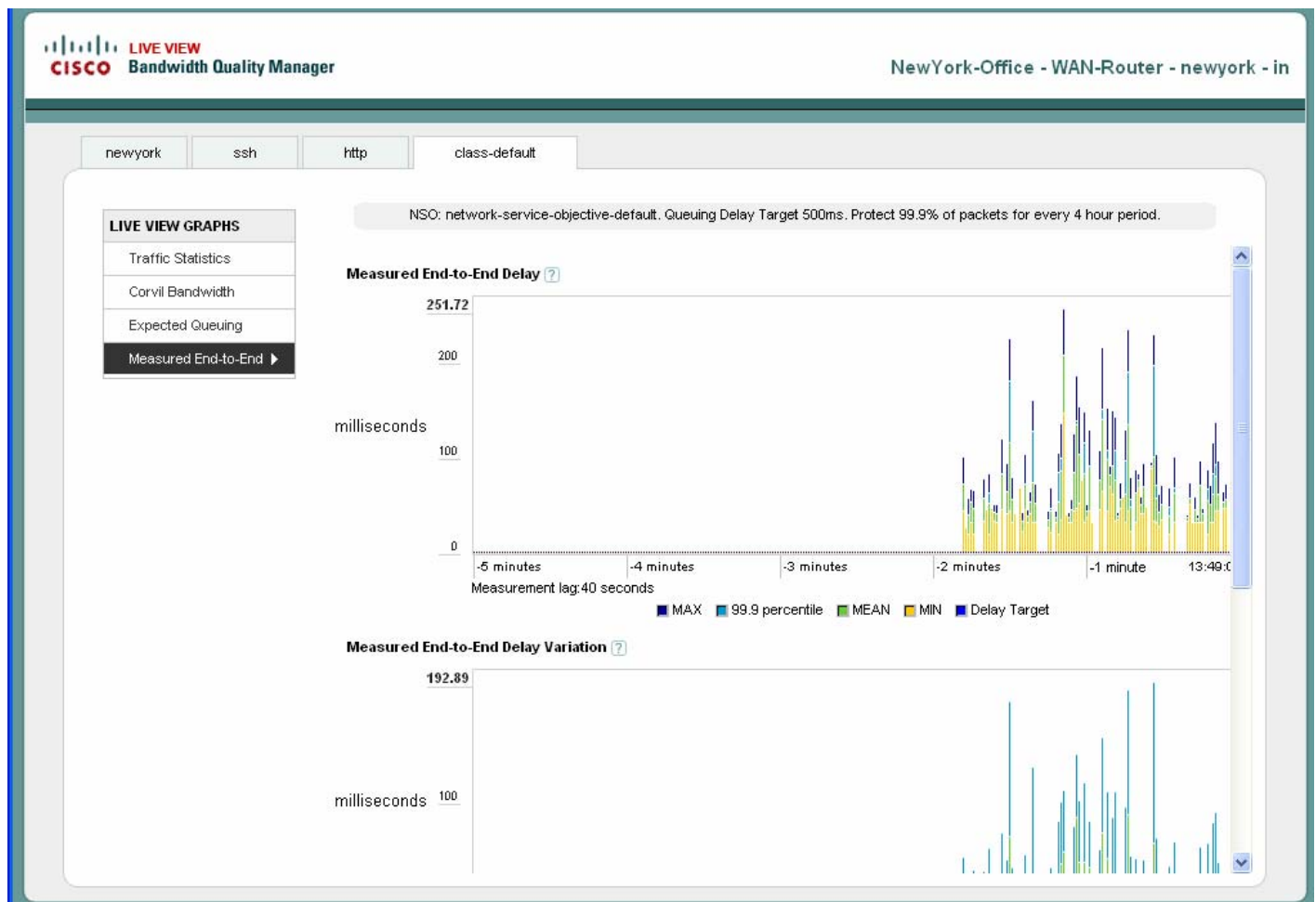


A new window opens and by default displays traffic statistics for the chosen interface. All graphs displaying bandwidth results include a unit formatter so you can view results in kbps, Mbps, or Gbps. The graphs available at interface level are

- Interface Microburst
- Average Rate

There are tabs displayed for each configured class on the interface. Click a tab to display live results for that class.

Figure 4-18 Live View – Class Results



There are a range of live graphs available for classes. When you open a class tab, the following traffic statistics graphs are displayed by default:

- Class Microburst
- Average Rate

New data points are plotted from the right of the graph each second and the plot grows to the left as time elapses. The timeline is displayed along the x-axis, with the current system time displayed to the right.

To view the other live results, you choose a category from the **Live View Graphs** menu:

- **Corvil Bandwidth** for Corvil Bandwidth delay and queue length graphs
- **Expected Queuing** for Expected Queuing Latency, Expected Queuing Delay Variation, and Expected Queuing Loss graphs
- **Measured End-to-End** for End-to-End Latency, End-to-End Jitter, and End-to-End Loss graphs


Each of these graphs plots the maximum, configured percentile, mean, and minimum values for the one-second period, along with any configured thresholds.



Note There is a time delay associated with the display of Measured End-to-End results in the live view compared to the display of the other results. The duration of the time delay is indicated below each graph.

The unique visibility into current network traffic behavior enables you to troubleshoot issues affecting user experience as they happen.

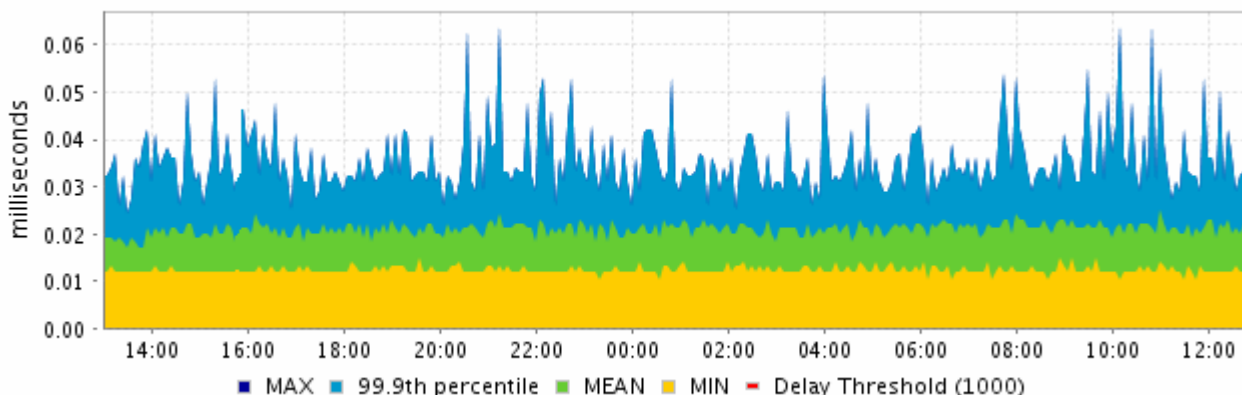
Viewing ICMP Round Trip and Packet Loss

When you expand an interface by clicking , the graphs available for round trip events are as follows:

- ICMP Roundtrip time
- ICMP Roundtrip jitter
- ICMP Roundtrip loss

The ICMP Roundtrip Time 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. The graph legend indicates the colors used to display the following:

Figure 4-19 ICMP Roundtrip Time Graph



Max - displays the maximum round trip time (in milliseconds) per ICMP ping packet each five minutes during the chosen reporting period.

x% percentile - displays the xth 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

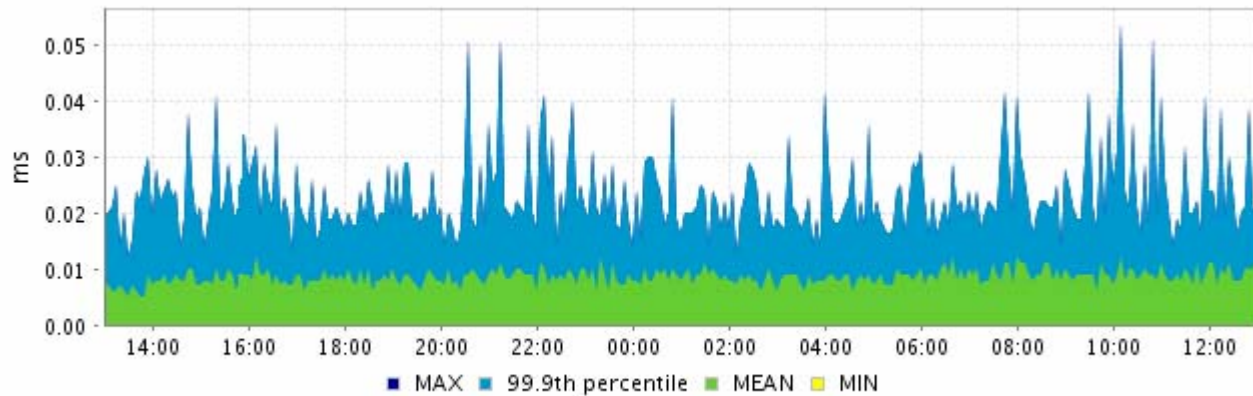
Mean - displays the mean of the round trip times for each five minutes during the chosen reporting period

Min - displays the minimum round trip time per ICMP ping packet each five minutes during the chosen reporting period.

Delay Threshold - indicates the value of the delay threshold configured in the network service objective being applied. Default is twice the configured one-way latency.

The ICMP Roundtrip jitter graph plots the delay variation measured for a round trip between the chosen remote site and the local site by ICMP ping packets. The jitter is displayed as a series of millisecond measurements for each packet sent on the round trip, showing the difference between the maximum, percentile, and mean latency values and the minimum latency value. The graph legend indicates the colors used to display the following:

Figure 4-20 ICMP Roundtrip Jitter Graph



Max - displays the maximum round trip time (in milliseconds) per ICMP ping packet each five minutes during the chosen reporting period.

x% percentile - displays the xth 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

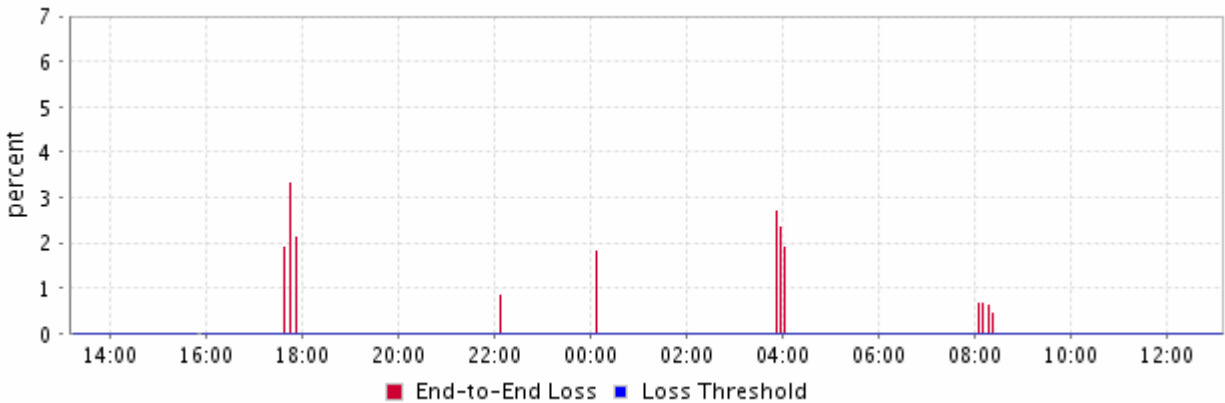
Mean - displays the mean of the round trip times for each five minutes during the chosen reporting period

Min - displays the minimum round trip time per ICMP ping packet each five minutes during the chosen reporting period.

Delay Threshold - indicates the value of the delay variation threshold configured in the network service objective being applied. Default is twice the one-way latency variation, if configured.

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 4-21 ICMP Roundtrip Loss Graph




End-to-end ICMP latency and loss measurement is enabled, and its characteristics defined, in the network service objective applied to the interface. The graphs are available for remote sites only.

In each case, 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.

The ICMP plots enable you to evaluate end-to-end performance. This can complement the local queuing latency 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 Class Measurements

Click  to view the graphs available for each class.

Text above the graphs shows the name of the network service objective used for this class, and which parameters are set for each (one-way latency, one-way latency variation, queuing-delay, protected packets % and time interval). There is also text above the End-to-End graphs indicating the percentage of time for which PNQM measurement was operating successfully during the selected reporting period. If traffic misclassification detection has been enabled for manual configuration of PNQM channels, then a count of misclassified packets is also displayed.

If GPS clock synchronization is set up, configured and operating, a GPS availability figure is also displayed, indicating the percentage of time GPS was working successfully during the selected report period.

If you are viewing class measurements for an interface in the Inbound direction and PNQM and EQ are both enabled, you can get the following results:

- End-to-End Latency
- End-to-End Loss
- End-to-End Jitter
- Expected Queuing Latency
- Expected Queuing Loss
- Expected Queuing Delay Variation

If you are viewing class measurement for an interface in the Outbound direction and PNQM and EQ are both enabled, you can get the following results:

- End-to-End Latency
- End-to-End Loss
- End-to-End Jitter
- EQ latency and loss retrieved from the far-end BQM and reported locally

If both of the mechanisms (PNQM and EQ) are disabled, the associated graph data is not available.

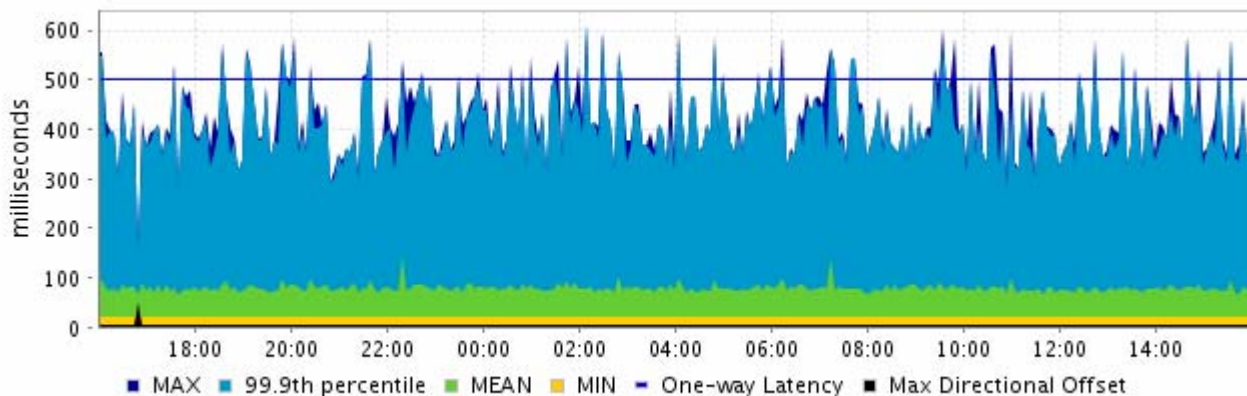
If you are viewing a configured priority class in a multiclass system, the Expected Queuing Loss graph is replaced by an Expected Priority Drops graph.

The end-to-end results (PNQM) complement the congestion-point queuing latency results (EQ). 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 End-to-End Latency, Jitter and Loss Results

The end-to-end graph results are based on PNQM measurements. If PNQM is not enabled, then these graphs are not available.

The End-to-End Latency graphs plots the measured latency for the chosen class. The one-way latency target is configured in the network service objective that is applied to the class.

Figure 4-22 End-to-End Latency Graph

The graph legend indicates the colors used to display each:

Max - displays the maximum of the end-to-end latency values (in milliseconds) measured each five minutes during the chosen reporting period.

x% - displays the xth percentile of end-to-end latency values in each five minutes during the chosen reporting period. This percentile is configurable as part of the packet protection target in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

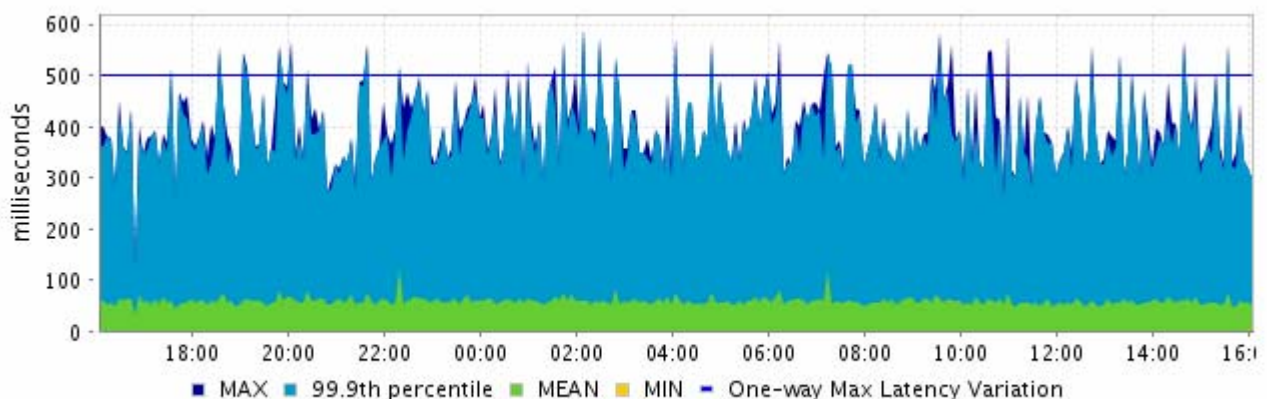
Mean - displays the mean of the end-to-end latency values for each five minutes during the chosen reporting period.

Min - displays the minimum of the end-to-end latency values for each five minutes during the chosen reporting period.

One-way Latency - indicated the configured one-way latency target

Max Directional Offset - displays the maximum uncertainty for each one-way latency measurement

The End-to-End Jitter graph plots the difference between the latency (maximum, percentile, or mean) and the minimum latency, for the selected class during the time interval displayed. On a five-minute plot it represents the difference between the 5-minute latency (whether the maximum, percentile, or mean value) and the 5-minute minimum. The one-way latency variation target is configured in the network service objective that is applied to the class.

Figure 4-23 End-to-End Jitter Graph

The graph legend indicates the colors used to display each:

Max - displays the maximum of the end-to-end jitter values (in milliseconds) measured each five minutes during the chosen reporting period.

x% - displays the xth percentile of end-to-end jitter values in each five minutes during the chosen reporting period. This percentile is configurable as part of the packet protection target in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

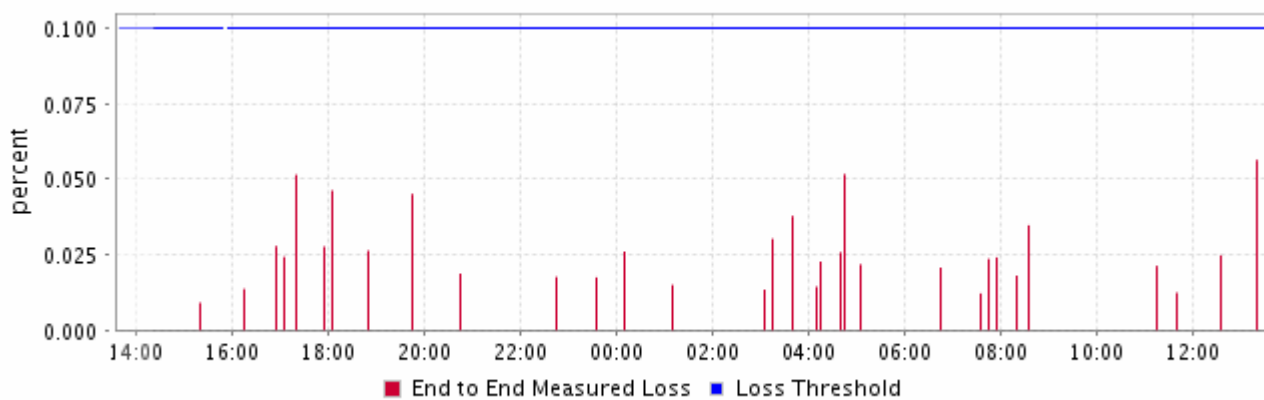
Mean - displays the mean of the end-to-end jitter values for each five minutes during the chosen reporting period

Min - displays the minimum of the measured end-to-end jitter values for each five minutes during the chosen reporting period.

One-way Max Latency Variation – indicates the configured one-way maximum latency variation target

The end-to-end measured loss graph plots the packet loss measured by the BQM for the chosen class traffic. The end-to-end loss is displayed as a percentage of the total packets measured by the BQM.

Figure 4-24 End-to-End Loss Graph



Loss estimation is enabled, and its characteristics defined, in the network service objective applied to the interface.

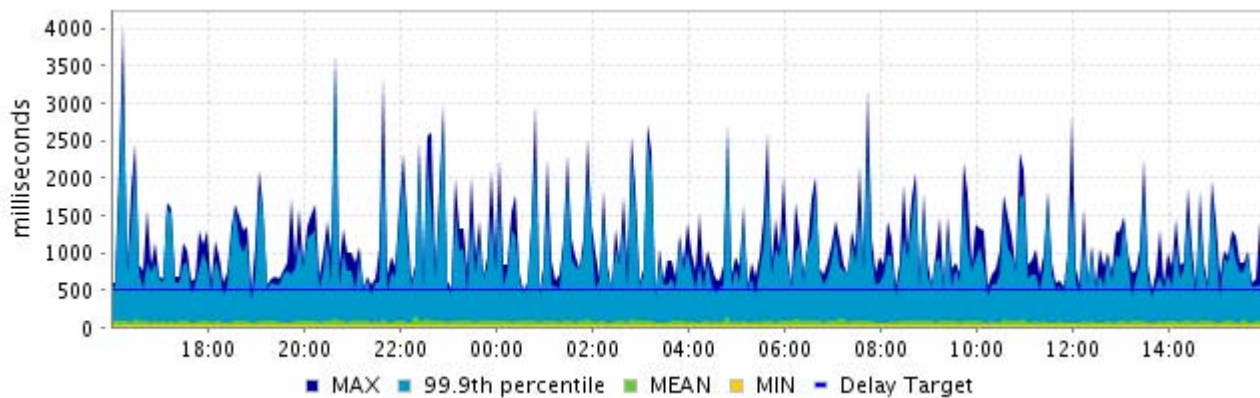
For all graphs, configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.

Viewing Expected Queuing Latency, Loss and Delay Variation Results

Each BQM supports the calculation of EQ results for pre-queuing points in the network only (that is, local-site outbound and remote site inbound interfaces from the perspective of each BQM). Results for post-queuing interfaces (local-site inbound and remote site outbound interfaces) from the perspective of the local BQM are in fact calculated on the remote BQM and exported to the local BQM for display. From the perspective of the remote BQM, these are pre-queuing interfaces, so the remote BQM calculates and exports EQ results to the local BQM. This effectively provides the local BQM with EQ results for its post-queuing interfaces that it would otherwise not support.

The expected queuing latency graph plots the per-packet latency calculated by the BQM using a simulation based on the chosen class traffic. The expected queuing latency is displayed as a series of millisecond values for each five minutes during the reporting period. The 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.

Figure 4-25 Expected Queuing Latency Graph



The graph legend indicates the colors used to display each:

Max - displays the maximum of the expected latency values (in milliseconds) calculated each five minutes during the chosen reporting period.

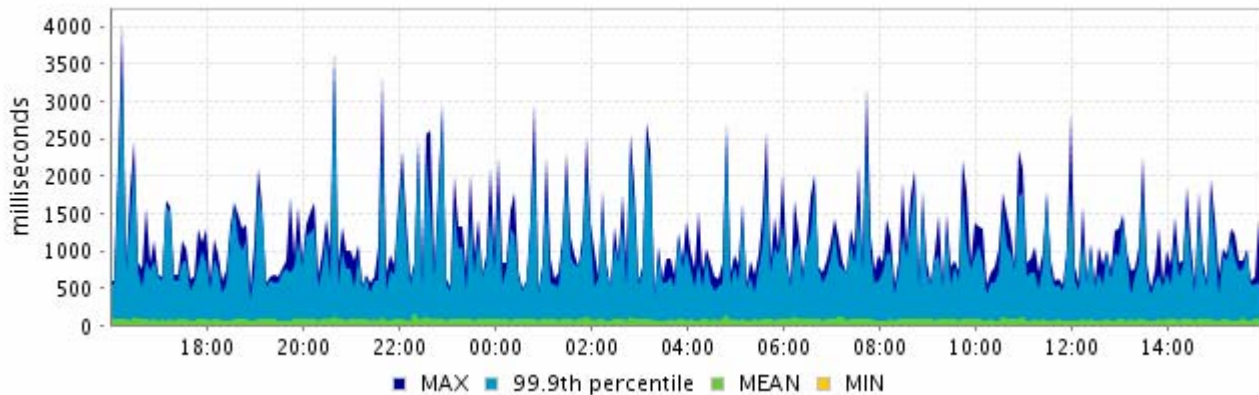
x% - displays the xth percentile of expected latency values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

Mean - displays the mean of the expected latency values for each five minutes during the chosen reporting period

Min - displays the minimum of the expected latency values for each five minutes during the chosen reporting period.

The expected queuing delay variation graph plots the per-packet delay variation calculated by the BQM using a simulation based on the chosen class traffic. The expected delay variation is displayed as a series of millisecond values for each five minutes during the reporting period. The expected delay variation 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.

Figure 4-26 Expected Queuing Delay Variation Graph



The graph legend indicates the colors used to display each:

Max - displays the maximum of the expected delay variation values (in milliseconds) calculated each five minutes during the chosen reporting period.

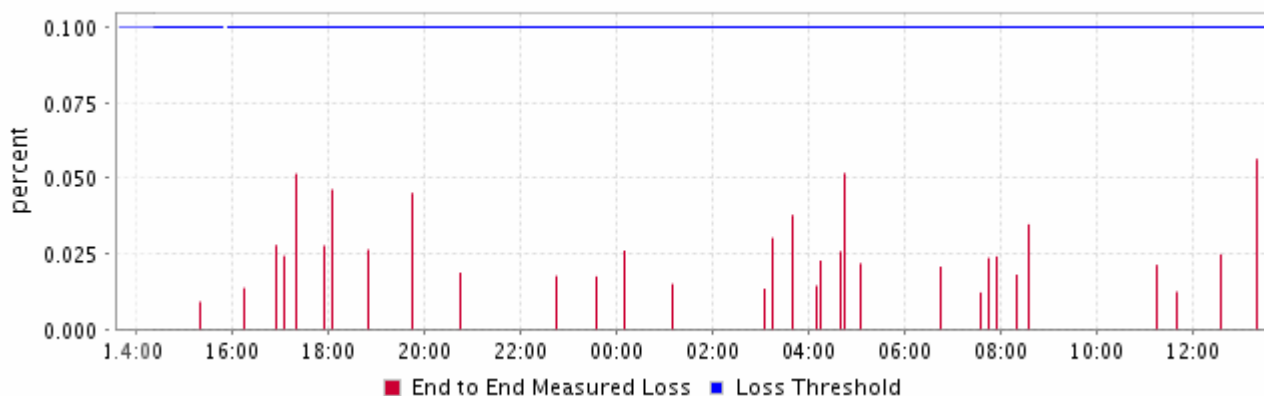
x% - displays the xth percentile of expected delay variation values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

Mean - displays the mean of the expected delay variation values for each five minutes during the chosen reporting period

Min - displays the minimum of the expected delay variation values for each five minutes during the chosen reporting period.

The expected queuing loss graph plots the expected packet loss due to queue buffer overflow calculated by the BQM using a simulation based on the chosen class traffic. The expected queuing loss is displayed as a percentage of the total packets measured by the BQM.

Figure 4-27 Expected Queuing Loss Graph



Loss estimation is enabled, and its characteristics defined, in the network service objective applied to the interface.

In each case, 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.

Viewing Priority Class Results

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.

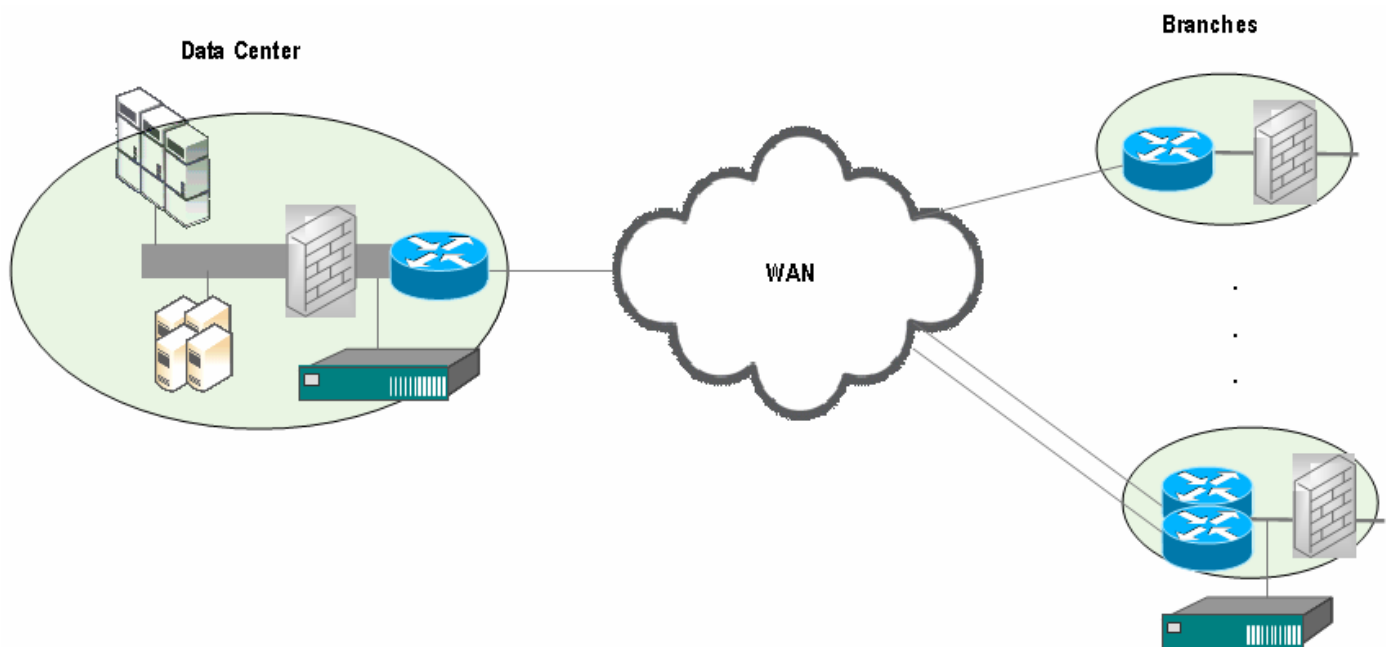
Priority drop estimation is enabled, and its characteristics defined, in the network service objective applied to the interface.

Identifying Network Service Quality Issues

The following example scenario describes how you can use BQM to identify network service quality issues in the network. In this example, we consider a 20 branch multi-class network with MPLS WAN connectivity and a single data centre:

- 19 of the branches have a single switch, router and interface
- One branch, for which user complaints are being received due to intermittent application performance issues, has one switch, two routers, and two subnet interfaces

Figure 4-28 Network Service Quality Example Scenario Deployment



The data center is instrumented with a BQM that models Expected Queuing and Corvil Bandwidth for all these branches. In this case there is some any-to-any traffic but traffic mostly dominates in the downstream direction from the data centre.



Note The branch experiencing issues is modeled in the data centre BQM as two separate sites, each with a single router and interface with subnets defined. The configuration is done this way to operate successfully with automatic PNQM configuration mode.

Expected Queuing and Corvil Bandwidth measurements to this site are indicating no issues with following caveats:

- due to the presence of any to any traffic there is some doubt about the usefulness of these measurements
- a shaper is being applied at the data centre for the traffic destined to the remote branch; this is not modeled accurately by Expected Queuing

A Cisco ADE running BQM is deployed as a PNQM responder in this branch. No remote Expected Queuing collection is required in this case, so automatic PNQM configuration mode is specified in the data center BQM configuration.

Figure 4-29 PNQM Configuration for Example Scenario

Passive Network Quality Management Settings

Remote BQM address:	192.168.5.60
PNQM Mode	<div> <input type="radio"/> manual (requires configuration of Remote BQM) <input checked="" type="radio"/> automatic (no retrieval of Remote EQ) </div> <div> Sample: <div> <input type="radio"/> Use class sample rate from NSO map (single class only) <input checked="" type="radio"/> All packets <input type="radio"/> One in <input type="text"/> packets </div> </div> <div> <input type="checkbox"/> ignoring rerouted/missing flows </div>
<div>Save Cancel</div>	

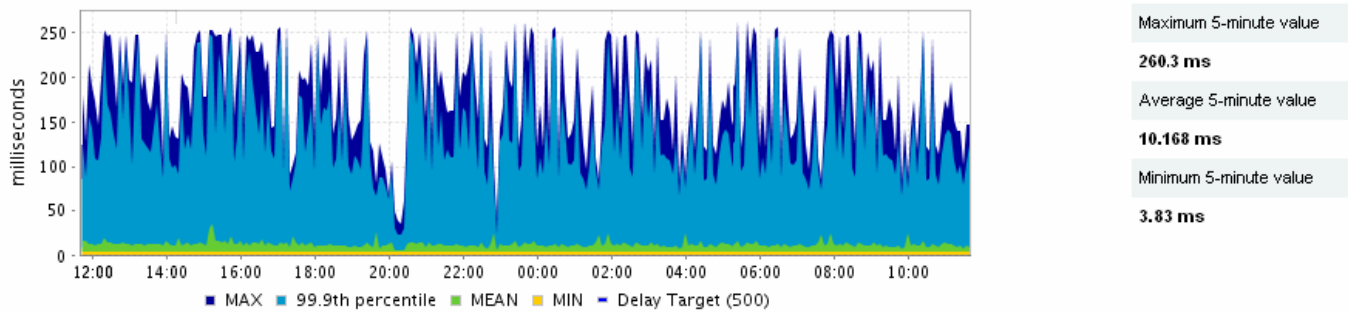
However, because this is a multi-class network, the per-class sampling configured in the network service objectives must be over-ridden with an interface sampling setting. This is configured to sample all packets on the interface.



Note For more information on network service objective configuration, see the section “Defining a Network Service Objective” in the chapter “Configuring Network Service Quality Monitoring.” For more information on PNQM configuration, see the section Configuring a PNQM Channel in the same chapter.

Some traffic from the branch is known to be routed through a separate data centre and will not be seen by the data centre BQM. These packets can be correctly reported as re-routed, as opposed to being counted as lost.

In this example scenario, PNQM results are available for both interfaces of the remote site and correlate quite highly with the Expected Queuing results for both interfaces. Therefore we conclude that the presence of any-to-any traffic is not significantly impacting both the Expected Queuing and Corvil Bandwidth results.

Figure 4-30 Example Scenario End-to-End Latency Results

During a period of users complaining about application performance issues, the following results are noted:

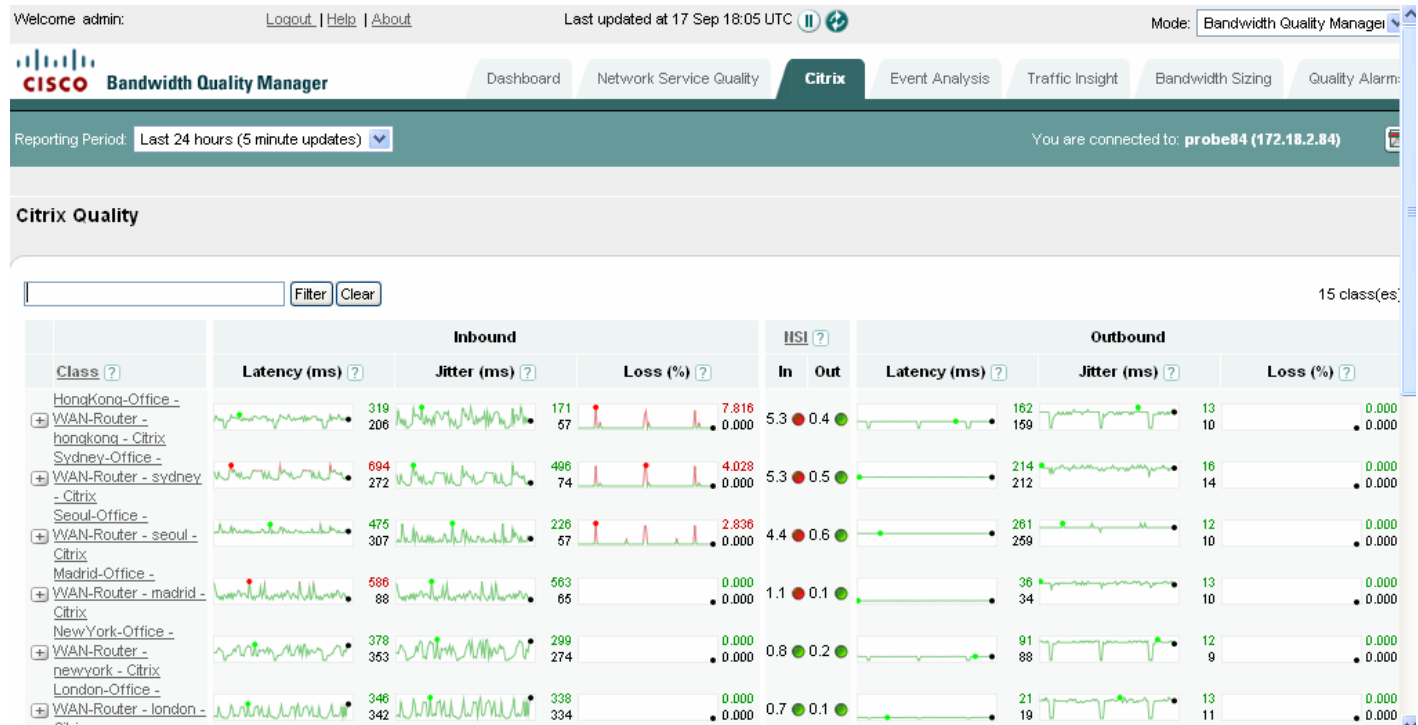
- no change in Expected Queuing and Corvil Bandwidth results
- PNQM reports excessive end-to-end measured latency for all traffic in both directions between the data center and branch site
- the reporting of re-routed traffic remains unchanged

Given these results, it is most likely that in this example scenario the problem is in the service provider network.

Monitoring Custom Dashboard Results

The purpose of the custom dashboard is to highlight the network service level being achieved by a user-defined set of classes.

Figure 4-31 Custom Dashboard Monitoring Page



The view is organized as a list of classes and their summary information sorted by Network Service Index value. Only remote sites are displayed on the custom dashboard. There is one entry for every monitored pre-queuing class whose class-map is selected in the list that you select when configuring the custom dashboard.

Each class is identified by a fully-qualified reference to the relevant site, router, interface and class name.

The summary information displayed is as follows:

- NSI: the summary Network Service Index number gives an indication of the long-term quality achieved in each direction.
- Inbound end-to-end latency, jitter and loss (to the remote site).
- Outbound end-to-end latency, jitter and loss (from the remote site).

The latency, jitter and loss statistics include a spark-line type chart of the historical performance. The upper numerical value displayed with the sparkline chart is the highest historical measured value during the chosen reporting period (red/green depending on whether targets are violated/achieved). The lower numerical value shows the most recent value (black).


Each class in the list can be expanded by clicking . The expanded view will show the selection of statistics selected by the user on the configuration screen.

Selecting a class opens the **Network Service Quality** tab results for that class.

You can choose from the predefined list of reporting periods up to 60 days over which to view data for individual classes. You can also sort the summary information by certain columns and you can drill into each class to view supporting graph details. Custom reporting period configuration is not available for the custom dashboard.

The custom dashboard summary table is sorted by the **NSI** column by default, but you can sort the table by the **Class** and **NSI** columns. Click the heading of the chosen column to sort. The information in the table is then arranged accordingly. You can click again to reverse the order of the sort. The **NSI** column shows inbound and outbound Network Service Index values, and sorts based on the larger of the two values.

You can use the search facility on the custom dashboard table to display a particular class or set of classes of interest. Enter the name of the required class or use a wildcard (*) to match a group of classes and click **Filter**. To clear the filter text field and return to the default display of results, click **Clear**.

In the same way as on the **Network Service Quality** tab, you can generate a report in .pdf format at any point when viewing results. To generate a report, click .

Viewing Custom Dashboard Results


By default, results for up to twenty classes are displayed per page and if there are more than twenty classes configured, you use the links to navigate between pages of results.

The following describes the information displayed in the custom dashboard summary table:


Table 4-5 Custom Dashboard

Field	Description
Class	Displays the full, qualified name identifying the class: site name - router name - interface name – class name. The site name, router name and interface name are those that have been configured in the BQM network model. Clicking the link opens the details for the chosen class in the Network Service Quality page.
Latency (ms)	Displays a sparkline chart of the one-way latency measurements for this class (PNQM or EQ) during the chosen reporting period.
Jitter	Displays a sparkline chart of the one-way latency variation measurements for this class (PNQM or EQ) during the chosen reporting period.
Loss (%)	Displays a sparkline chart of the packet loss for this class (PNQM or EQ) during the chosen reporting period.
NSI	Displays 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 latency experienced by the class

	<p>exceed the user-specified targets.</p> <p>If you have not enabled Network Service Index calculation in the network service objective being applied to an interface, the status is displayed as "Not Configured."</p> <p>If PNQM is not enabled, Network Service Index results are only available for local site outbound and remote site inbound interfaces.</p>
--	---

Each interface entry in the custom dashboard table can be expanded to display information for configured classes. Click  beside the interface name to expand an interface.

Viewing Class Results

Click  beside a class name in the custom dashboard to display graph results for the class.

Click a linked class name in the custom dashboard table to open the Network Service Quality tab page for the chosen class and display the associated graph results.

See the topic “Viewing Class Measurements” in the section “Monitoring Network Service Quality” for more information on the graph results.

You can switch to the traffic statistics and bandwidth sizing results for the interface by clicking the relevant link from **Related Links**.



5 Analyzing Network Events

This chapter describes how to use 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

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 BQM, a bar in the **Event Analysis** tab quality events timeline identifies the event. BQM performs calculations on the measured event data to support detailed analysis of the event. Initially, BQM uses default threshold values above which to trigger event detection, but you can configure the thresholds for detecting quality events in the network service objective 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, BQM generates an alarm if disk space is low due to the processing required. 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 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.

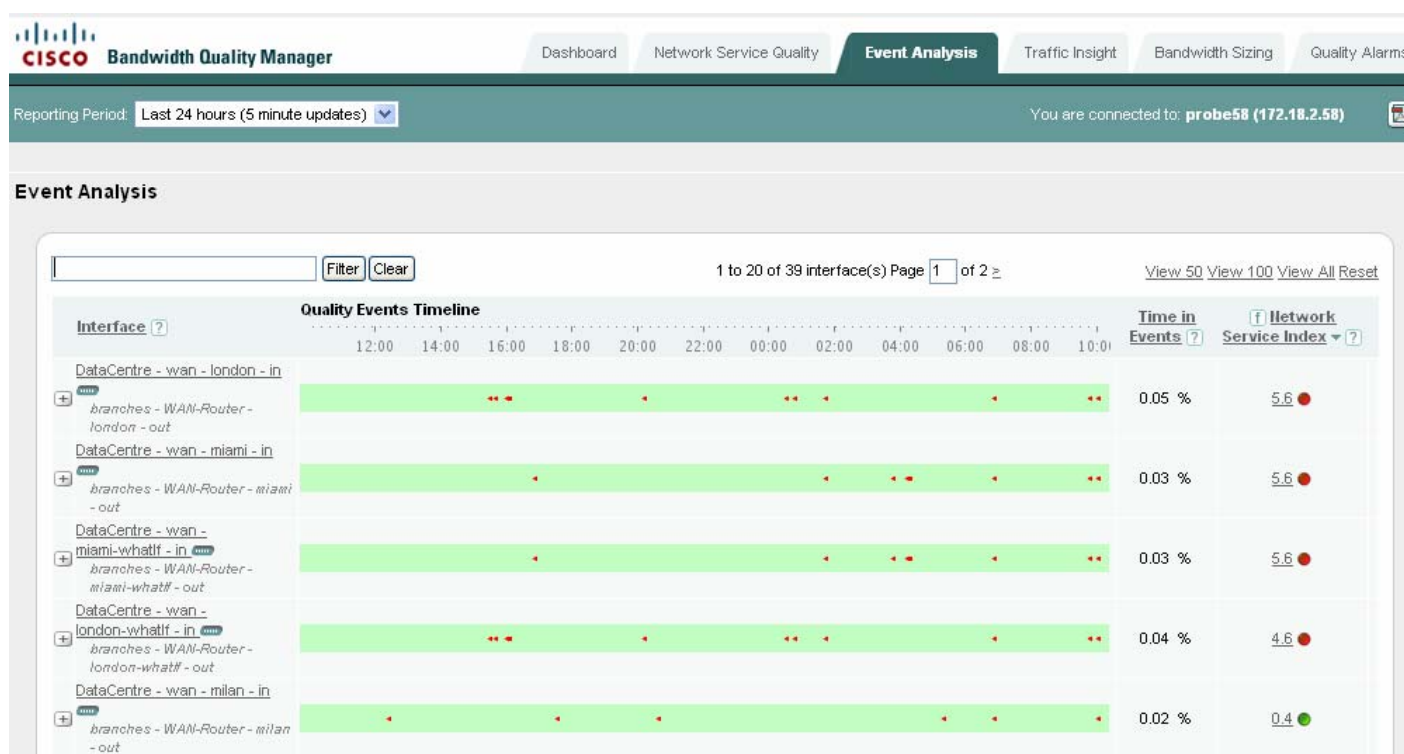
You can also define and start manual packet capture sessions. The packet capture file created in this case is also made available for event analysis.

By default the **Event Analysis** tab lists all of the interfaces you have configured in the BQM network model. The summary table information is sorted by Network Service Index 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 section “Troubleshooting an Event.”

Event 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 5-1 Event 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 event analysis summary table:

Table 5-1 Event Analysis Summary Table

Column	Description
Interface	<p>Displays the full, qualified name identifying the interface and the direction of the traffic (inbound or outbound) being measured by the interface: <i>site name – router name – interface name – direction</i>.</p> <p>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).</p>
Quality Events Timeline	<p>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 network service objective for the interface of interest, then no events will be displayed on the timeline.</p> <p>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).</p> <p>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 network service objective applied to the interface.</p>
Time in Events	<p>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.</p>
NSI	<p>Indicates network service quality degradation issues in the network. The Network Service Index (NSI) uses PNQM measurements and EQ, when configured, to detect events impacting end-to-end network quality based on the specified quality of service targets and sizing policy. Use the Network Service Objectives page in System Administration mode to set the quality targets and sizing policy that are used to calculate the Network Service Index.</p>

	<p>The Network Service Index 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 latency experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Network Service Index value seen on any class on that interface.</p> <p>A Network Service Index value greater than 1 means that loss or latency is above an acceptable level, as specified in the BQM configuration. This interface or class is not meeting its quality targets.</p> <p>A Network Service Index of less than or equal to 1 means the loss and/or latency 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.</p> <p>If you have not enabled Network Service Index calculation in the network service objective being applied to an interface, a dash (-) is displayed.'</p>
--	---



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 event analysis graphs for interfaces.

Each interface entry in the **Event 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.

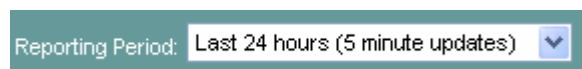


Note The results presented by BQM are based on the assumption that the device has not dropped packets. You can check this status on the **Quality Alarms** tab. If packets have been dropped then the presented results may not be an accurate reflection of the network traffic.

Selecting a Report Period

By default, the **Event Analysis** tab displays summary information for all configured interfaces for the last 24 hours.

Figure 5-4 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** field 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 Event Analysis Table


The **Event Analysis** table is sorted by the **NSI** 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 Network Service Index values, you click the **NSI** column heading to sort. The summary is rearranged according to the maximum Network Service Index values per interface, with the highest value first. Click the **NSI** column heading again to sort the summary screen again, this time with the lowest measured Network Service Index value first.

Filtering the Event Analysis Table

You can use the search facility on the **Event 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 **Event Analysis** tab also provides the option to filter results based on Network Service Index values. Click  beside the **NSI** 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 Event Analysis Results


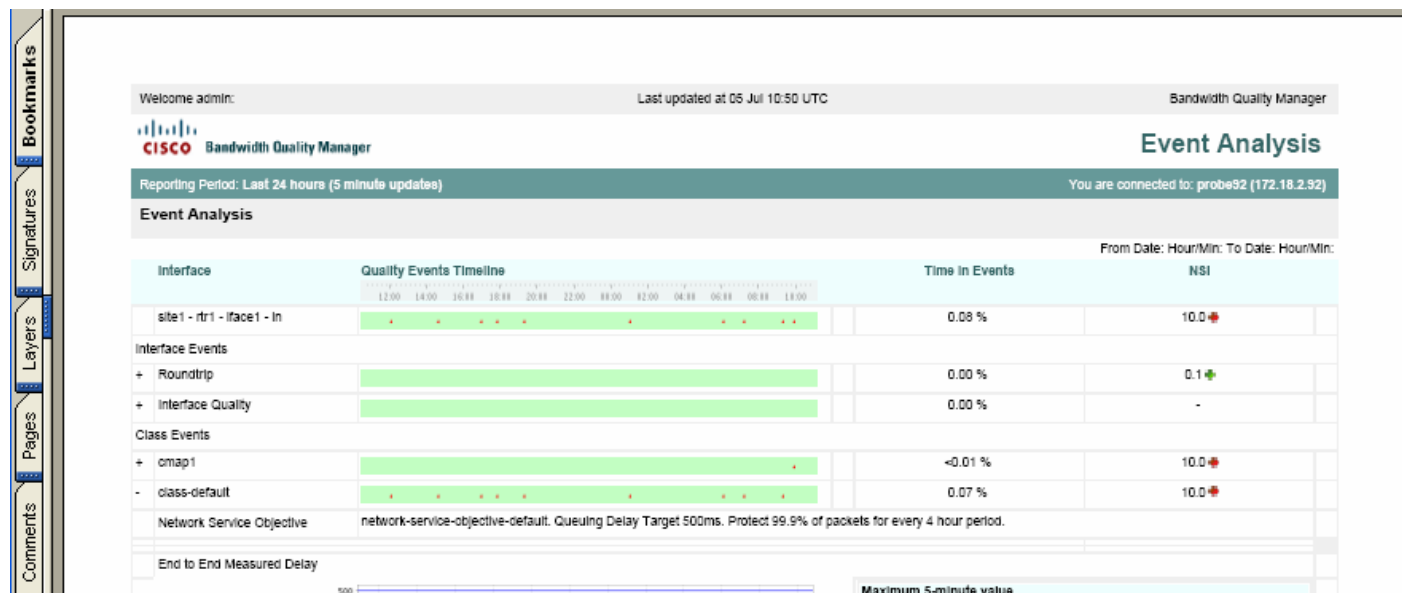
You can generate a report in .pdf format at any point when viewing event analysis results. To generate a report, click . The generated report is available for download in .pdf format. Reports are not stored on the appliance.

Figure 5-5 Event 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 Network Service Index 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 BQM time zone.

Viewing Interface and Class Events

Click the linked interface name in the **Event 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 outbound interface information.

You can switch to the traffic statistics and bandwidth sizing results for the interface by clicking the relevant link from **Related Links**.

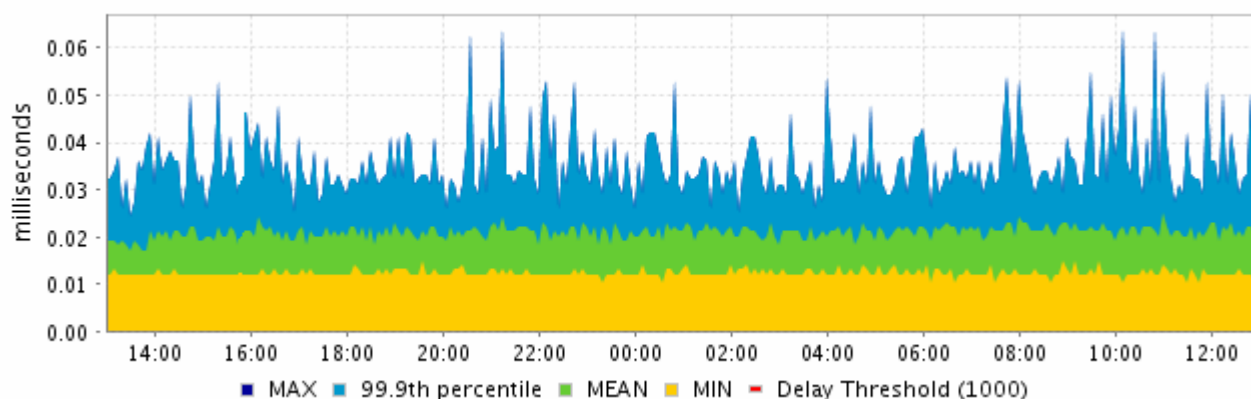
You can also define a custom reporting period for viewing interface results. See “Selecting a Report Period” for more information.

Viewing Round Trip Time and Loss

When you expand interface roundtrip events, the graphs available for site round trip events are as follows:

- ICMP roundtrip time
- ICMP roundtrip loss

The ICMP roundtrip time graph plots the round trip time between the chosen remote site and the local site for ICMP ping packets. The roundtrip time is displayed as a series of millisecond measurements for each packet sent on the round trip.

Figure 5-6 ICMP Roundtrip Time Results

The graph legend indicates the colors used to display the following:

Delay Threshold - indicates the value of the delay threshold configured in the network service objective being applied. The default value is two times the configured one-way latency figure.

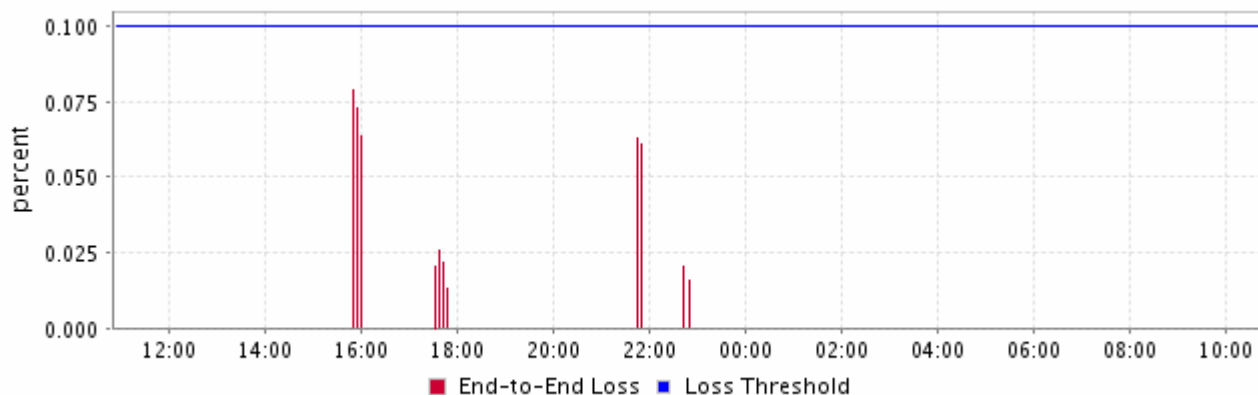
Max - displays the maximum round trip time (in milliseconds) per ICMP ping packet each five minutes during the chosen reporting period.

x% - displays the xth 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th 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 5-7 ICMP Roundtrip Loss Results

End-to-end latency and loss measurement is enabled, and its characteristics defined, in the network service objective 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 latency and loss plots enable you to evaluate end-to-end performance. This can complement the local queuing latency 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.



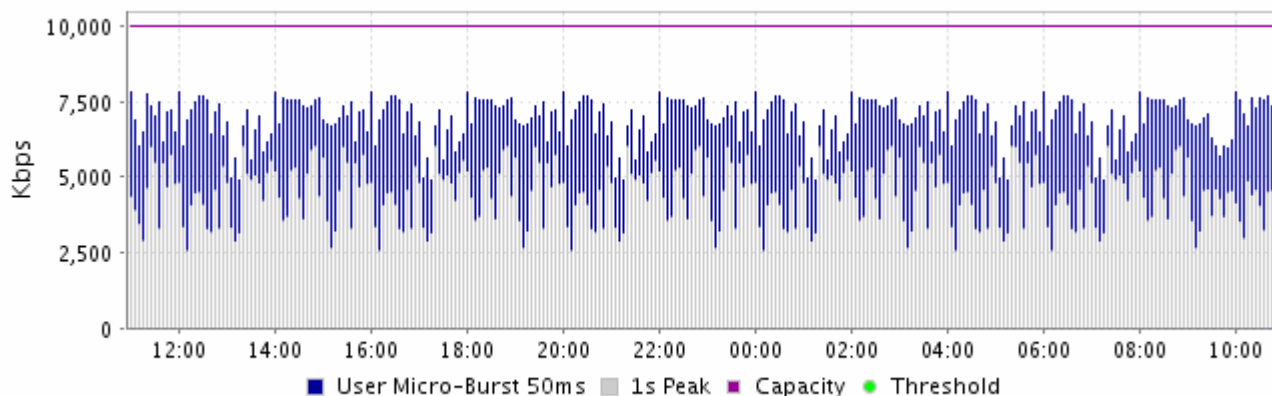
Note ICMP loss and delay events do not trigger packet captures, and so drill-down analysis is not available from the ICMP Quality Events Timeline. The reason for this behavior is that ICMP events are usually caused by external factors (such as unavailability of the remote device, or loss in the Service Provider network) that are not visible in local packet captures.

Viewing Interface Microburst and Network Service Index Measurements

When you expand interface quality events, the Microburst Detection and Network Service Index graphs are displayed.

The Microburst Detection graph displays measured peak bit rates at a configurable millisecond-level resolution. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps.

Figure 5-8 *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 network service objective for measuring microbursts (for example, 50 ms)

The threshold configured in the network service objective for triggering event detection on microbursts (for example, 1000 kbps 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 network service objective 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 network service objective values are used.



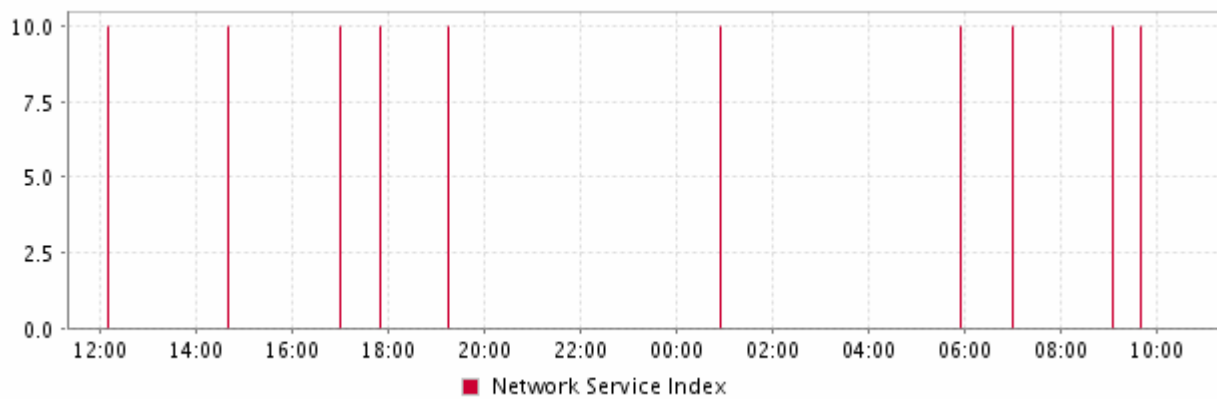
Note Under certain conditions it is possible to see higher peak values measured for larger millisecond resolutions than for smaller ones. For example, let's say you have configured a queuing delay target of 500ms and a microburst peak measurement resolution of 400ms. If traffic arrives in separate groups 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 Network Service Index graph displays the values calculated every five minutes during the selected reporting period.

Figure 5-9 Network Service Index



Note The summary Network Service Index value presented for the interface is based on the busy period configured in the network service objective 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 **Network Service Objectives** 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 Network Service Quality Monitoring Features” section of the “Configuring Network Service Quality 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:

- End-to-End Latency
- End-to-End Jitter
- End-to-End Loss
- Expected queuing latency
- Expected queuing loss
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length
- Network Service Index

If there is a doubt over measured data points due to packet drops, a red line is plotted on the graph at that point.

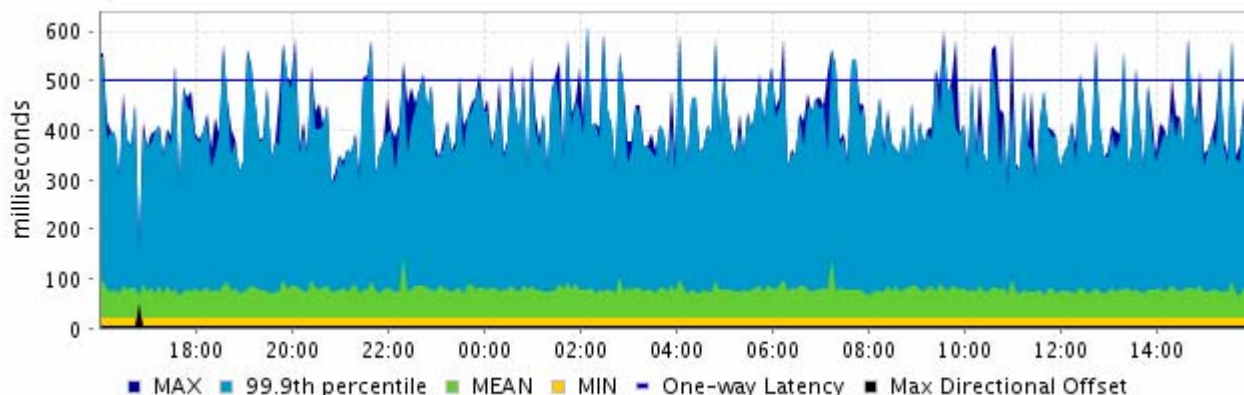
The end-to-end graph results are based on PNQM measurements. If PNQM is not enabled, then these graphs are not available. If PNQM is enabled, the **PNQM Availability** percentage indicates the percentage of time since the last configuration change that PNQM has been operating successfully.

If GPS clock synchronization is set up, configured and operating, a GPS availability figure is also displayed, indicating the percentage of time GPS was working successfully during the selected report period. A successfully operating GPS system reduces the maximum directional offset values plotted on the graphs.

End-to-End Latency

The End-to-End Latency graph plots the per-packet delay measured by the BQM for the chosen class traffic. The end-to-end latency is displayed as a series of millisecond values for each five minutes during the reporting period.

Figure 5-10 End-to-End Latency Results



The end-to-end latency calculation is made for every packet in the chosen class measured by 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 end-to-end latency values (in milliseconds) calculated each five minutes during the chosen reporting period.

x% - displays the xth percentile of end-to-end latency values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

Mean - displays the mean of the end-to-end latency values for each five minutes during the chosen reporting period

Min - displays the minimum of the end-to-end latency values for each five minutes during the chosen reporting period.

Max Directional Offset - displays the maximum uncertainty for each one-way latency measurement

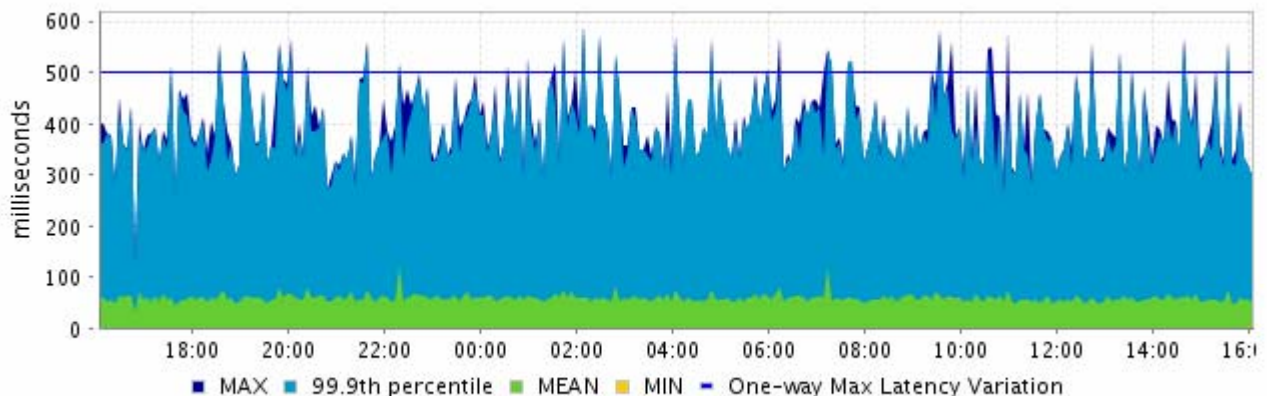
Configuration changes are indicated by a vertical line at the point where the change was made. The graph to the left of the line is shaded gray to indicate that it refers to an old configuration.



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 Jitter graph plots the difference between the latency (maximum, percentile, or mean) and the minimum latency, for the selected class during the time interval displayed. On a five-minute plot it represents the difference between the 5-minute latency (whether the maximum, percentile, or mean value) and the 5-minute minimum. The one-way latency variation target is configured in the network service objective that is applied to the class.

Figure 5-11 End-to-End Jitter Graph



The graph legend indicates the colors used to display each:

Max - displays the maximum of the end-to-end jitter values (in milliseconds) measured each five minutes during the chosen reporting period.

x% - displays the xth percentile of end-to-end jitter values in each five minutes during the chosen reporting period. This percentile is configurable as part of the packet protection target in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

Mean - displays the mean of the end-to-end jitter values for each five minutes during the chosen reporting period

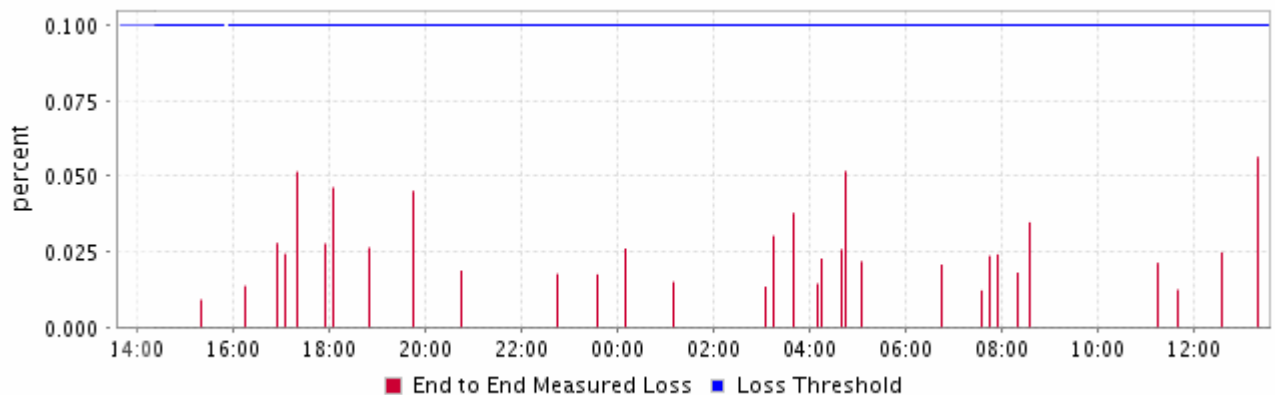
Min - displays the minimum of the measured end-to-end jitter values for each five minutes during the chosen reporting period.

One-way Max Latency Variation – indicates the configured one-way maximum latency variation target

End-to-End Loss

The End-to-End Loss graph plots the packet loss measured by BQM for the class traffic. The end-to-end loss is displayed as a percentage of the total packets measured by BQM.

Figure 5-12 End-to-End Loss Results



Loss measurement is enabled, and its characteristics defined, in the network service objective 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.

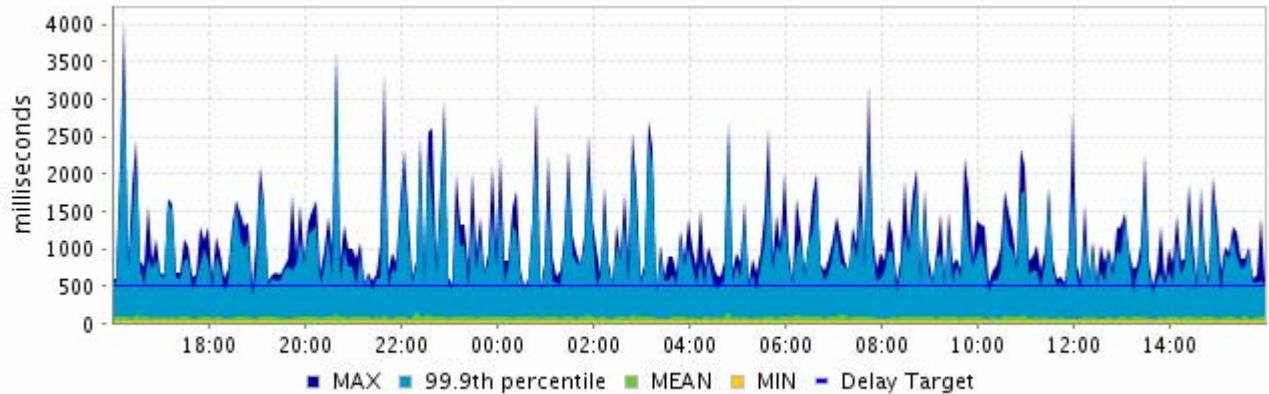


Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Expected Queuing Latency

The expected queuing latency graph plots the per-packet delay calculated by BQM using a simulation of the chosen class traffic. The expected queuing latency is displayed as a series of millisecond values for each five minutes during the reporting period.

Figure 5-13 Expected Queuing Latency Results



The expected queuing latency calculation is made for every packet in the chosen class measured by 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 latency values (in milliseconds) calculated each five minutes during the chosen reporting period.

x% - displays the xth percentile of expected latency values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

Mean – displays the mean of the expected latency values for each five minutes during the chosen reporting period

Min – displays the minimum of the expected latency 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.



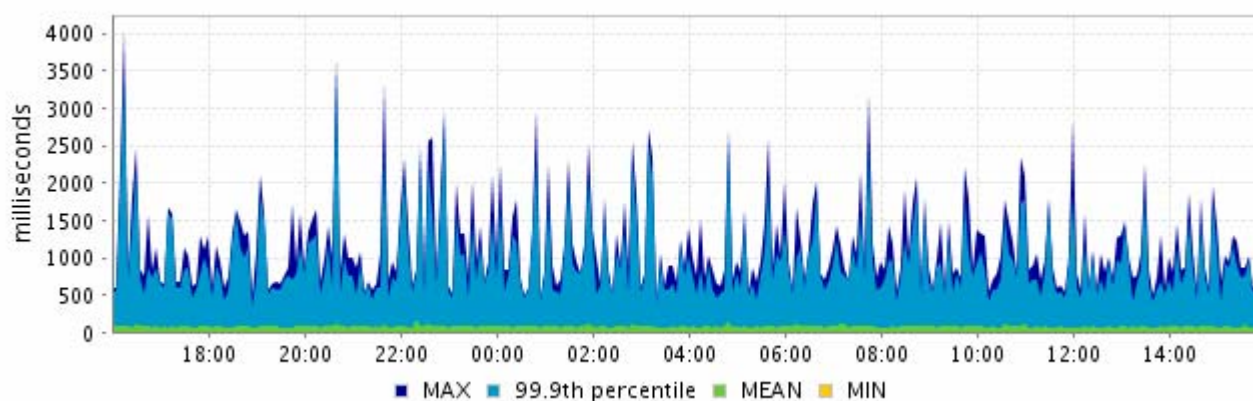
Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Expected Queuing Delay Variation

The expected queuing delay variation graph plots the per-packet delay variation calculated by the BQM using a simulation based on the chosen class traffic. The expected delay variation is displayed as a series of millisecond values for each five minutes during the reporting period. The expected delay variation graph plots the difference between the expected queuing latency (maximum, percentile, or mean) and the minimum expected queuing latency, for the selected class during the time interval displayed. On a five-minute plot it represents the difference between the 5-minute expected queuing latency (whether the maximum, percentile, or mean value) and the 5-minute minimum.

The expected queuing delay variation 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.

Figure 5-14 Expected Queuing Delay Variation Graph



The graph legend indicates the colors used to display each:

Max - displays the maximum of the expected queuing delay variation values (in milliseconds) calculated each five minutes during the chosen reporting period.

x% - displays the xth percentile of expected queuing delay variation values in each five minutes during the chosen reporting period. This percentile is configurable as part of the sizing policy in the network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th percentile.

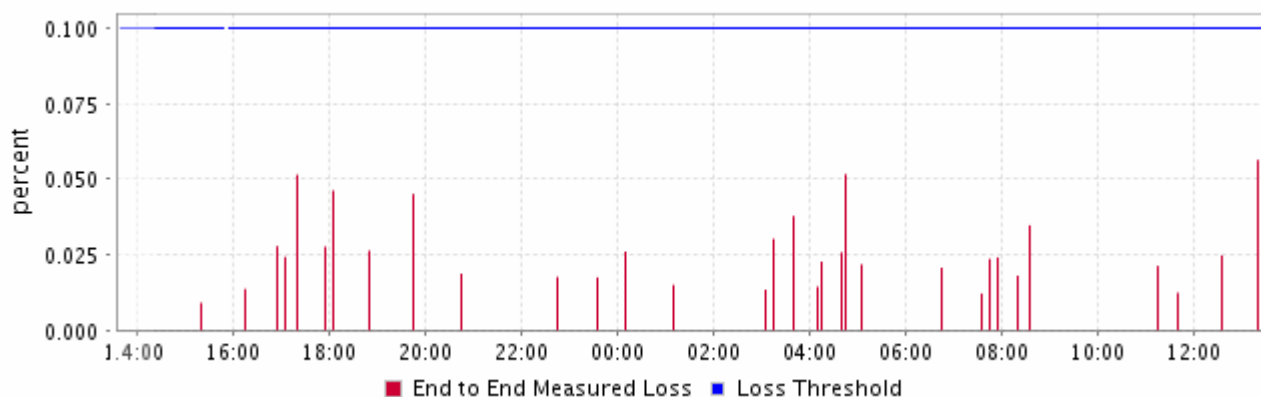
Mean - displays the mean of the expected queuing delay variation values for each five minutes during the chosen reporting period

Min - displays the minimum of the expected queuing delay variation values for each five minutes during the chosen reporting period.

Expected Queuing Loss

The expected queuing loss graph plots the expected packet loss due to queue buffer overflow calculated by BQM using a simulation of the chosen class traffic. The expected queuing loss is displayed as a percentage of the total packets measured by BQM.

Figure 5-15 Expected Queuing Loss Results



Loss estimation is enabled, and its characteristics defined, in the network service objective 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.

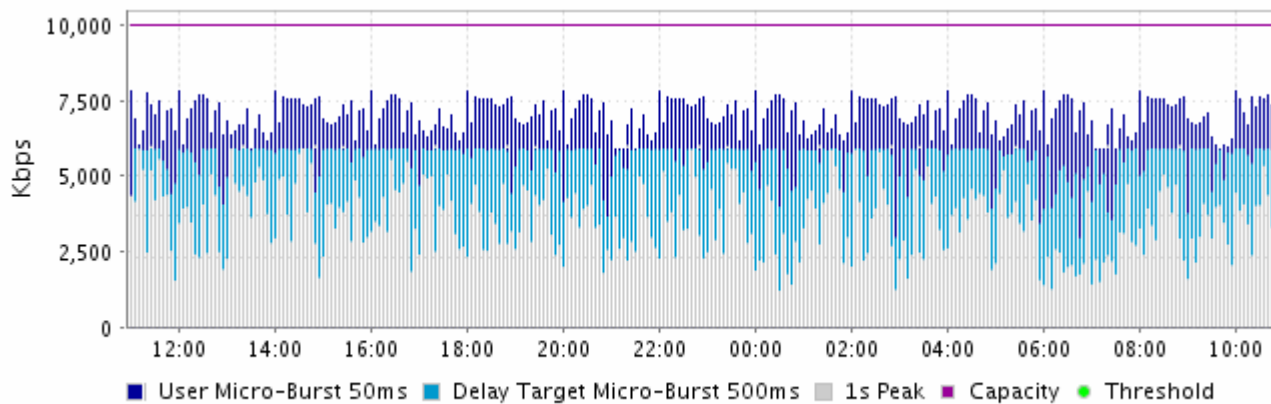


Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Microburst Detection

The Microburst Detection graph displays measured peak bit rates for the class traffic at a configurable millisecond-level resolution. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps.

Figure 5-16 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 network service objective queuing targets for delay (for example, 500 ms)
- the timescale resolution configured in the network service objective for measuring microbursts (for example, 50 ms)

The threshold configured in the network service objective for triggering event detection on microbursts (for example, 1000 kbps 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 network service objective 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 network service objective 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 **Network Service Objectives** 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 Network Service Quality Monitoring Features” section of the “Configuring Network Service Quality 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.

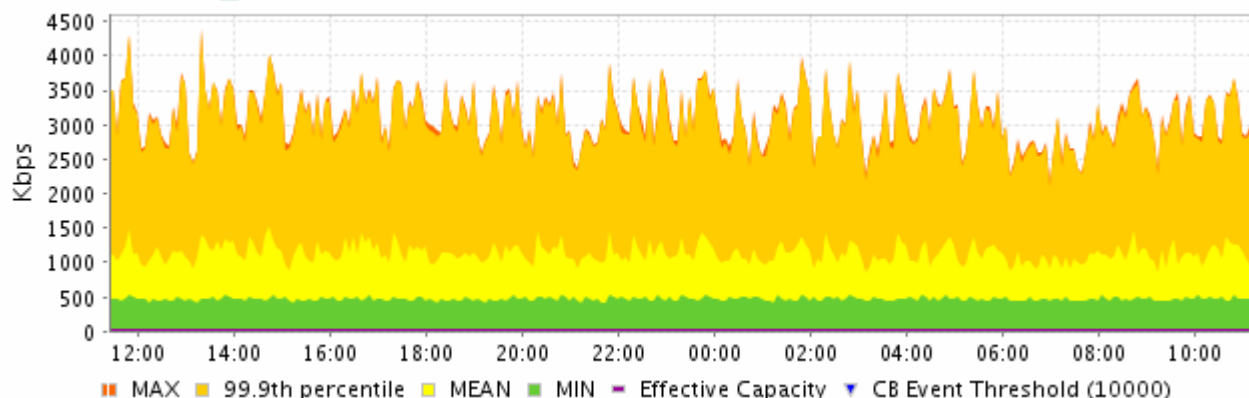
If the class traffic is perfectly smooth (that is, it is transmitting at a constant bit rate) then all three measurements listed above will be the same. The more bursty the traffic, the more variation there will be between these measurements. This can help you understand why an application that looks like it has very low bandwidth requirements on average may actually be causing drops in the network when it transmits very sharp short spikes.

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 network service objective 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 5-17 Corvil Bandwidth Delay Results

Corvil Bandwidth - Delay ?



The Corvil Bandwidth values are displayed as a series of values for each five minutes during the reporting period. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps.

The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values calculated each five minutes during the chosen reporting period.

x% - 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th 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 network service objective 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 **Network Service Objectives** 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 Network Service Quality Monitoring Features” section of the “Configuring Network Service Quality 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.



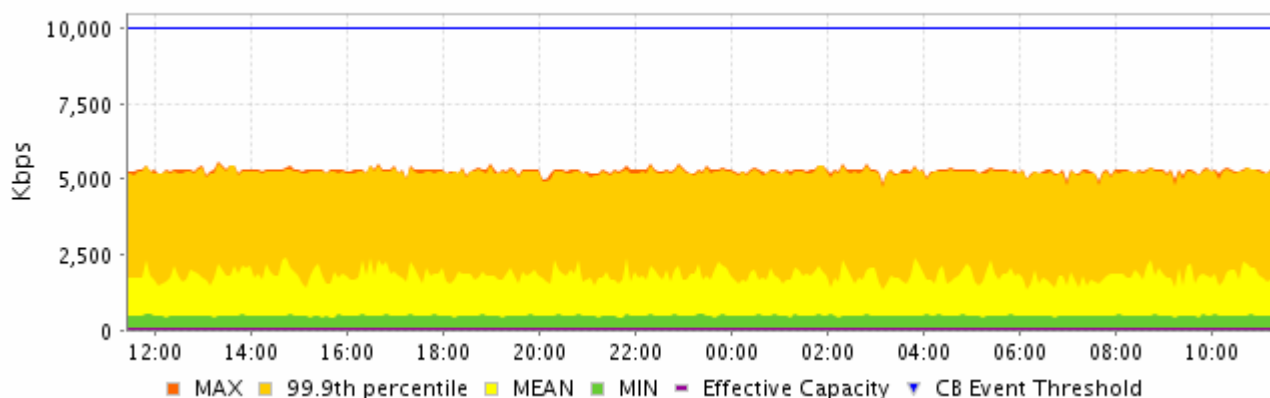
Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

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 5-18 Corvil Bandwidth Queue Length Results

Corvil Bandwidth - Queue Length ?



The graph displays a series of Corvil Bandwidth values for each five minutes during the chosen reporting period. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values calculated each five minutes during the chosen reporting period.

x% - 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th 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 network service objective 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 **Network Service Objectives** 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 Network Service Quality Monitoring Features” section of the “Configuring Network Service Quality 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.

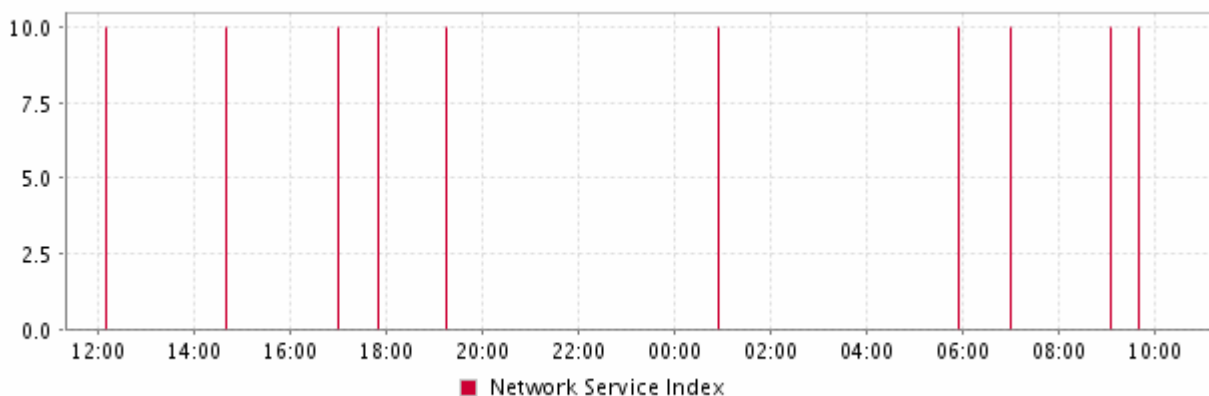


Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

Network Service Index

The Network Service Index graph plots the 5-minute values calculated by BQM for chosen class traffic during the selected reporting period.

Figure 5-20 Network Service Index Results





Note The summary Network Service Index value presented for the class is based on the busy period configured in the network service objective 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 network service objective 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 Event Analysis calculations you now see. Otherwise the default network service objective values are used.

Use the **Network Service Objectives** 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 Network Service Quality Monitoring Features” section of the “Configuring Network Service Quality 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.

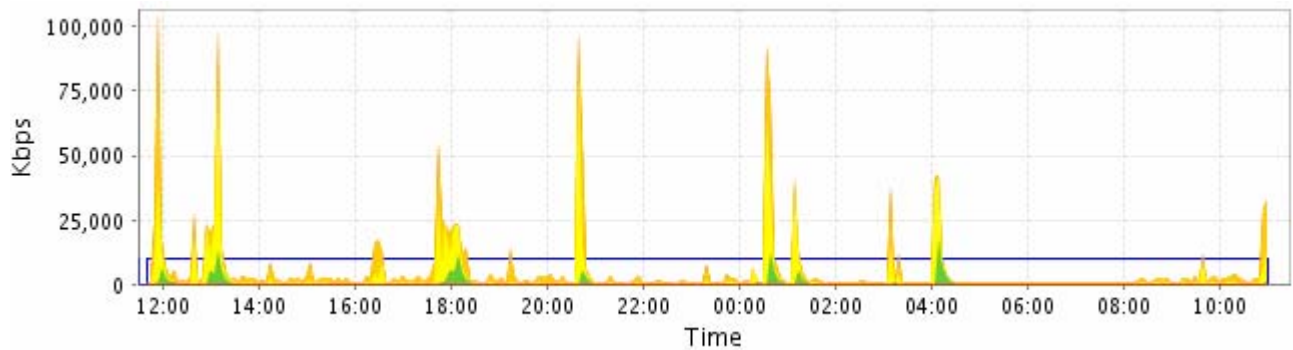
Viewing Priority Class Results

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 5-21 Corvil Bandwidth Priority Results

The graph is displayed as a series of kbps values for each five minutes during the reporting period. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps. For each five-minute period, the maximum, configured percentile, mean and minimum values are plotted:

Max - the maximum of the Corvil Bandwidth values 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th 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 network service objective for triggering event detection based on the Corvil Bandwidth value is indicated on the graph, as is the capacity of the link.

Use the **Network Service Objectives 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 Network Service Quality 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.

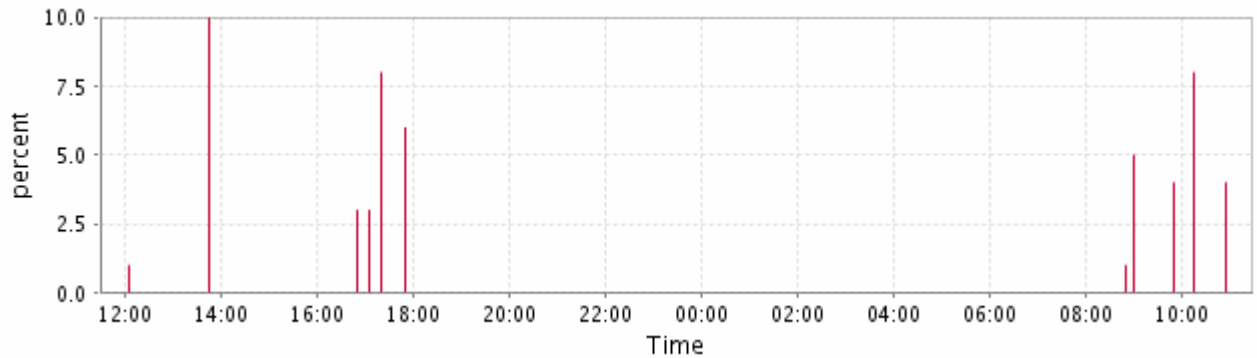


Note The displayed maximum, minimum and mean values are calculated over the entire selected reporting period. Each value includes data measured before any configuration changes during this period.

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 BQM using a simulation based on the chosen class traffic.

Figure 5-22 *Expected Priority Drop Results*

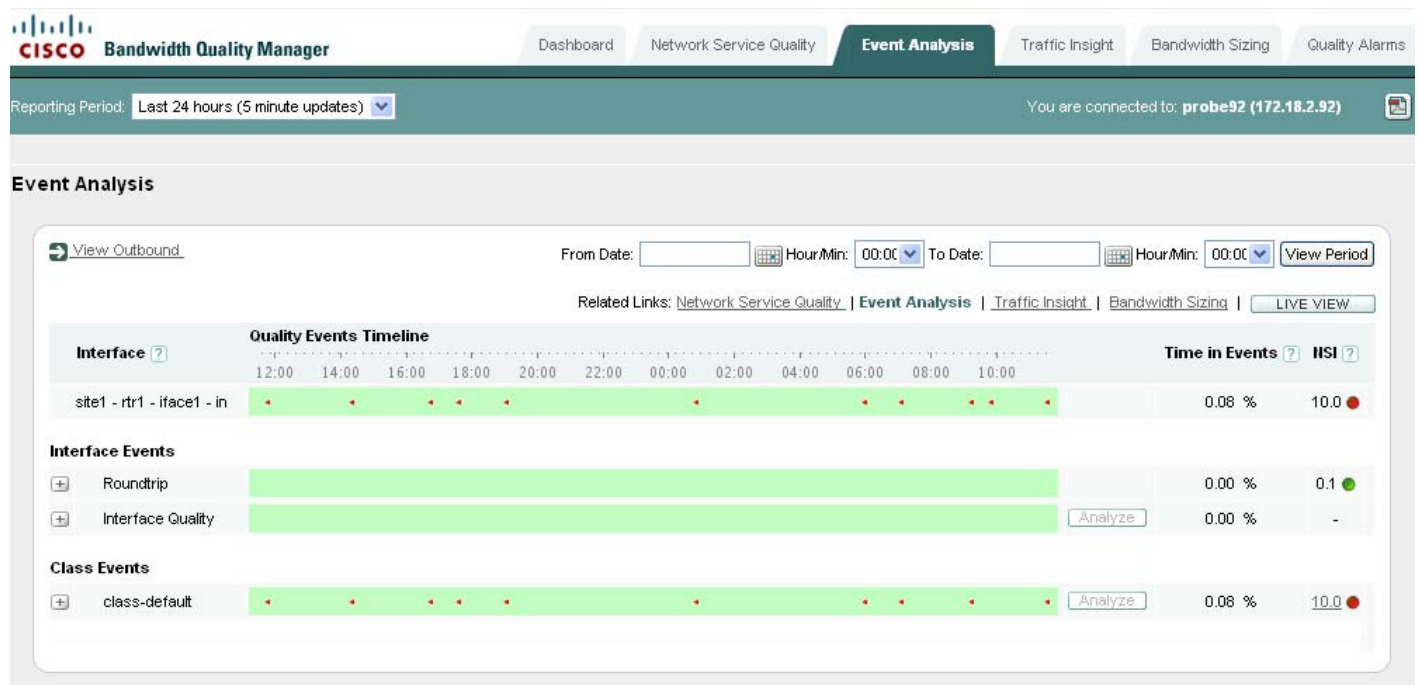


Priority drop estimation is enabled, and its characteristics defined, in the network service objective applied to the interface.

Investigating Network Events

When you open the **Event Analysis** tab, the complete list of interfaces configured on 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 5-23 Event Analysis



Choosing to analyze a particular interface or class launches the Event Analysis Inspection window. This window displays the Quality Events Timeline for the selected reporting period. The set of graphs displayed in the event inspection window for event analysis are as follows:

- End-to-End Latency
- End-to-End Jitter
- End-to-End Loss
- Expected Queuing Latency
- Expected Queue Length
- Expected Loss
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length

The charts for identifying event traffic leaders are as follows:

- Top applications
- Top talkers
- Top listeners
- Top conversations

The charts providing event traffic insight are as follows:

- Micro Burst Detection graph
- Average bit rate and byte counts
- Average packet rate and packet counts
- Active flows
- Packet Size Distributions

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.

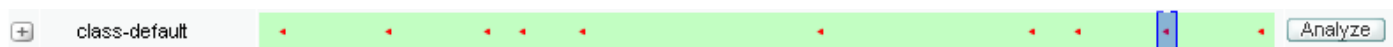
Click **select** beside the **To Date** fields and choose the event date from the calendar.

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.

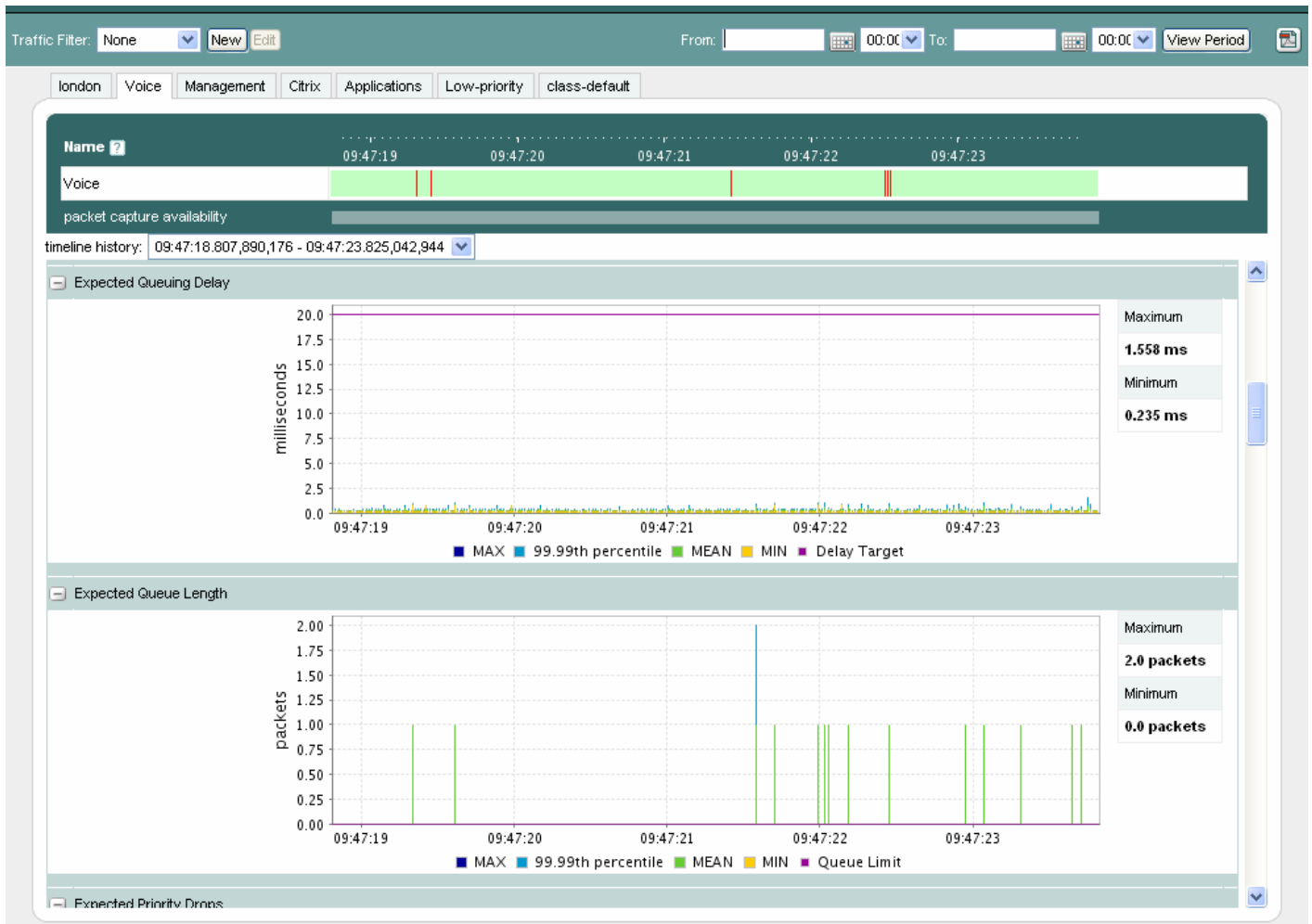
Figure 5-24 *Selecting an Event for Analysis*



- 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 is 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 5-25 *Event Analysis Inspection Window*

Note It is possible to see an event displayed on the quality events timeline in the Event 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 Event 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

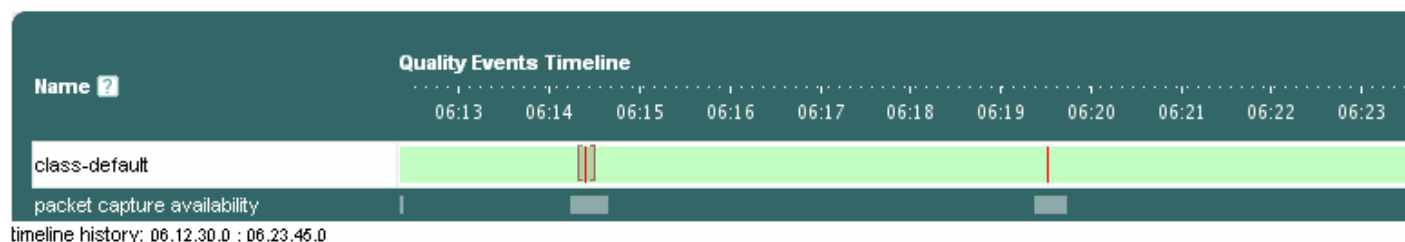
Check the displayed timeline again. You can define another time period as described above to focus on a particular event. You can also use the zoom feature on the Quality Events Timeline

or any of the displayed graphs to investigate the details behind the event you are troubleshooting.

Step 7

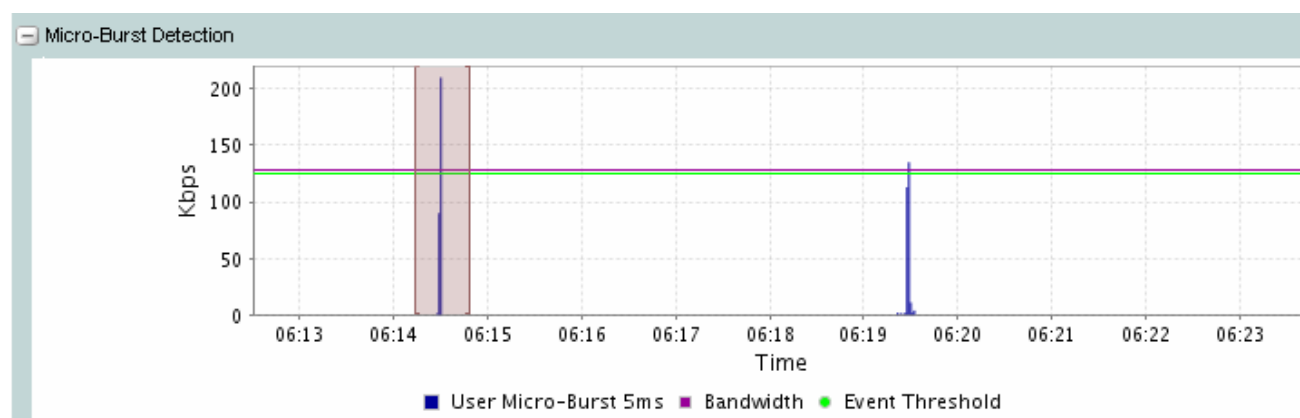
To zoom in on the Quality Events Timeline or on a chosen graph, click and drag the mouse across a selected portion of the timeline.

Figure 5-26 *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 5-27 *Zooming in on a Graph*

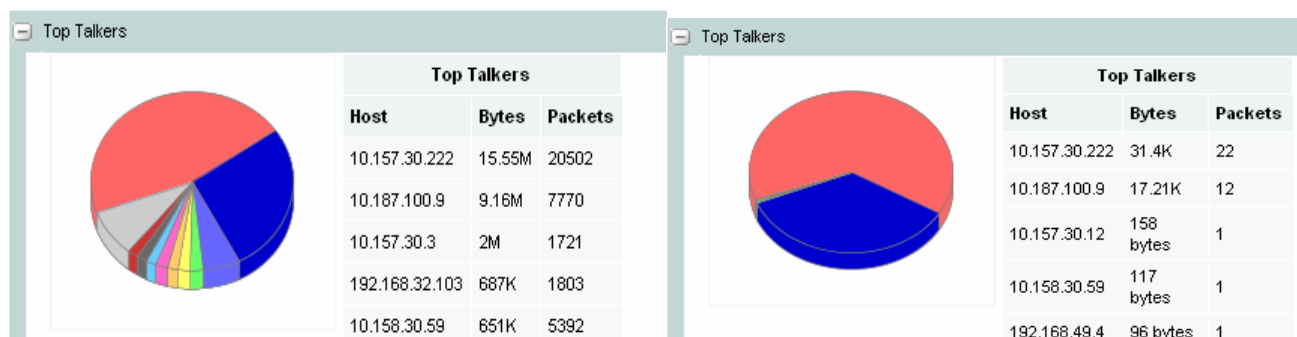


So you can click and drag across that five-minute period on the Microburst Detection graph to zoom in to the five-minute graph.

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.

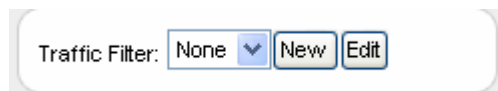
Figure 5-28 Top Talkers Before and After Zooming

You can use the **timeline history** list provided to jump back to different ‘zoom’ levels.

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 5-29 Event Analysis Traffic Filter

To define an traffic filter for event inspection, you do the following:

Step 1 Click **New**.

Figure 5-30 Defining an Event Analysis Traffic Filter

Action	Match	Application	Protocol	Source IP	Src Port	Destination IP	Dst Port	TOS
show	if is	Any	Any	any		any		Select TOS Value
hide		All other traffic.						

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 Analysis Results

The detailed analysis for each event includes graphs of the following:

- End-to-End Latency
- End-to-End Jitter
- End-to-End Loss
- Expected Queuing Latency
- Expected Queue Length
- Expected Queuing Loss
- Corvil Bandwidth – Delay
- Corvil Bandwidth – Queue Length

See the section “Viewing Class Measurements” for more information on the details displayed in each graph.

In all cases, you can click and drag on a point of interest on a given graph to zoom in to the next level of detail.

Identifying Event Traffic Leaders

The charts identifying traffic congestion leaders for the event are as follows:

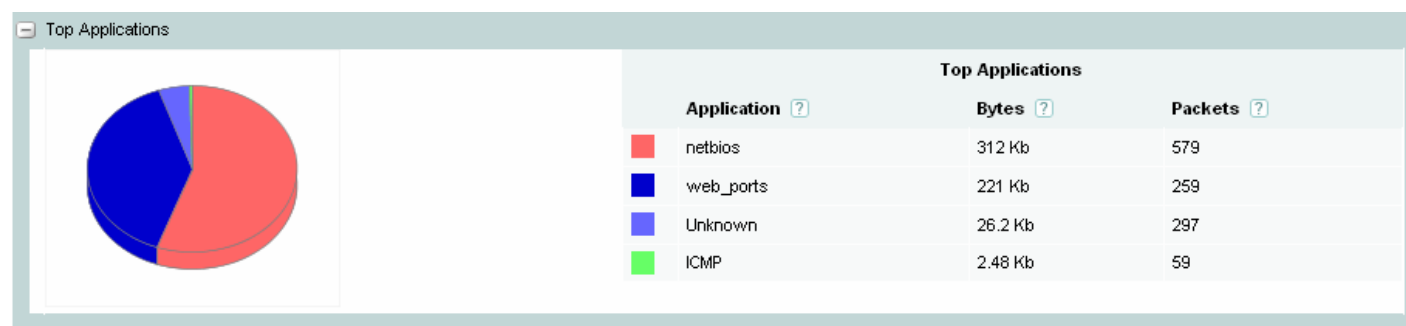
- Top applications
- Top talkers
- Top listeners
- Top conversations

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 5-31 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.

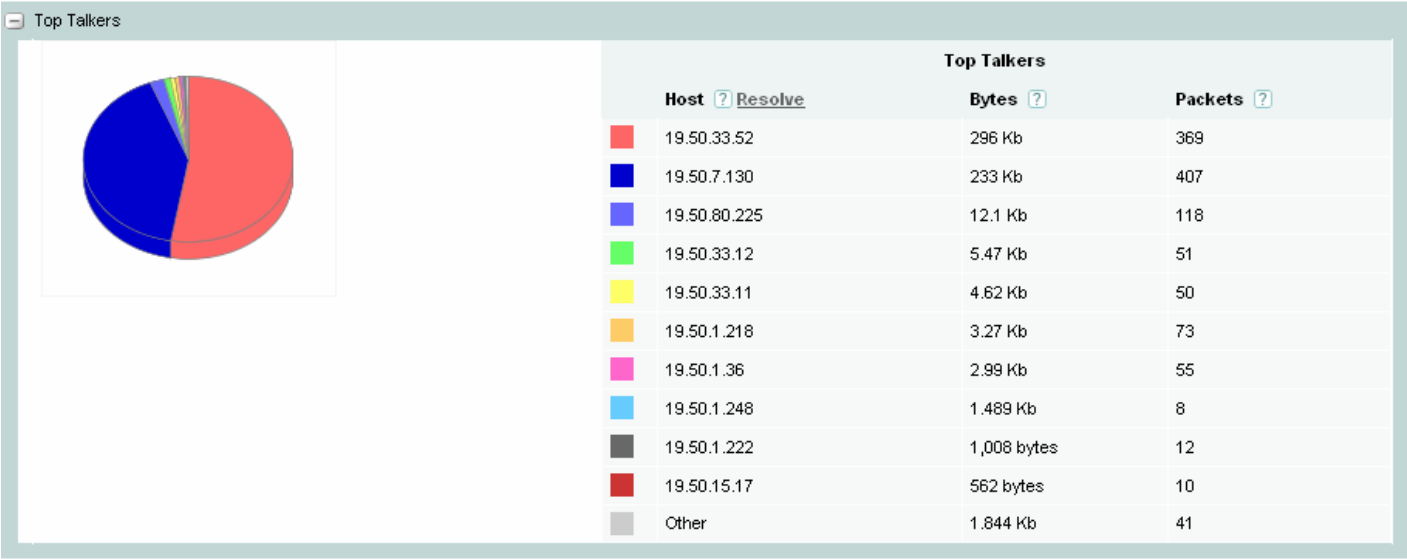
The **Packets** column displays the total number of packets for the application during the selected timescale.

The colors match each colored segment of the chart to a listed application.

Viewing Top Talkers

You can view pie charts illustrating the top talkers during the selected timescale.

Figure 5-32 *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.

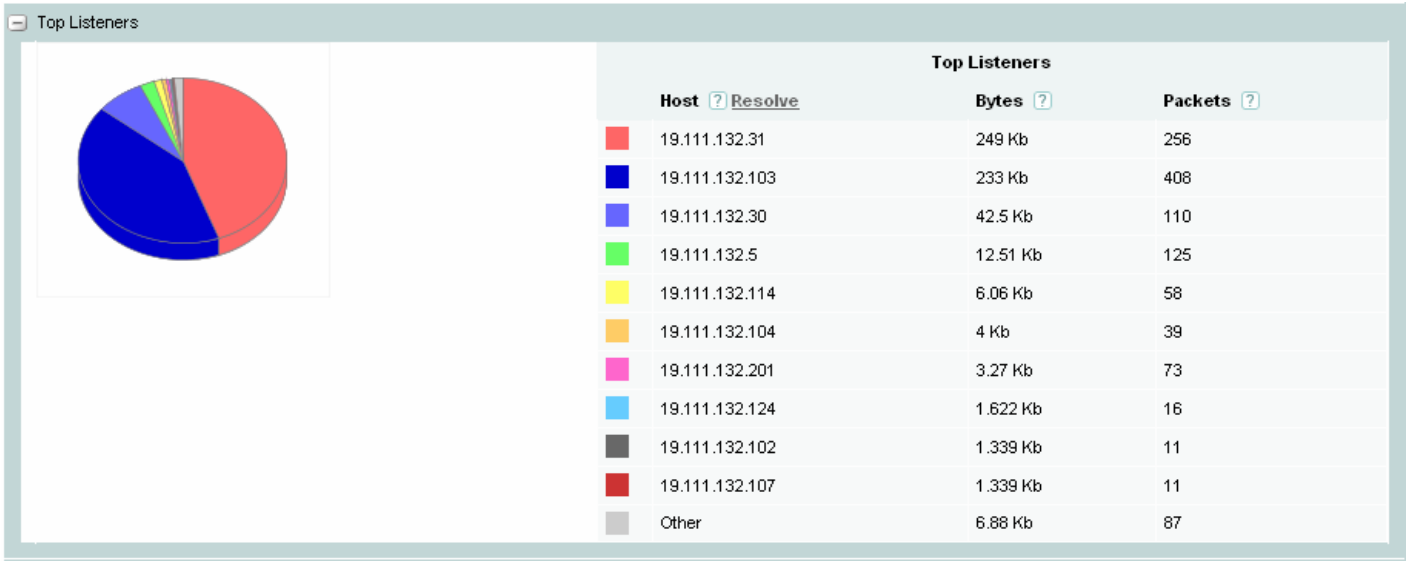
The **Packets** column displays the total number of packets transmitted by each host during the selected timescale.

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 5-33 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 5-34 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.

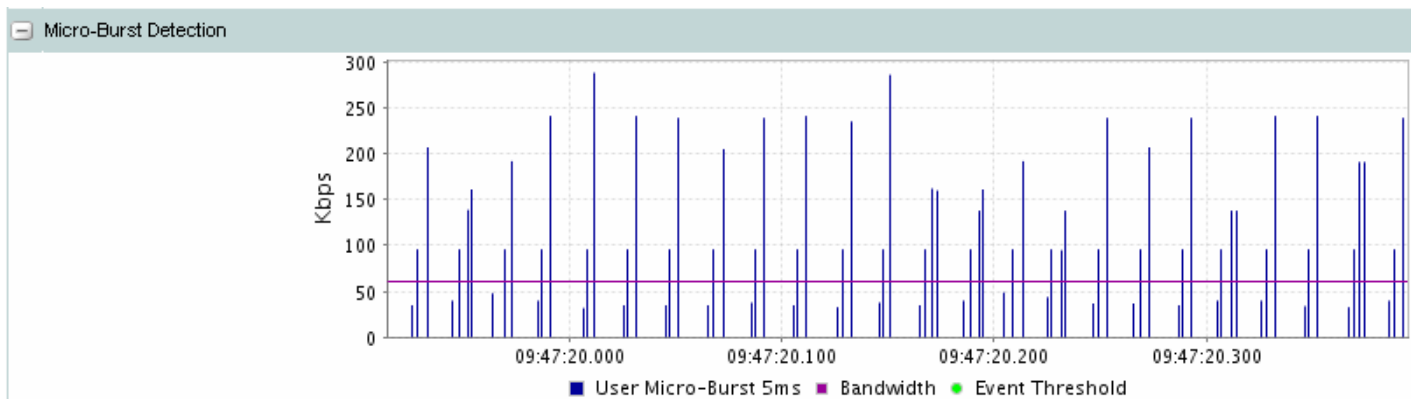
The colors match each colored segment of the chart to a listed conversation.

Identifying 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 network service objective for measuring microbursts (for example, 50 ms)
- the threshold configured in the network service objective for triggering event detection on microbursts (for example, 1000 kpbs on a 1024 kpbs link)

Figure 5-35 Event Microburst Graph



The legend below the graph identifies the color of each plotted line.

Identifying Event Traffic Patterns

The basic traffic statistic graphs displayed for the event are as follows:

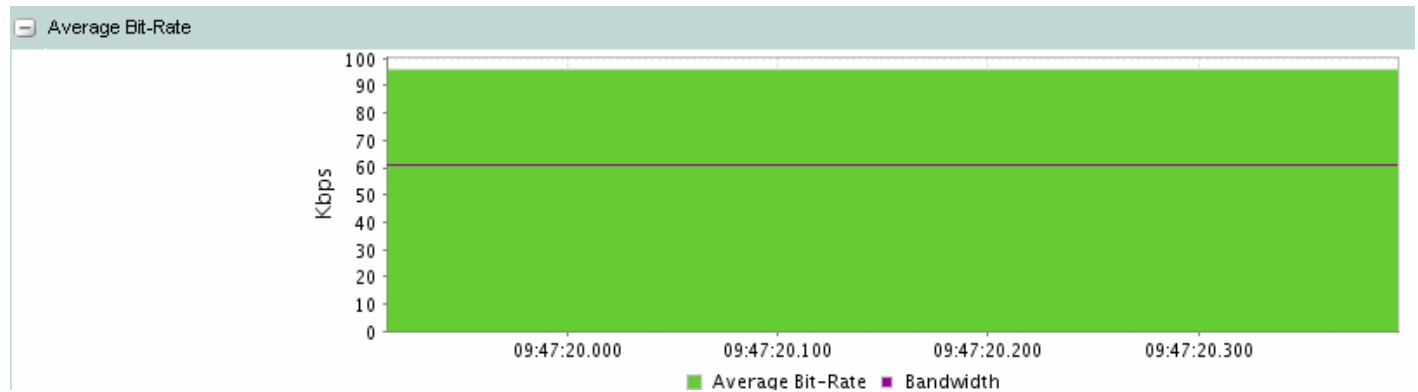
- Average Bit Rate
- Byte-counts
- Packet Rate
- Packet-counts
- Active flows
- Packet size distributions

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

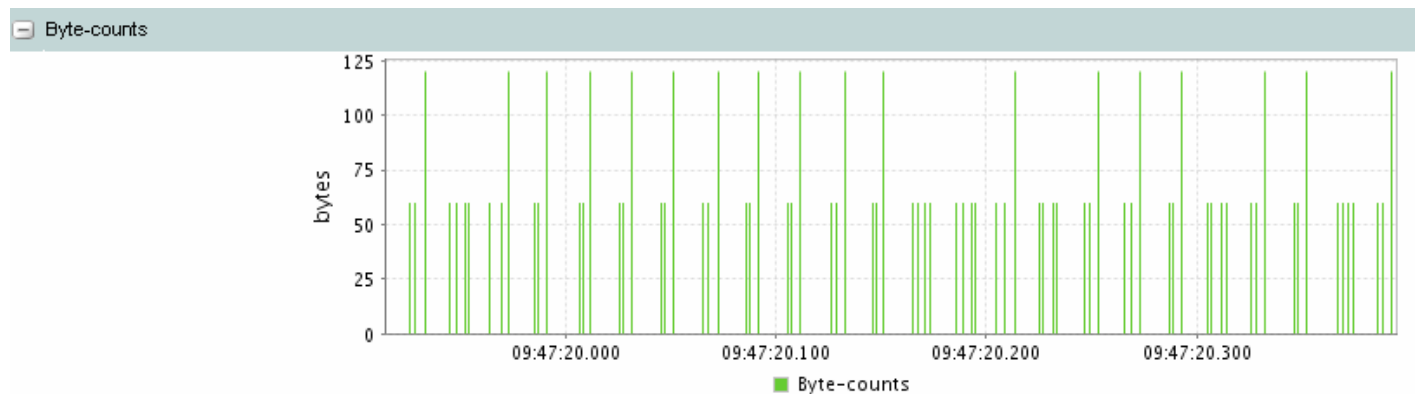
The Average Bit Rate graph plots the average number of bits measured for the traffic during the selected reporting period.

Figure 5-36 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 5-37 Event Byte-counts Graph

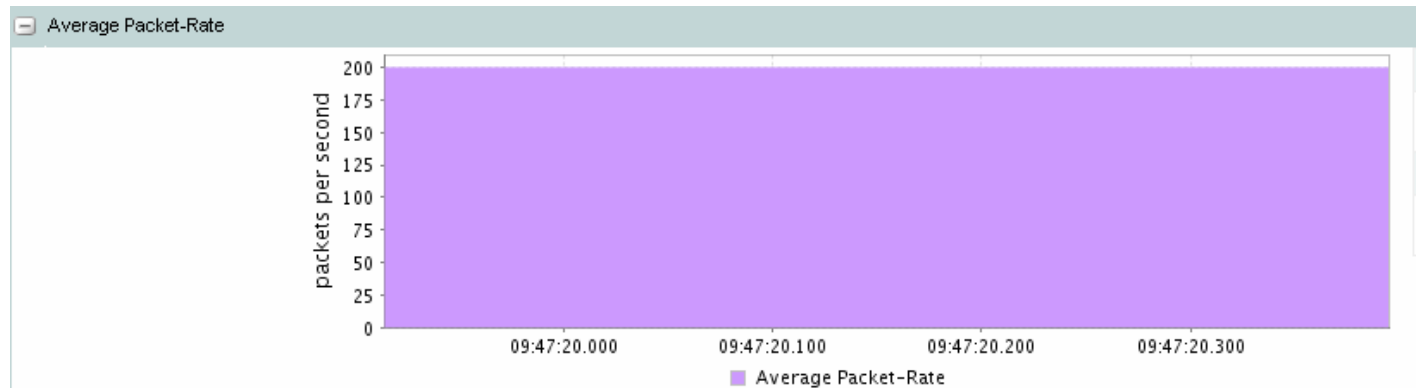


The Byte-counts graph plots the number of bytes measured for the traffic during the selected time interval.

Average Packet Rate and Packet-counts Graphs

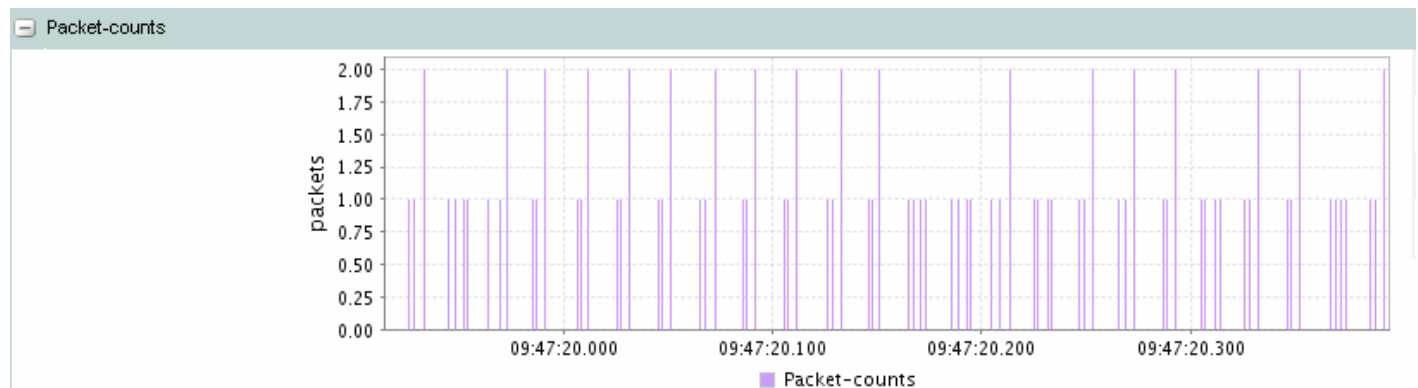
The Average Packet Rate graph plots the average number of packets measured for the traffic during the selected reporting period.

Figure 5-38 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 5-39 Event Packet-counts Graph

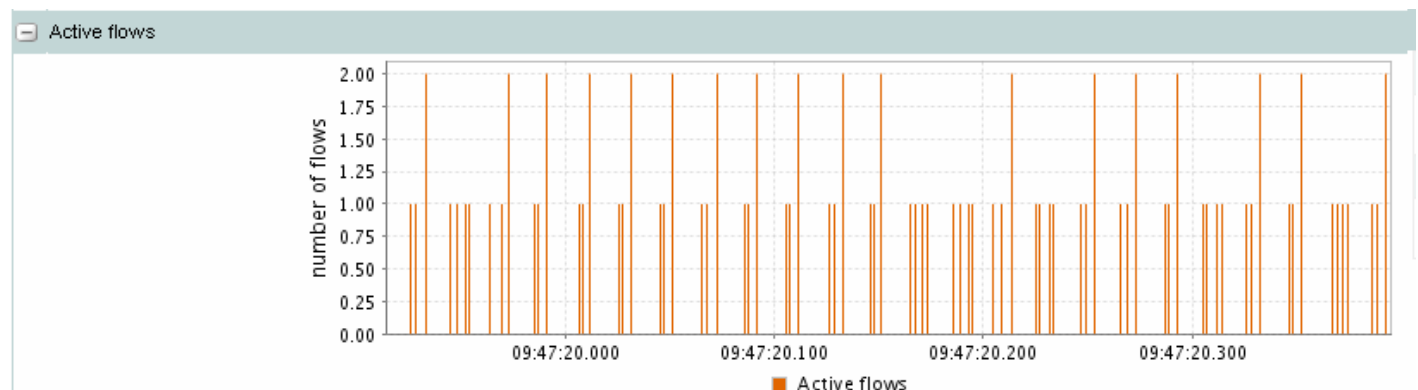


The Packet-counts graph plots the number of packets measured for the traffic during the selected time interval.

Active Flows Graph

The Active Flows graph plots the number of active flows during the selected time interval.

Figure 5-40 Event Active Flows Graph

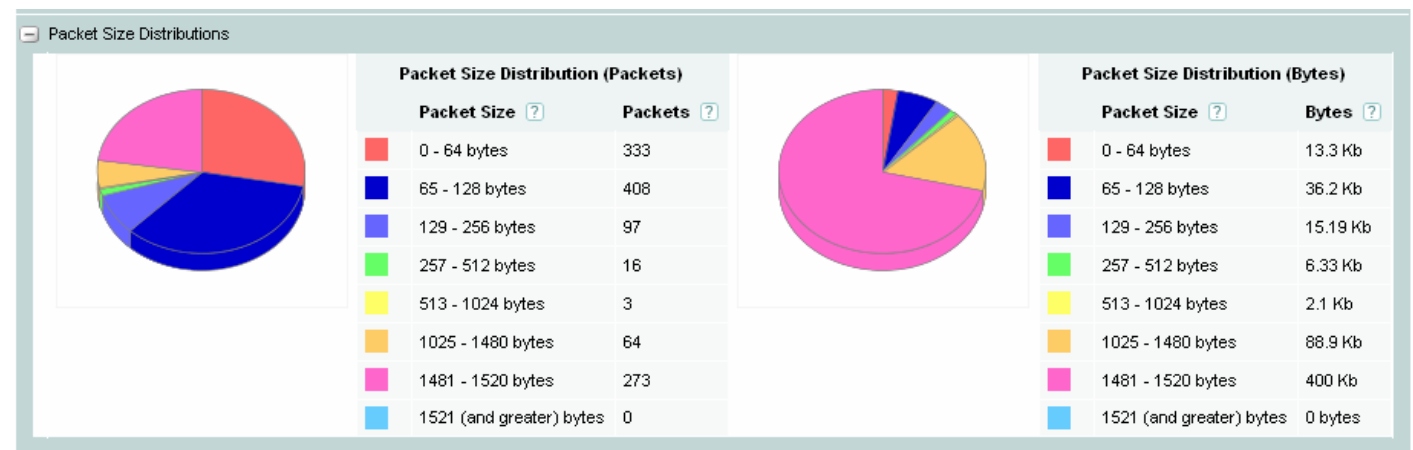


There may be other flows open, but at the selected timescale, you see only the number of flows that are actively transmitting data.

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 5-41 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.

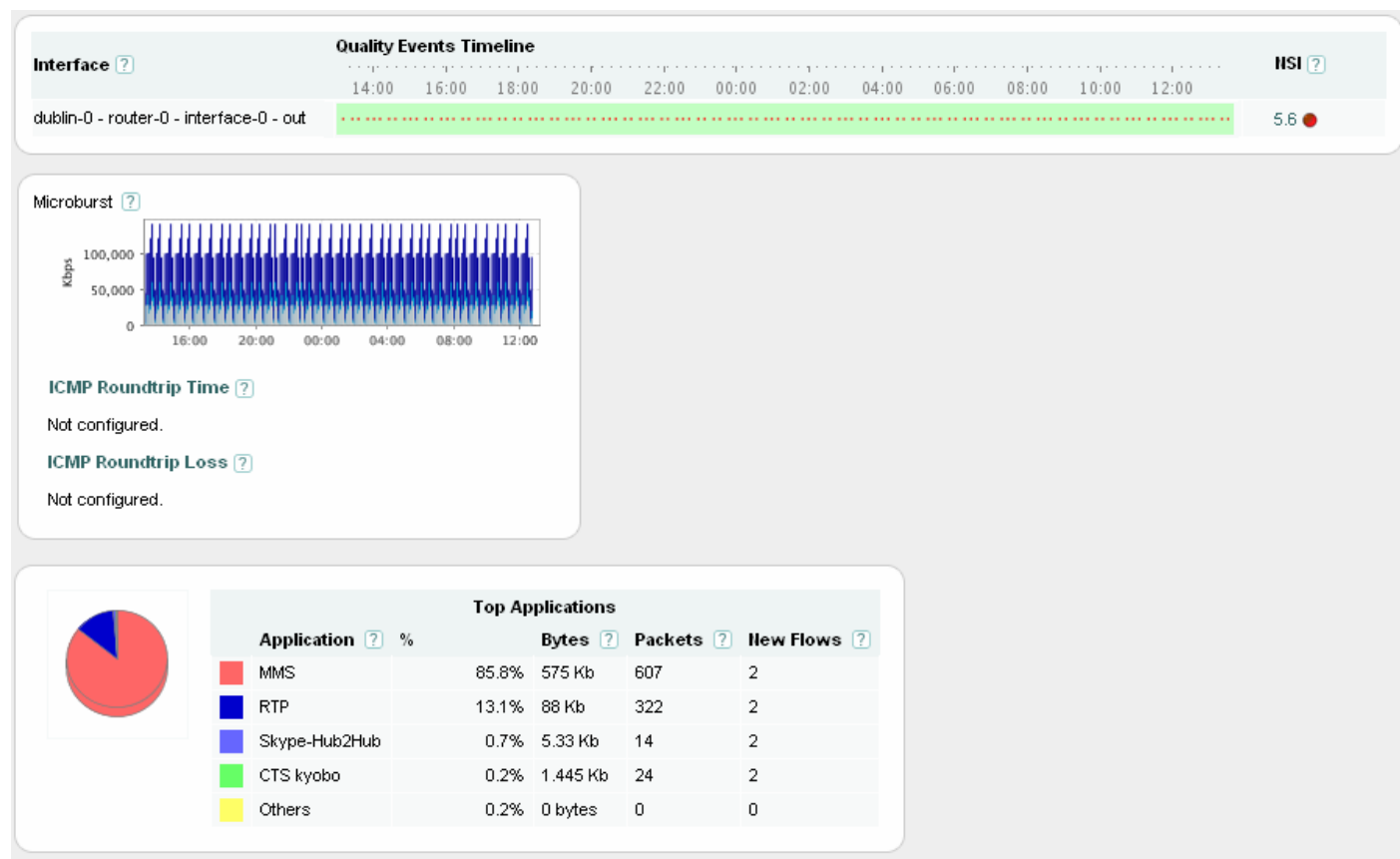
The **Bytes** column displays the total number of bytes transmitted during the selected timescale of each packet size.

Identifying the Source of Application Performance Problems

The following example scenario shows how you can use 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.

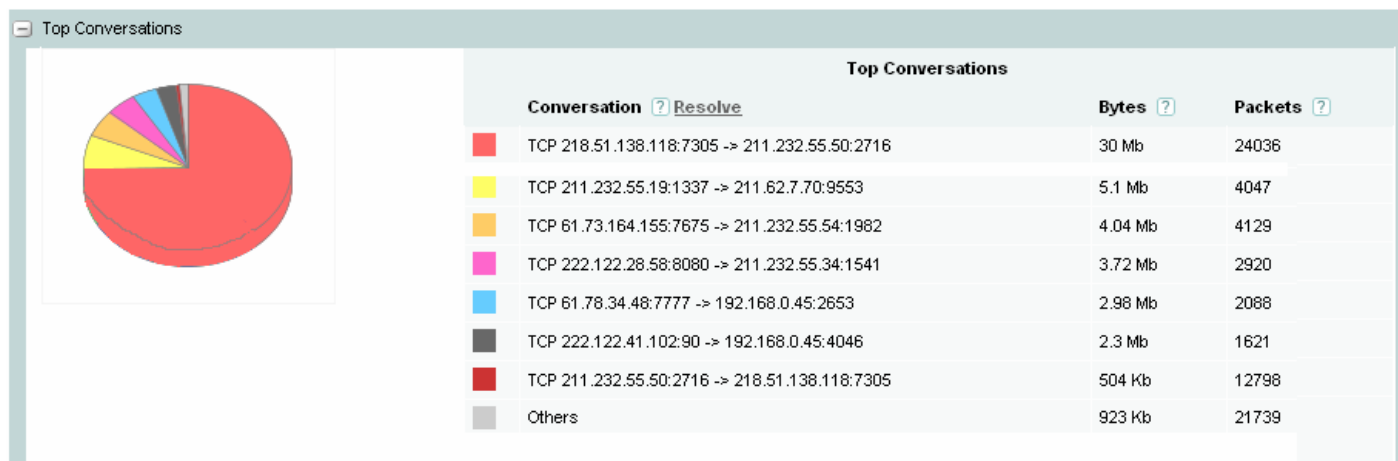
Figure 5-42 Events and Microburst



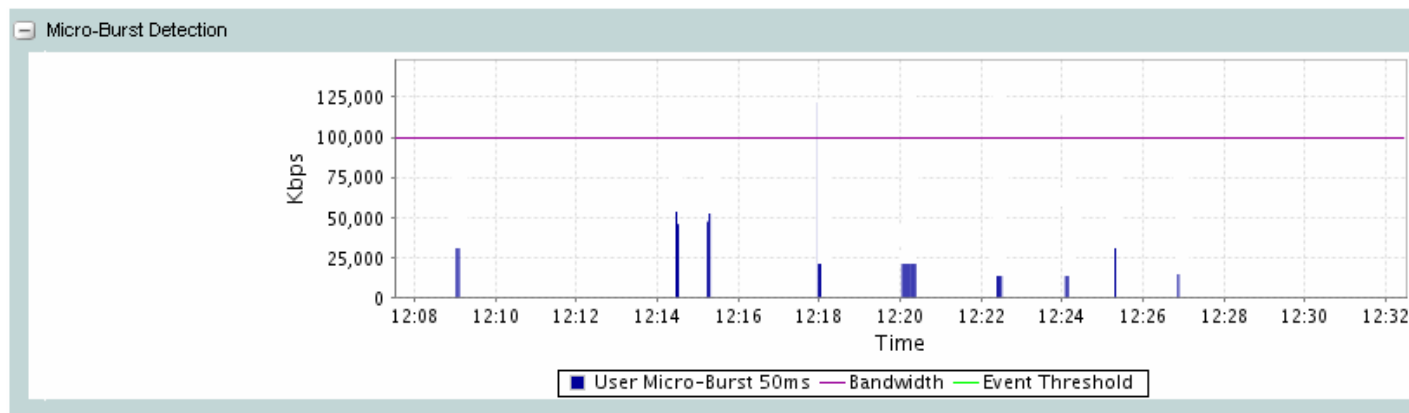
Also, in this example, the micro-burst plot shows that the traffic is peaking to line rate frequently.

In this case there is a threshold set to 90% of link rate, so we navigate to the **Event Analysis** tab from the Dashboard. On the **Event Analysis** tab, there are many micro-burst events in the data class for that branch office that 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 5-43 Top Conversations

For confirmation, we create a traffic filter to exclude that specific IP address.

Figure 5-44 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.

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 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 system:

```
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 already be configured. 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:

```
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 5-2 **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 may increase the file size.



Note If the appliance 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 appliance so that you have all captured data available. The temporary file contains data up to the point that the appliance 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 appliance 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 appliance because a certain amount of the additional data appended to the file for use in event analysis 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 appliance. See the section "Setting a Packet Capture Password" for more information.



Note As an alternative to “pushing” the captures files from the appliance to a remote server, you can also “pull” them from the appliance from a remote machine that uses scp to contact the BQM ssh server.

If you have physical access to the appliance, the winscp client program is recommended for transferring files to a directly-connected Windows laptop. This program allows the available capture files 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:

```
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 Cisco ADE employs a separate logical 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 logical disk.



Note For more information on the mapping of BQM logical disks to physical disks in the Cisco ADE, see the section “Physical and Logical Disks” in the chapter “System Administration.”

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
```

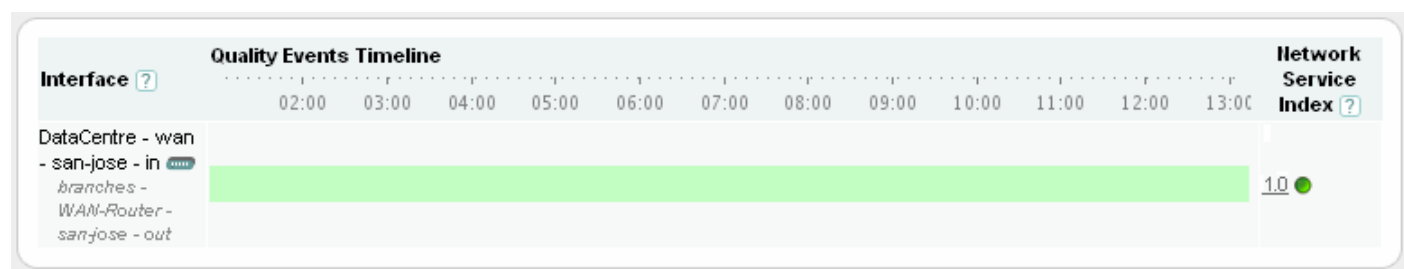
The password should be at least six characters long with a mixture of letters and numbers.

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.

Figure 5-45 Quality Events Timeline Showing No Events



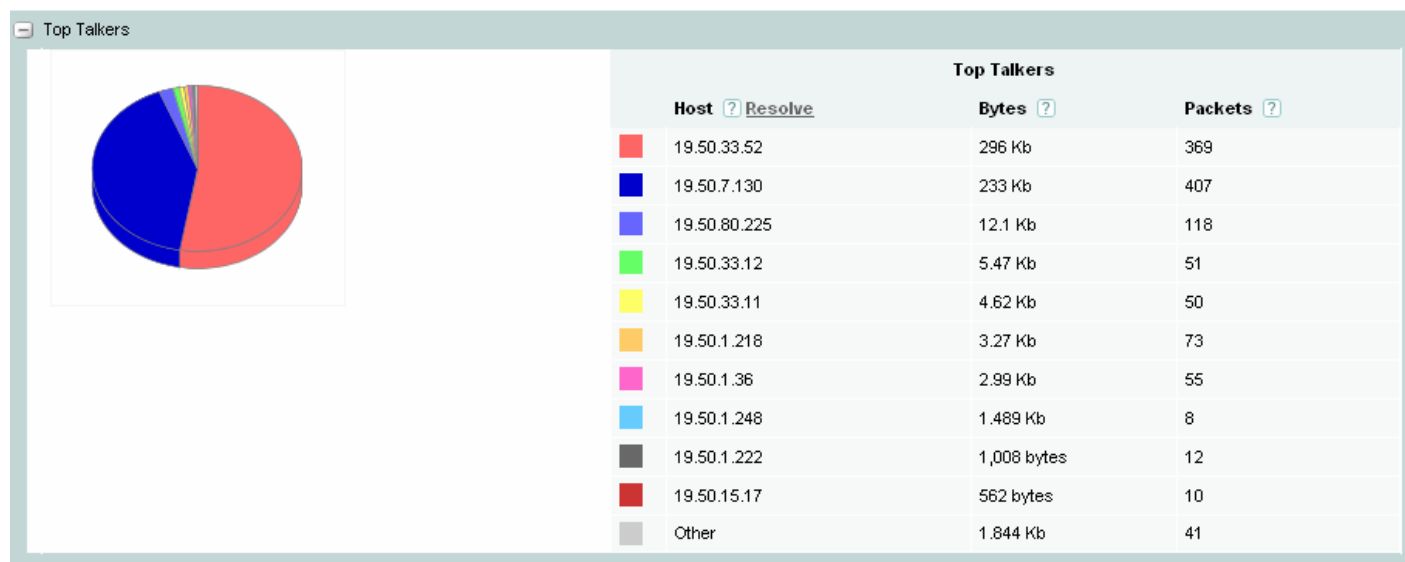
We start a manual packet capture around 9:00 am for 3 hours with a snap length of 1500 bytes to capture entire packets:

```
host(config-capture)# capture default_serial1
host(config-capture)# attach interface sanfranhq default_serial1
host(config-capture)# snaplength 1500
host(config-capture)# duration 120 minutes
host(config-capture)# start
host(config-capture)# capture default_peer
host(config-capture)# attach peer-interface sanfranhq default_serial1
host(config-capture)# snaplength 1500
host(config-capture)# duration 120 minutes
host(config-capture)# start
```

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.

Figure 5-46 Event Top Talkers Based on Manual Packet Capture



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 BQM.

```
host(config)# copy capture:serial0 scp://admin@192.168.3.4:serial0
```



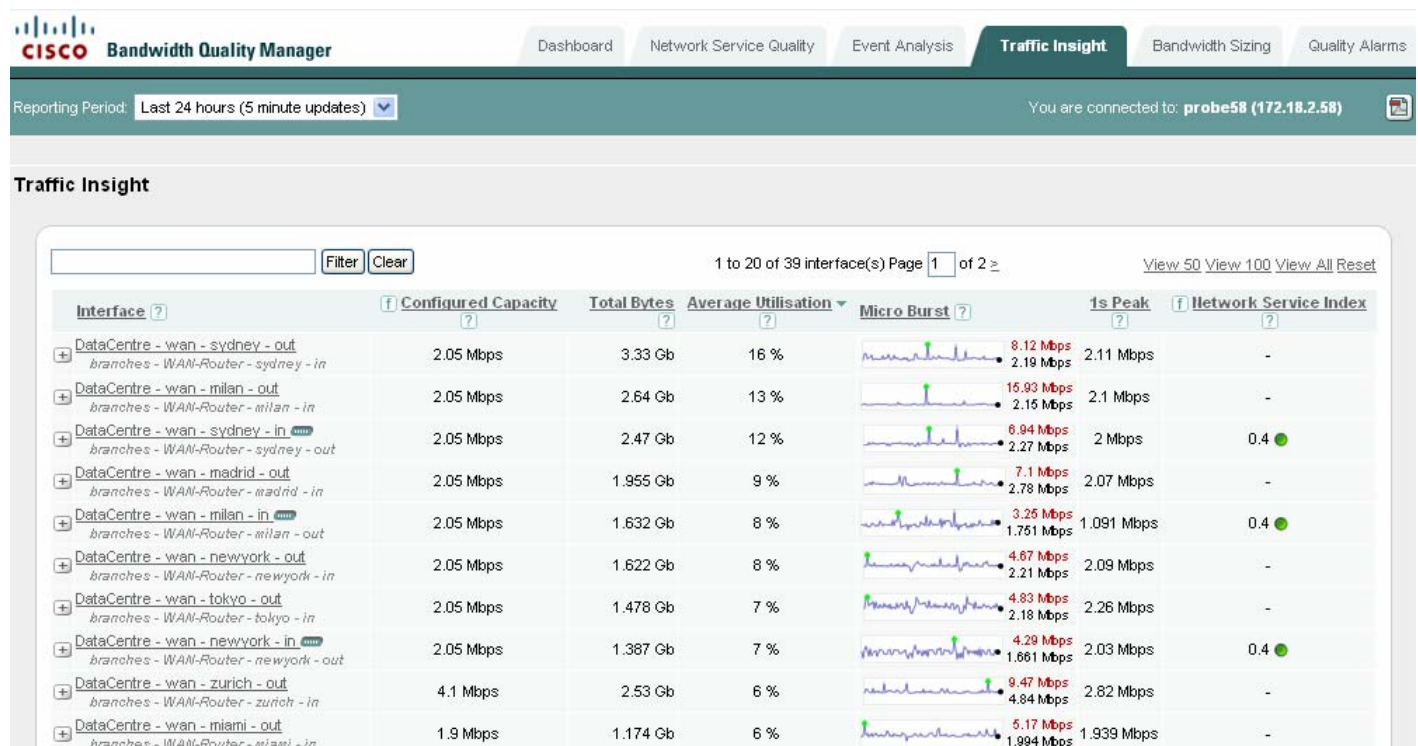
6 Monitoring Network Traffic

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 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 Network Service Index) for each of these interfaces.

Figure 6-1 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 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 6-1 **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).
Configured Capacity	Displays the configured capacity of the interface or class.
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 or class 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.
1s Peak	Displays the maximum measured one-second peak value during the chosen reporting period. Comparing this value with the maximum microburst value indicated on the sparkline 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.
Network Service Index	<p>Indicates quality degradation issues in the network. The Network Service Index uses PNQM measurements and EQ, when configured, to detect events impacting end-to-end network quality based on the specified quality of service targets and sizing policy. Use the Network Service Objectives menu in System Administration mode to set the quality targets and sizing policy that are used to calculate the Network Service Index.</p> <p>The Network Service Index 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 latency experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Network Service Index value seen on any class on that interface.</p> <p>A Network Service Index value greater than 1 means that loss or latency is above an acceptable level, as specified in the BQM configuration. This interface or class is not meeting its quality targets.</p> <p>A Network Service Index of less than or equal to 1 means the loss and/or latency 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.</p> <p>If you have not enabled Network Service Index calculation in the network service objective being applied to an interface, a dash (-) is displayed.</p>

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 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 field 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** 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 **NSI** column heading. The summary is rearranged according to the maximum network service indicator value per interface, with the highest value first. Click the **NSI** column heading again to sort the summary screen again, this time with the lowest 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 Network Service Index values. Click  beside the **Configured Capacity** or **NSI** 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


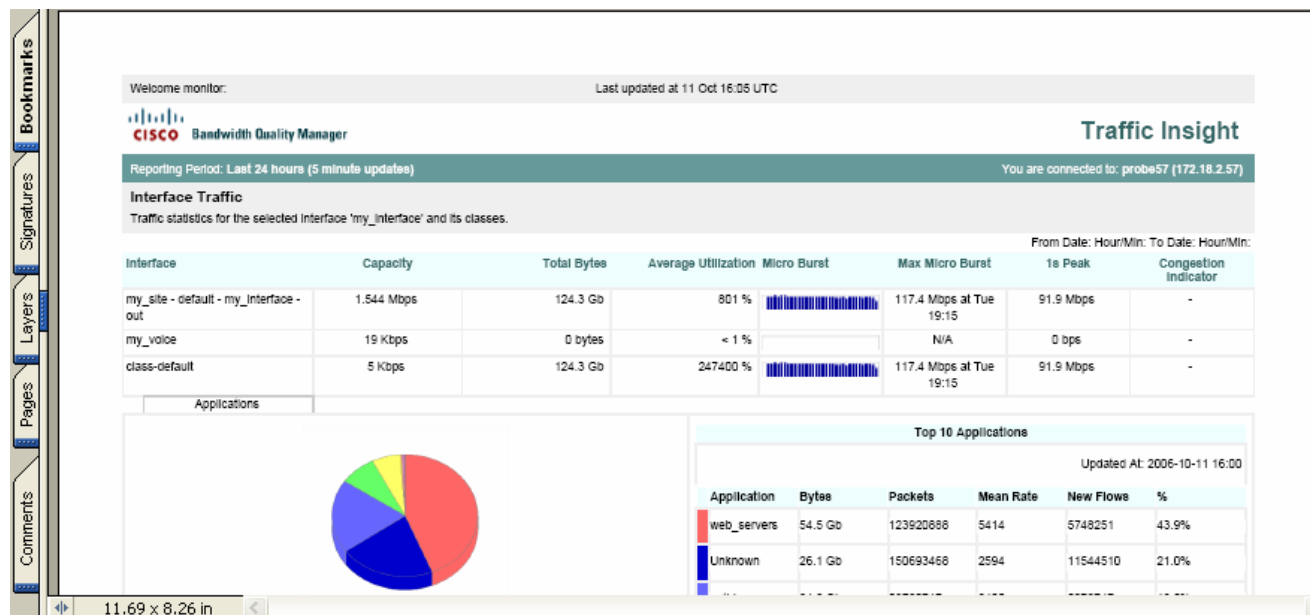
You can generate a report in .pdf format at any point when viewing event analysis results. To generate a report, click . The generated report is available for download in .pdf format. Reports are not stored on the appliance.

Figure 6-2 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 Network Service Index 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 BQM time zone.

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:

- Micro Burst 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 outbound interface information.

You can switch to the event 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

All graphs displaying bandwidth results include a unit formatter so you can view results in kbps, Mbps, or Gbps.

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:

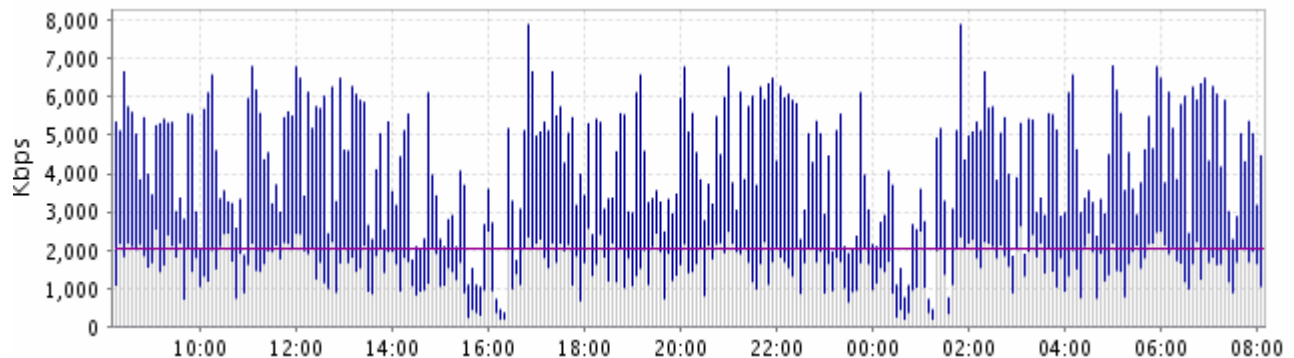
Table 6-2 Class Statistics Summary Table

Column	Description
Class	Displays the name of the configured class.
Configured 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.
1s Peak	Displays the maximum measured one-second peak value for the class traffic during the chosen reporting period. Comparing this value with the maximum microburst value indicated on the sparkline 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.
Network Service Index	<p>Indicates quality degradation issues in the network. The Network Service Index uses PNQM measurements and EQ, when configured, to detect events impacting end-to-end network quality based on the specified quality of service targets and sizing policy. Use the Network Service Objectives menu in System Administration mode to set the quality targets and sizing policy that are used to calculate the Network Service Index.</p> <p>The Network Service Index 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 latency experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Network Service Index value seen on any class on that interface. A Network Service Index value greater than 1 means that loss or latency is above an acceptable level, as specified in the BQM configuration. A Network Service Index of less than or equal to 1 means the loss and/or latency are within the specified targets.</p> <p>If you have not enabled Network Service Index calculation in the network service objective being applied to an interface class, a dash (-) is displayed.</p>

Identifying Microburst Measurements

When you view the details for an interface or a class, the Microburst Detection plot is displayed.

Figure 6-3 *Microburst Results*



The legend below the graph identifies the color of each plotted line. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps. The graph is based on 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 network service objective for measuring microbursts (for example, 50 ms)
- for classes only, the graph includes the measured peak rate based on the timescale configured in the network service objective queuing targets for delay (for example, 500 ms)

The threshold configured in the network service objective for triggering event detection on microbursts (for example, 1000 kbps 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 network service objective 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 network service objective 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 **Network Service Objectives** 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 Network Service Quality Monitoring Features” section of the “Configuring Network Service Quality 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

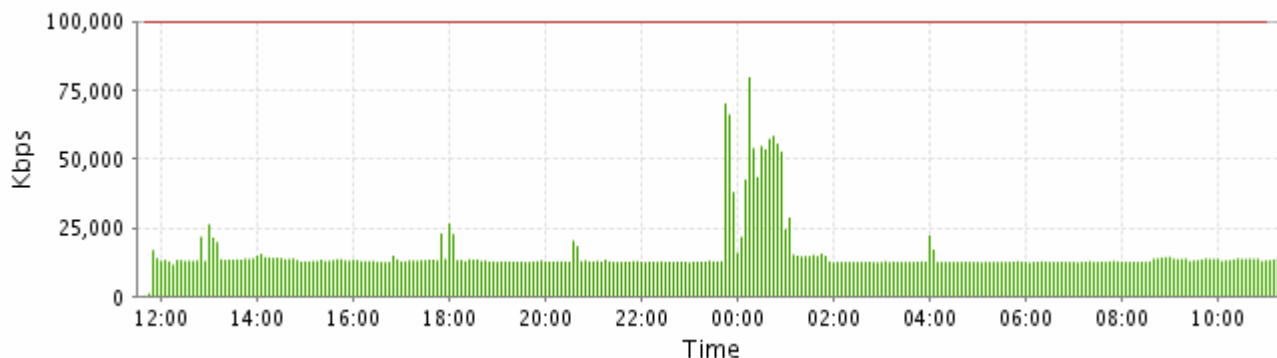
You can use these graphs to identify the traffic patterns for the chosen reporting period. For example, if values displayed in the average bit rate and packet rate graphs vary significantly, the traffic is probably bursty. Smoother traffic will tend to have fewer variations of these statistics over time. 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 6-4 Average Bit Rate Graph

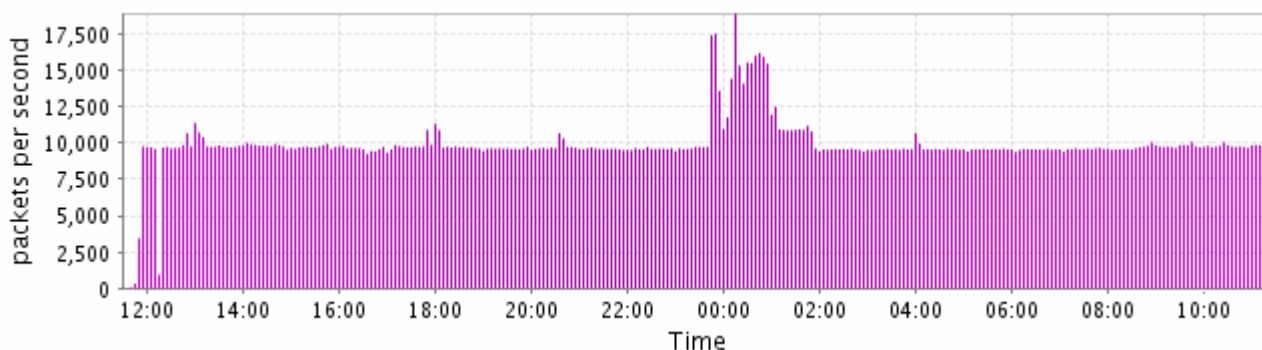


The maximum, minimum and mean values are listed beside the plot. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps.

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 6-5 Average Packet Rate Graph

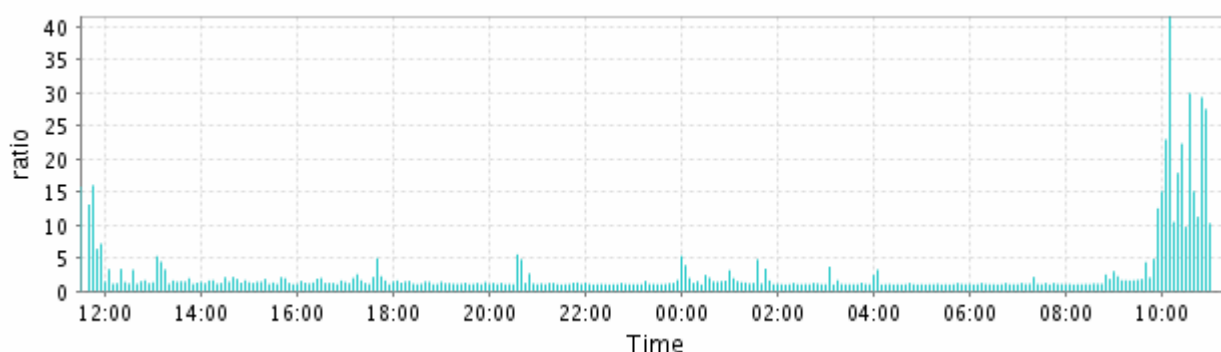


The maximum, minimum and mean values are listed beside the plot.

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 6-6 Peak-to-Mean Ratio Graph

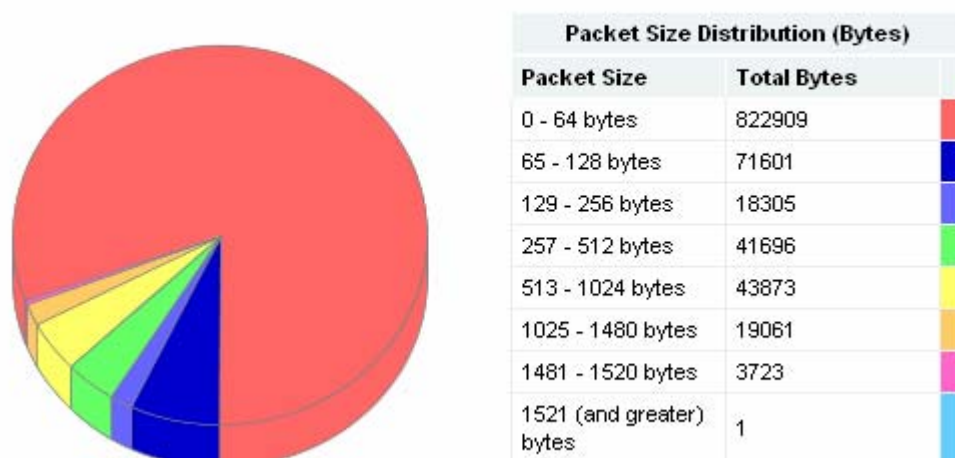


The maximum, minimum and mean values are listed beside the plot.

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 6-7 *Packet Size Distribution Chart*



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:

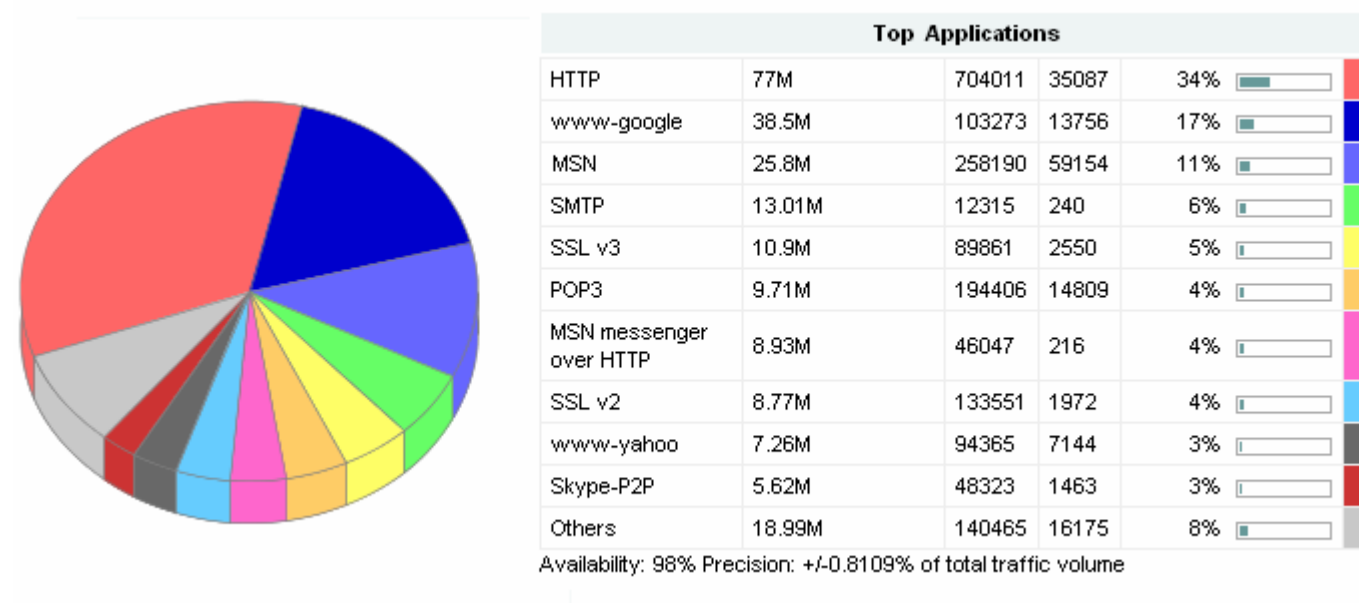
- Top applications
- Top talkers
- Top listeners
- Top conversations

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 6-8 Top Applications



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.

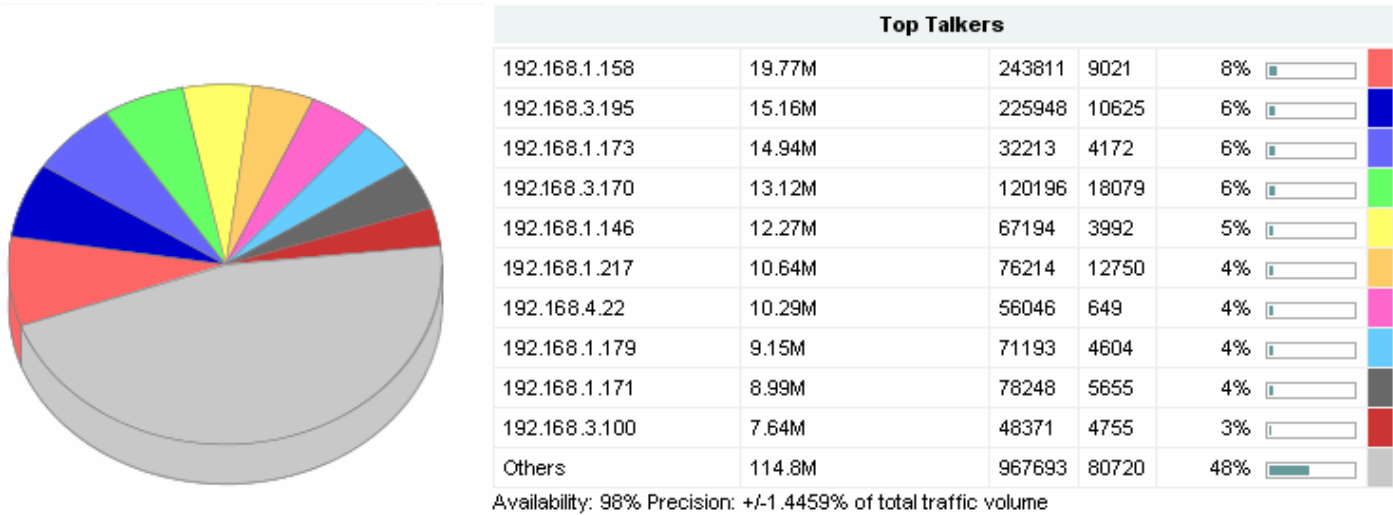
Availability and Precision statements provide information on the amount of traffic on which the results are based.

A second chart and list provides further information on the top 50 applications.

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 6-9 Top Talkers



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**. Place the cursor over the DNS name to view the associated IP address.

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.

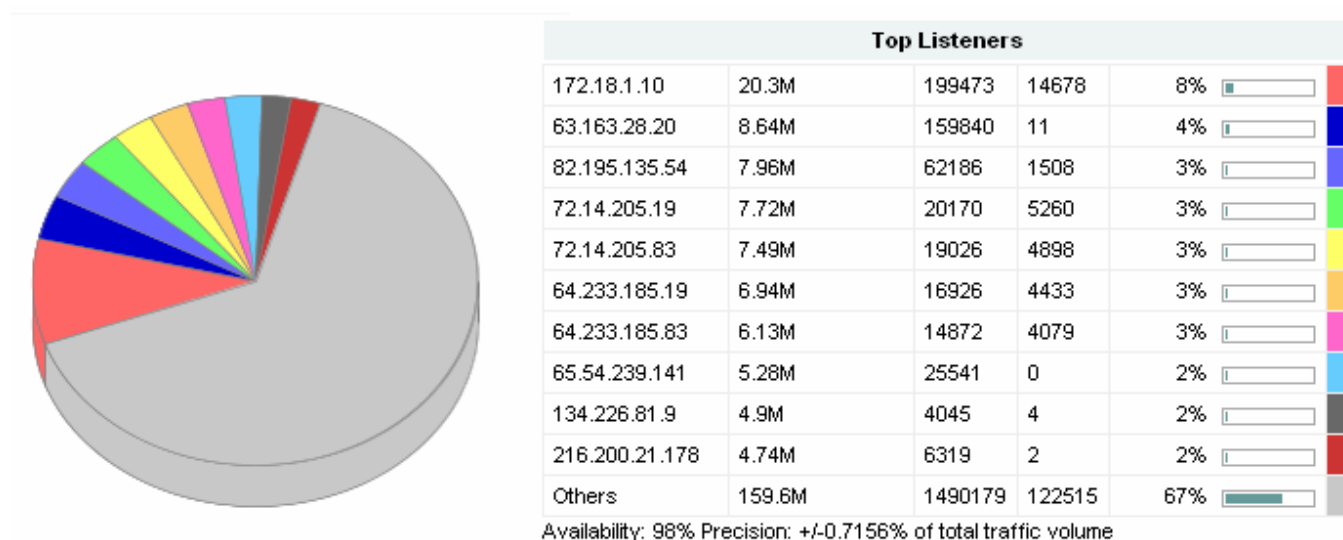
Average bit rate and packet rate graphs are available for each of the top talkers listed.

A second chart and list provides further information on the top 50 applications.

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 6-10 Top Listeners



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**. Place the cursor over the DNS name to view the associated IP address.

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.

A second chart and list provides further information on the top 50 applications.

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 6-11 Top Conversations



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**. Place the cursor over the DNS name to view the associated IP address.

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.

A second chart and list provides further information on the top 50 applications.



7 Bandwidth Sizing

This chapter describes how to use BQM to estimate the interface bandwidth required to prevent queuing latency 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 least 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.



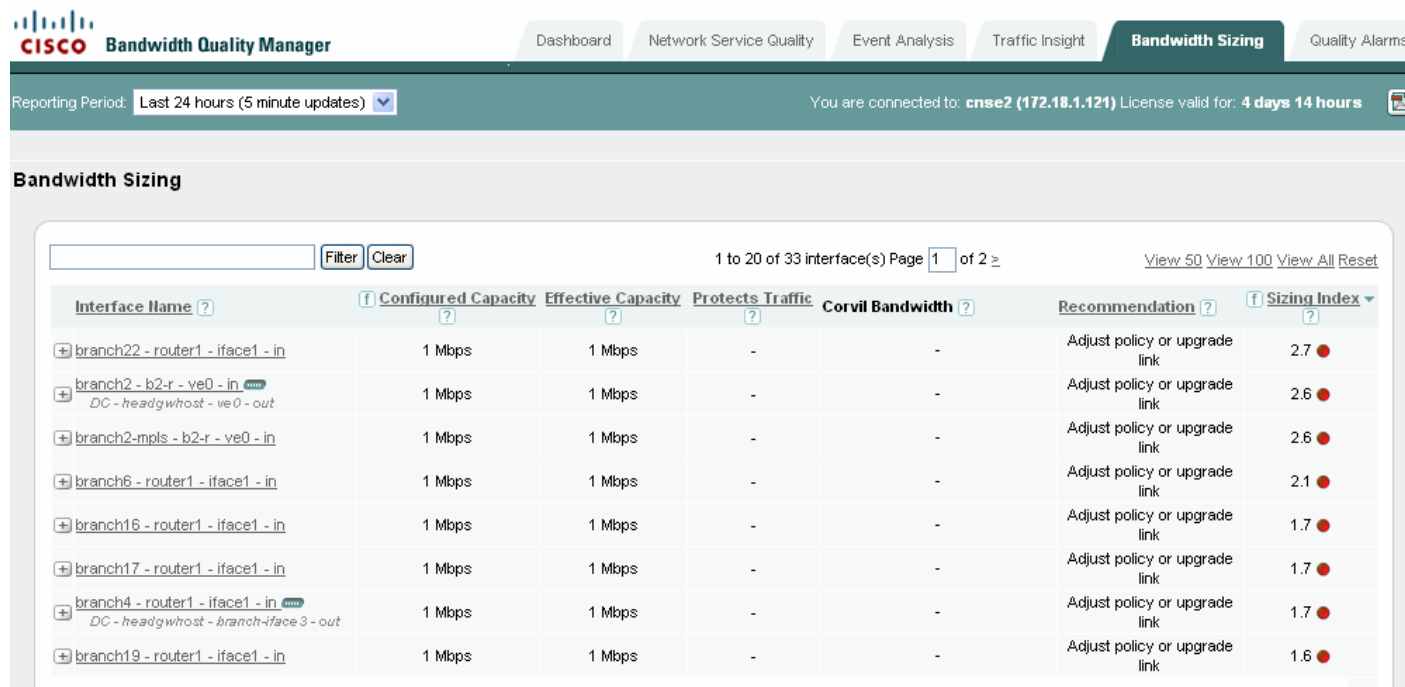
Note . To enable bandwidth sizing as a feature, you must enable Corvil Bandwidth measurement, and configure both a set of queuing targets and a sizing policy, in the network service objective that is applied to the class.

For more information on queuing targets and the sizing policy in the class network service objective, see “Enabling Network Service Quality 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 7-1 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 7-1 Bandwidth Sizing Summary Table

Column	Description
Interface	<p>Displays the full, qualified name identifying the interface and the direction of the traffic (inbound or outbound) being measured by the interface: <i>site name – router name – interface name – direction</i>.</p> <p>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).</p>

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 Traffic	<p>Displays (for classes) the percentage of traffic to which the listed recommendation and Sizing Index calculation applies. The percentage value here is configurable as part of defining the sizing policy for an interface. The sizing policy is configured in the network service objective applied to the interface and its classes.</p> <p>Permitting a certain fraction of the packets to violate the queuing targets reduces the bandwidth required from that needed to guarantee no loss or latency for every single packet.</p> <p>For example, by protecting 99% of traffic, the resulting bandwidth requirement calculated by BQM ensures that 99% of arriving packets encounter</p> <ul style="list-style-type: none"> - a total per-hop queuing latency no greater than the queuing-targets delay value defined in the network service objective - a queue length no greater than the configured queue limit defined for the class
Corvil Bandwidth	<p>The graphic illustrates the Corvil Bandwidth values measured for each class during the selected reporting period. In single class configurations, the class data is displayed at interface level. In multiclass configurations, no interface data is displayed.</p> <p>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 latency and loss in every busy-period in the displayed interval.</p>
Recommendation	<p>Displays the recommended course of action based on the calculated bandwidth requirement for the interface and class.</p> <p>See the section “Viewing Sizing Results” for more information on the displayed recommendations.</p>
Sizing Index	<p>Indicates quality degradation issues in the network. The Sizing Index uses PNQM measurements and EQ, when configured, to detect events impacting end-to-end network quality based on the specified quality of service targets and sizing policy. Use the Network Service Objectives menu in System Administration mode to set the quality targets and sizing policy that are used to calculate the Sizing Index.</p> <p>The Sizing Index value is a unitless number which reflects the congestion level on a link or class. For a class, it reflects the extent</p>

	<p>by which the loss and/or latency experienced by the class exceed the user-specified targets for these. For an interface, it represents the worst Sizing Index value seen on any class on that interface.</p> <p>A Sizing Index value greater than 1 means that loss or latency is above an acceptable level, as specified in the BQM configuration. This interface or class is not meeting its quality targets.</p> <p>A Sizing Index of less than or equal to 1 means the loss and/or latency 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.</p> <p>A low Sizing Index value could indicate a candidate for bandwidth downgrade.</p> <p>If you have not enabled Sizing Index calculation in the network service objective being applied to an interface, a dash (-) is displayed'</p>
--	---



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 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** field 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 Sizing Index values, you click the **Sizing Index** column heading to sort. The summary is rearranged according to the maximum measured microburst values per interface, with the highest value first. Click the **Sizing Index** 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 Sizing Index values. Click  beside the **Configured Capacity** or **Sizing Index** 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 event analysis results. To generate a report, click . The generated report is available for download in .pdf format. Reports are not stored on the appliance.

Figure 7-2 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 Sizing Index 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 BQM time zone.

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 **Network Service Quality**, **Event 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 necessary. 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 Sizing Index values calculated for each class. In turn the Sizing Index 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 network service objective.

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 Sizing Index 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 Sizing Index 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 Sizing Index 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 Sizing Index 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 Sizing Index for the class is greater than one and the sizing calculation is dominated by the delay target. The queuing latency 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 Sizing Index 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 latency, 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 7-3 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 percentage of packets in every busy period included in the reporting period, where the busy period is specified in the associated network service objective.

The Corvil Bandwidth values are displayed as a series of values for each five minutes during the reporting period. The graph includes a unit formatter so you can view results in kbps, Mbps, or Gbps. The graph legend indicates the colors used to display each:

Max - the maximum of the Corvil Bandwidth values calculated each five minutes during the chosen reporting period.

x% - 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 network service objective being applied to the class. If none has been configured, the system defaults to the 99.9th 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 network service objective, 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 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 the greatest Sizing Index values.

Figure 7-4 Bandwidth Sizing

Reporting Period: Last 30 days (3 hour updates) You are connected to: probe101 (172.18.2.101)

Bandwidth Sizing

1 to 20 of 22 interface(s) Page 1 of 2 [View 50](#) [View 100](#) [View All](#) [Reset](#)

Interface Name ?	Configured Capacity ?	Effective Capacity ?	Protects Traffic ?	Corvil Bandwidth ?	Recommendation ?	Sizing Index ?
+ NewYork-Office - WAN-Router - newyork - in	2.05 Mbps	2.05 Mbps	-	-	Adjust policy or upgrade link	12.2 ●
+ Miami-Office - WAN-Router - miami - in	1.024 Mbps	1.024 Mbps	-	-	Adjust policy or upgrade link	7.3 ●
+ Madrid-Office - WAN-Router - madrid - in	2.05 Mbps	2.05 Mbps	-	-	No action required	0.9 ●
+ London-Office - WAN-Router - london - in	2.05 Mbps	2.05 Mbps	-	-	No action required	0.7 ●
+ Milan-Office - WAN-Router - milan - in	2.05 Mbps	2.05 Mbps	-	-	No action required	0.7 ●
+ Sydney-Office - WAN-Router - sydney - in	2.05 Mbps	2.05 Mbps	-	-	No action required	0.7 ●
+ Tokyo-Office - WAN-Router - tokyo - in	2.05 Mbps	2.05 Mbps	-	-	No action required	0.6 ●
+ HongKong-Office - WAN-Router - hongkong - in	4.1 Mbps	4.1 Mbps	-	-	No action required	0.3 ●
+ Lisbon-Office - WAN-Router - lisbon - in	4.1 Mbps	4.1 Mbps	-	-	No action required	0.3 ●
+ Paris-Office - WAN-Router - paris - in	2.05 Mbps	2.05 Mbps	-	-	No action required	0.3 ●
+ Seoul-Office - WAN-Router - seoul - in	4.1 Mbps	4.1 Mbps	-	-	No action required	0.3 ●
+ Toronto-Office - WAN-Router - toronto - in	4.1 Mbps	4.1 Mbps	-	-	No action required	0.3 ●
+ Zurich-Office - WAN-Router - zurich - in	4.1 Mbps	4.1 Mbps	-	-	No action required	0.3 ●

Local intranet

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 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 Sizing Index 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 **Event Analysis** tab and examining the expected queuing latency 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 Sizing Index 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 BQM to identify class resource requirements on a multi-class network.

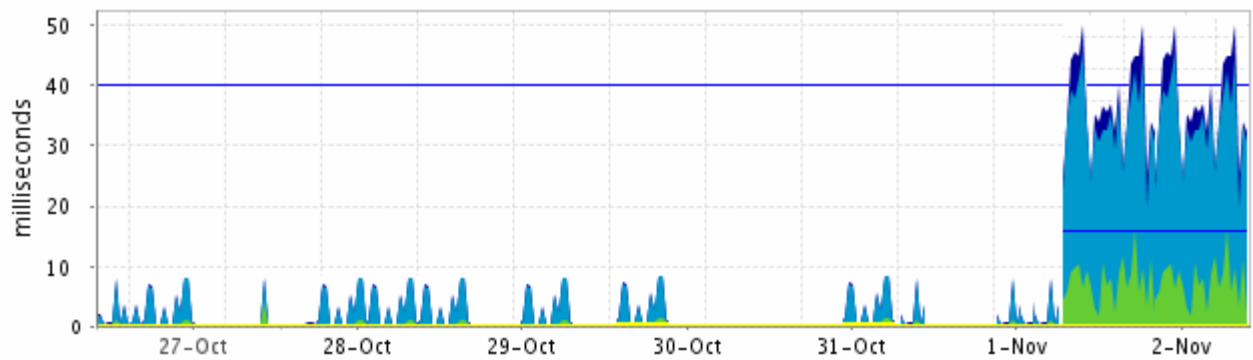
In this example, the **Bandwidth Sizing** tab is showing a remote site representing a branch office as having a Sizing Index of 7.3.

Figure 7-5 Sizing Index High

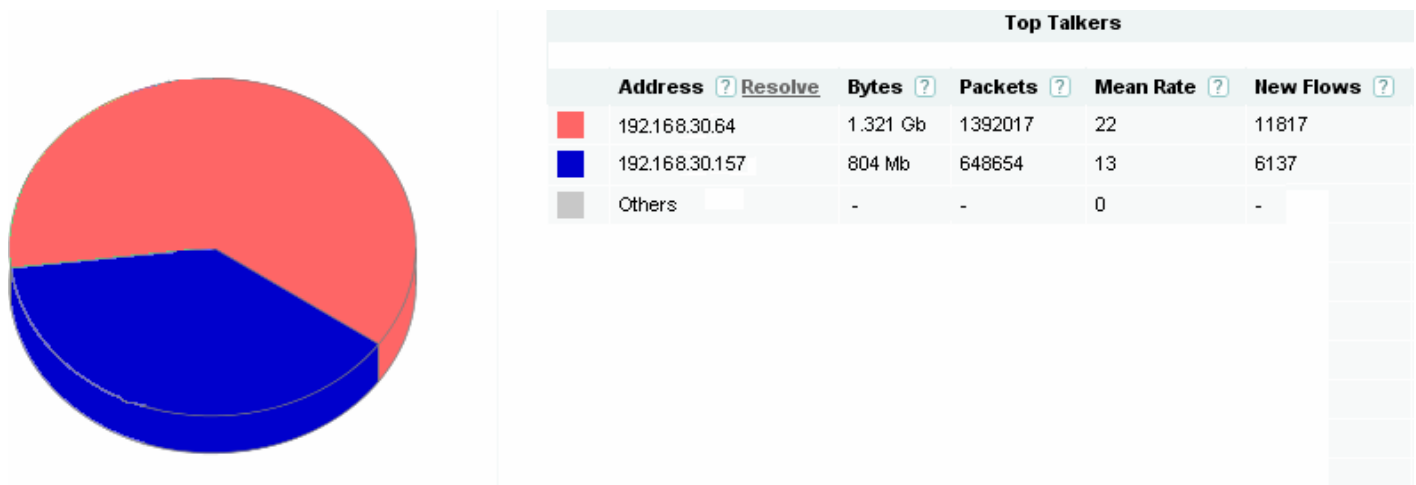
<div><div></div><div>Miami-Office - WAN-Router - miami - in</div></div>	1.024 Mbps	1.024 Mbps	-	-	Adjust policy or upgrade link	7.3 <div></div>
---	------------	------------	---	---	---	-----------------

Next, we navigate to the **Event Analysis** tab for the branch remote site.

The Sizing Index value is caused by the latency 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 latency being experienced from 24 hours earlier.

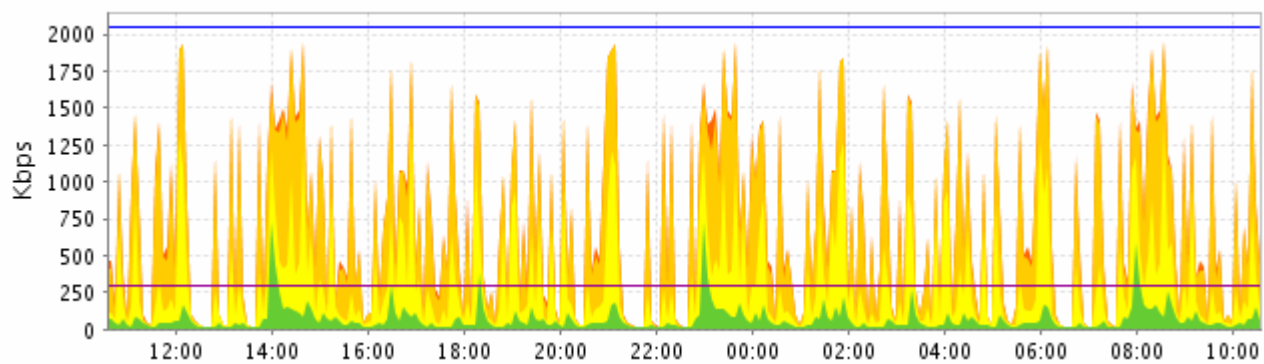
Figure 7-6 Increased Latency

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 7-7 Top Talkers

In this example, someone had installed a second video conference unit without notifying networks.

We navigate to the bandwidth sizing related link and view sizing information for the video class over the past 24 hours.

Figure 7-8 24-hour Class Sizing Results

We can then submit a network change to increase the size of the video class.



8 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 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 CLI 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 CLI:

- Configuration mode
- Network service objective 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
- Port 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 for 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 appliance 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
  network service objective Configure a network service objective
  no             Reverses next command, such as creation of a class-
map.
  ntp             Configures Network Time Protocol Services.
  --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 BQM configuration 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 BQM configuration 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 get information about the running system, 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 clear the network model configuration and delete any network model 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)?
```



Note The **clear config** command does not affect system configuration commands, for example, the **allow**, **logging**, **domain name-server** and **[no] service** commands. Therefore you need to use the clear config command with caution.

For example, let’s say you issue the commands **allow 10.1.1.0/24** and **no service telnet** and later use the **clear config** command followed by the **setup** command and enter new setup parameters. If this device is then shipped to a location not on the 10.1.1.0 network, connectivity will not be possible. Even if it is on the 10.1.1.0 network, telnet is still disabled.

Saving and Restoring Configuration Changes

You use the **copy** command in configuration mode to save the current configuration.

To save the current configuration, you use the following command:

```
host(config)# copy config
```

Logging Out of the BQM CLI

Enter the **logout** command at any time to end your configuration session and log out of BQM:

```
host(config)# logout
```

Configuring BQM Using the CLI

As is the case when using the GUI, you configure BQM in a certain order with network service objectives 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 Network Service Objective

The purpose of a network service objective is to define the required end-to-end QoS monitoring features, and associated event detection thresholds, establishing an end-to-end latency and loss-based event detection policy for traffic between sites.

You use the **nso-map** configuration command to create a network service objective. The syntax of the nso-map command is as follows:

```
nso-map name
no nso-map name
```

The following table describes the configuration commands available from the network service objective context:

Table 8-1 Network Service Objective Commands

Command	Description
description	Specifies a text description for the network service objective.
one-way-latency milliseconds <i>msecs</i> [variation milliseconds <i>msecs</i>]	Specifies the maximum tolerable one-way packet latency for end-to-end measurements, with an option to specify a maximum one-way latency variation.
protect-packets percent <i>percent</i> busy-period [minutes <i>mins</i> hours <i>hours</i> day week]	Specifies the percentile and busy period values for network service index and bandwidth sizing calculation. The configured percentile value is also used to display graph data.
measure-pnqm [packets-per-second <i>pckts</i> all] [event-thresholds	Specifies passive network quality monitoring measurements, and sets optional event detection thresholds.

Using the Command Line Interface (CLI)

[latency] [latency variation] [loss]	
measure-icmp [interval-milliseconds <i>msecs</i>][bytes <i>bytes</i>][roundtrip-target-delay-milliseconds <i>msecs</i>][event-thresholds [delay][loss]]	Specifies the ICMP ping packets parameters and optional thresholds at which to trigger event detection.
measure-eq [event-threshold {bandwidth <i>kbps</i> percent <i>percent</i> }]	Specifies that calculation of Expected Queuing Latency and Expected Queuing Loss is enabled, and sets optional event detection thresholds.
measure-bandwidth [event-threshold {bandwidth <i>kbps</i> percent <i>percent</i> }]	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 <i>msecs</i> [event-threshold {bandwidth <i>kbps</i> percent <i>percent</i> }]	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 [use-one-way<msecs>] protect-packets [use-one-way percent <percent>]	Specifies the delay target in milliseconds and enables loss tracking for Corvil Bandwidth calculation, expected queuing and bandwidth sizing.

For more details on the full syntax and examples of the use of each command, see the “Command Reference” chapter of this document.

The following example show the default network service objective named *network-services-objective-default*. It is applied by default to the default policy-map and may be edited, but cannot be deleted. The default network service objective defines a one-way latency target of 500 milliseconds. 99.9% of packets must meet the defined target over every four-hour period. PNQM measurement is enabled to provide end-to-end result, along with associated event detection thresholds, as is ICMP ping measurement. Expected Queuing measurement is enabled with associated event detection thresholds. Corvil Bandwidth measurement for bandwidth sizing is explicitly enabled. No explicit queuing targets are specified, so the configured one-way latency value is used for the queuing delay target (500 milliseconds). Microburst measurement down to a resolution of 50 milliseconds is also enabled:

```
nso-map network-service-objective-default
  measure-microburst milliseconds 50
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period hours 4
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 10000 size 36 event-thresholds delay loss
  one-way-latency milliseconds 500
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
```



Note .If you want to disable Expected Queuing calculation or ICMP measurement using the **no measure-eq** or **no measure-icmp** commands when configuring multiclass policy maps you must disable EQ or ICMP in all classes and also at the interface level. The interface level usually has the default network service object applied but this is not shown when you use the **show config** command and in addition no EQ or ICMP results are displayed at interface level.

When you attempt to disable EQ or ICMP you should use the **show policy-map**, or **show detailed-config** commands to check and ensure that both network service objectives used by the class and interface have EQ or ICMP disabled.

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.



Note We recommend that if you define class-map match rules in the CLI, you edit them using the CLI. If you define match rules using the GUI, edit them using the GUI.

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 8-2 **Class match Commands**

Command	Description
<code>match any</code>	Specifies that all packets will be matched.
<code>match application</code>	Specifies the name of an application to be used as a matching rule.
<code>match not match-criteria</code>	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.
<code>match class-map class-name</code>	Specifies the name of a traffic class to be used as a matching rule (for nesting traffic classes [nested class-maps] within one another).
<code>match ethertype ethertype value</code>	Specifies the ethertype value used to match traffic based on Ethernet Type field of the Ethernet MAC header (assuming Ethernet Type II frames).
<code>match ip</code>	Configures the match criteria for a class-map to be successful for IP packets, subject to certain specified conditions
<code>match ip dscp ip-dscp-value</code>	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.
<code>match ip precedence ip-precedence-value</code>	Specifies up to eight well-known IP Precedence values used as match criteria, or alternatively a numeric value from 0 to 7.
<code>match mpls match-criteria</code>	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.
<code>match tcp match-criteria</code>	Configures the match criteria for a class-map to be successful for TCP traffic, subject to certain specified conditions.
<code>match udp match-criteria</code>	Configures the match criteria for a class-map to be successful for UDP traffic, subject to certain specified conditions.
<code>match vlan vlan-id</code>	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 172.16.1.11. 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.c` includes some of the characteristics of traffic class `snmp.c`, 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.c`, 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 8-3: 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 8-4: 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 Server 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
SNNTTP	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 network service objectives). 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 network service objective are associated with the class using the **nso** 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 nso command is as follows:

```
nso network service objective name
no nso network service objective 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 8-5 Policy-map Commands

Command	Description
<code>policy-map <i>policy-name</i></code>	Specifies the name of the traffic policy to configure. Names can be a maximum of 40 alphanumeric characters.
<code>class <i>class-name</i></code>	Specifies the name of a predefined traffic class, which was configured with the class-map command, used to classify traffic to the traffic policy.
<code>class class-default</code>	Configures the properties of the default class created as part of the traffic policy.
<code>bandwidth {<i>bandwidth-kbps</i> remaining percent <i>percent</i> percent <i>percent</i>}</code>	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.
<code>class-adjust</code>	Specifies how much (in bytes) to adjust the size of a packet that matches the current class.
<code>priority {<i>kbps</i> percent <i>percent</i>} [<i>burstbytes</i>]</code>	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.
<code>priority-level {high medium normal low}</code>	Specifies the strict priority level of a class within a policy-map.
<code>queue-limit <i>packets</i></code>	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 network service objective 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 network service objective and a bandwidth allocation request.

```

policy-map high-speed

  class real_time_traffic
    nso realtime
    bandwidth 3000
    queue-limit 32

  class transact_traffic
    nso transactional
    bandwidth 2000

```

You configure measurement of the parameters specified by a network service objective by applying the latter with a **nso** command inside a policy-map, for example:

```
policy-map pmap
  nso nso1
  class cls
    nso mql
```

It is important to note the positioning of **nso** 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 network service objective named mql 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
  nso nso1
```

This results in mql being applied to class cls only. To achieve the desired effect, you insert an explicit exit command between the bandwidth and nso commands. For greater clarity, the **nso** command should be placed in the policy-map before any class configuration, as shown below:

```
policy-map pmap
  nso nso1
  class cls
    bandwidth percent 10
```

Although a network service objective enables Corvil Bandwidth and estimated queuing, 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 network service objectives in these contexts; where bandwidth and estimated queuing 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 network service objective which cannot be deleted. It is named nso-default by analogy with class-default. If no **nso** command is used within a class, the default is applied. If no **nso** command is used within policy-maps, no network service objective 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 nso
  class cls
    nso nso-default
```

The parameters of nso-default can be changed with the **nso-map** command. For example, the default peak-rate timescale can be changed to 100ms with the following CLI fragment:

```
nso-map nso-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 network service objectives, and never for nso-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 8-6 Router Commands

<code>attached-port</code>	Specifies which physical ports (PortA, PortB, PortC, PortD) are used for traffic measurement by the default local site.
<code>description</code>	Specifies a text description of the router.
<code>interface</code>	Specifies the name of an interface on a router.
<code>peer-interface</code>	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.
ping-address	Sets the ICMP responder address for an interface.
ping-address-test	Sends test packets to the configured ICMP responder address to verify connectivity.
pnqm-server	Defines a PNQM measurement channel between the interface and a remote site interface.
pnqm-server-test	Sends test traffic to the remote site interface to verify PNQM connectivity.
ppp	Specifies that link fragmentation and interleaving is enabled for an interface.
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

ICMP responder address: 10.2.1.1

```

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 Serial1/0
host(config-site-router-if)# description "Link to Data Center"
host(config-site-router-if)# bandwidth 512
host(config-site-router-if)# ping-address 10.2.1.1
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

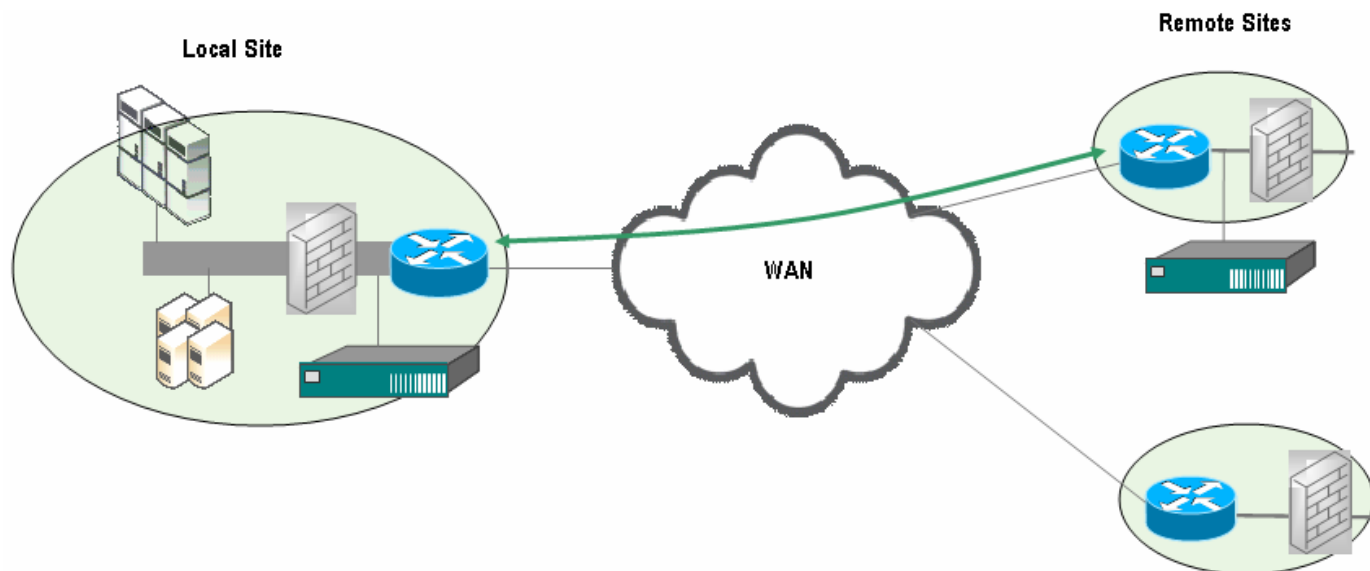
remote site router interface Serial1/0 is connected to the local site router interface named Data center core 1 Serial1/0.

```
host(config-site-router-if)# connects-to Data center core1 Serial0/1
```

Defining a Passive Network Quality Monitoring (PNQM) Channel

To measure end-to-end latency and loss between two points on the network, you define a PNQM channel between those points. The local BQM and remote BQM(s) communicate when the PNQM channel is to be established, and versions are checked, as well as the general ability to communicate.

Figure 8-1 *PNQM Channel Between Interfaces*



If there is a break in the operation of the channel, the system attempts to establish contact at regular intervals, and produces log messages about each of those attempts.

A status change results in an alert and a log message. Remote data may not be available or may be partially available due to a number of reasons:

- Remote BQM unreachable
- Remote BQM configuration miss-match
- Remote BQM down for maintenance
- Remote BQM configuration changes
- GPS status change

Passive end-to-end quality measurement requires that packet signatures and timestamps are exported from one BQM device and then processed on another BQM device. The export mechanism is a streaming protocol running over a TCP connection, the Corvil Signature Streaming Protocol (SSP). Each BQM listens on a well-known TCP port, and another BQM wishing to accept packet signatures makes a connection to this port and can then initiate multiple signature streams multiplexed over the single connection.

The packet signature export service implements the TCP server side of the signature streaming protocol. It authenticates connections from other BQM units (currently IP level only, but better authentication mechanism required) and then processes messages from the client BQM. When the client BQM requests a signature stream, the signature export service updates the packet classification state to enable signature generation for the specified stream with the client-specified parameters (hash seed, sample rate etc). Then as packets arrive, the packet signature export service generates the packet signatures and queues them up for transmission according to the streaming protocol timing rules.

In the event that the client BQM disconnects, stops responding or violates the streaming protocol rules, the signature export service is responsible for cleaning up all state relating to the streaming channels.

The packet signature correlation service initiates and processes packet signature streams from both the local and remote BQM units. The set of channels to monitor is determined from the local BQM configuration. It opens at most one concurrent TCP connection to each remote BQM, and then initiates multiple signature streams as required over each TCP connection.

The correlation service implements the client side of the signature streaming protocol.

The basic unit of passive quality measurement is a bidirectional pair of channels; one channel representing traffic for a particular class flowing in one direction (for example, from the data centre to the branch office) and another channel representing traffic on a particular class flowing in the opposite direction.

Each unidirectional channel requires packet signature generation at two separate BQM units, so a bidirectional channel pair requires four signature streams. The correlation service first matches up signatures from the two signature streams on each unidirectional channel (one stream is sent over the network from the remote BQM and the other is collected locally). Each matched signature gives a pair of timestamps corresponding to the times a single packet was observed at the two BQM units. When a pair of matching signatures from one of the channels is compared against another pair of matching signatures from the other direction channel, a round-trip estimate can be computed. The passive ping bounded one-way latency estimation algorithm uses these samples to split the round-trip time into one-way latency components, optionally assisted by GPS clock synchronization.

Each time a packet signature from both ends of a channel matches up, a single one-way latency estimate is generated. These one-way latency estimates are gathered into per-class latency distributions and then written out to the database every five minutes.

If a packet is seen at the start stream of a channel, but never arrives at the end stream, then the packet is considered lost, and loss counters are incremented. These counters (total packets and total loss) are also maintained per class and written to the database every five minutes.

If a remote BQM unit stops responding or resets its signature streaming protocol connections, the correlation service must detect this, and then periodically attempts to reconnect. The correlation service also provides status information allowing a CLI or GUI user to see whether passive measurement is operating correctly, and if not, which streams or channels are having problems.

The current release of the software also provides two configuration modes when configuring PNQM channels between interfaces on local and remote Cisco ADEs running BQM:

- Automatic PNQM configuration
- Manual Remote BQM configuration

Automatic PNQM Configuration

Automatic configuration is performed at the local Cisco ADE only. You configure the appropriate BQM network model but you do not need to log on to remote Cisco ADEs to configure them. Automatic configuration maintains configuration 'stubs' for each remote Cisco ADE independent of the active configuration on each. Consequently, automatic configuration provides full PNQM results but only EQ results for the outbound direction from the local Cisco ADE.

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
PNQM channel responder address: 10.2.1.2
ICMP responder address: 10.2.1.1

You use the **pnqm-server** command to enable a PNQM channel and effectively ‘switch on’ PNQM measurement between the local site and the specified interface. In this example configuration, the default policy-map is applied to the interface. The default policy-map uses the default network service objective and PNQM parameters are enabled.

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 Data center core 1 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)# ping-address 192.168.5.3
host(config-site-router-if)# pnqm-server 192.168.5.2 autoconf
host(config-site-router-if)# connects-to Data center core1 Serial0/1
```

You use the **pnqm-server-test** command to verify connectivity and complete functionality of PNQM when you have configured a channel. The test consists of the following steps:

- Local BQM configuration is complete (that is, interface configures and reverse direction configured)
- Remote BQM PNQM service available
- Remote BQM version compatible
- Remote BQM configuration is compatible
- Channels can be established and report signature generation at both ends per class for 45 seconds.

```
host(config-site-router-if)# pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic (notice), 0
could not be established (error).
Test completed...
```

You do not have to save the configuration before the PNQM channel test is performed.

The PNQM channel test may fail for a number of reasons, including the following:

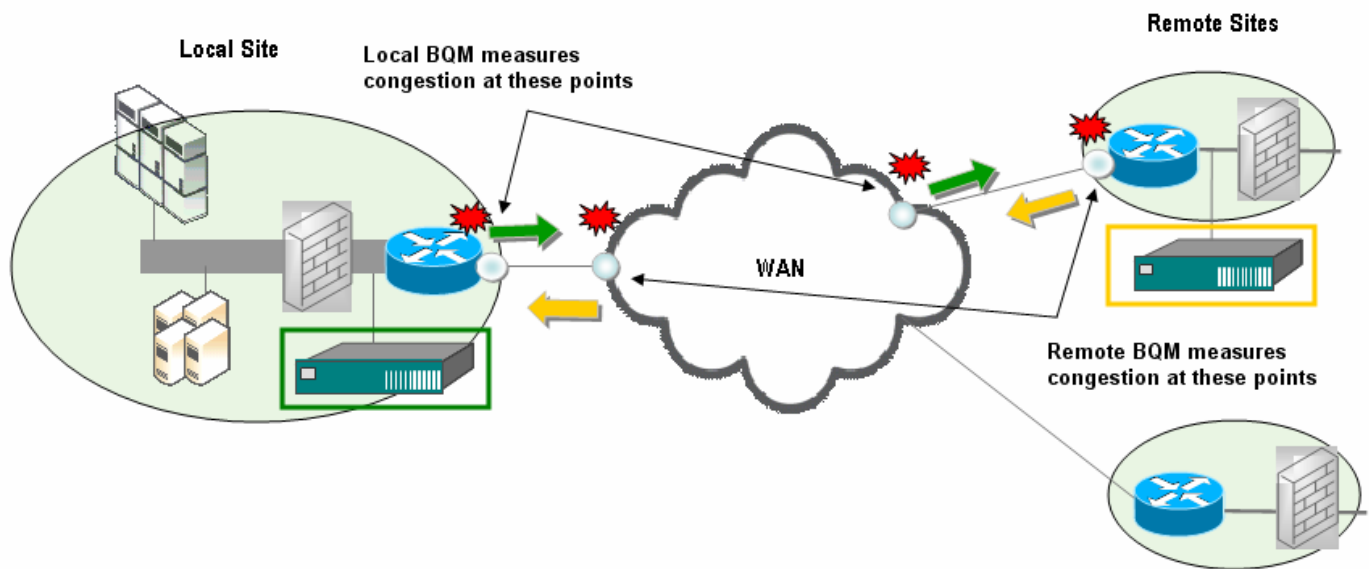
- Remote BQM unreachable
- Remote BQM version or configuration mismatch
- Remote BQM down for maintenance
- Remote BQM configuration changes

For more examples of configuring PNQM channels using automatic configuration mode, see “Configuring Network Deployment Models Using the CLI.”

Manual PNQM Configuration

In the case of manual configuration you configure the local Cisco ADE with the appropriate BQM network model and then you go to each remote Cisco ADE and manually configure each with a matching configuration in terms of interfaces, policy-maps, class-maps and match rules, but with the network model configured from the perspective of that remote Cisco ADE. Manual configuration provides you with a full set of PNQM and EQ results for both directions of the PNQM channel.

Figure 8-2 Expected Queuing Results from Local and Remote Devices

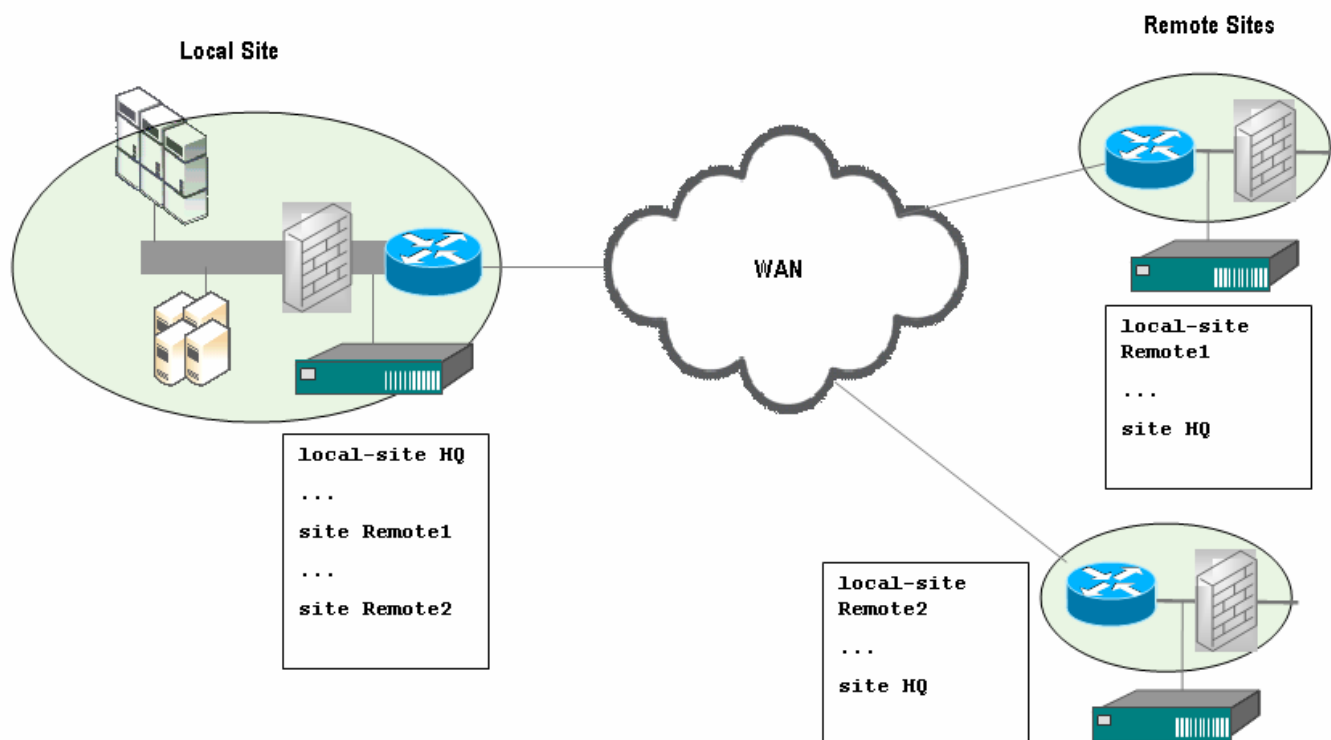


So if you want to view EQ results for both directions of the end-to-end link, you need to configure the remote BQM manually. If full PNQM results with EQ results for the outbound direction only are sufficient, then you can use PNQM auto-configuration mode.

Guidelines for Manual Configuration

This section provides guidelines for manually generating a valid configuration for a remote BQM given an existing local BQM configuration.

To get a manual PNQM configuration to work, you must provide a configuration on the remote BQM that exactly 'mirrors' the local BQM configuration.

Figure 8-3 Manual Remote BQM Configuration Based on Local Configuration

As illustrated in the preceding figure The local site in the local BQM configuration becomes a remote site in each remote BQM configuration. Likewise, remote sites in the local BQM configuration become local sites in each remote BQM configuration.

In general, router and interface names and attributes, including nso-maps and associated attributes, policy-map names and attributes and class-map names and match rules all remain the same when translating a configuration from the perspective of the remote BQM. There are some potential exceptions for match rules where packet remarking occurs in the service provider network and these are noted in the following table.

The following table lists all BQM CLI commands that must be copied **exactly** or instead must be revised when putting together the configuration for each remote BQM.

Table 8-7: Manual Remote BQM Configuration Guidelines

CLI Command	Context	Action
bandwidth	config-cmap	copy verbatim
class-adjust	config-pmap-c	copy verbatim
class-map	config	copy verbatim
custom-application	config	copy verbatim
interface	config-local-site-router	copy verbatim
interface	config-site-router	copy verbatim
link-adjust	config-site-router-if	copy verbatim
match	config-cmap	copy verbatim
match	config-custom-app	copy verbatim
match any	config-cmap	copy verbatim
match application	config-cmap	copy verbatim
match class-map	config-cmap	copy verbatim

match ethertype	config-cmap	copy verbatim
match ip.*{precedence dscp tos}	config-cmap	copy verbatim NOTE: match ip precedence, dscp and tos may not be valid if remarking occurs
match ip <other>	config-cmap	copy verbatim
match mpls	config-cmap	copy verbatim
match tcp.*{precedence dscp tos}	config-cmap	copy verbatim NOTE: match tcp precedence, dscp and tos may not be valid if remarking occurs
match tcp <other>	config-cmap	copy verbatim
match udp.*{precedence dscp tos}	config-cmap	copy verbatim NOTE: match udp precedence, dscp and tos may not be valid if remarking occurs
match udp <other>	config-cmap	copy verbatim
match vlan	config-cmap	copy verbatim
max-reserved-bandwidth	config-local-site-router-if	copy verbatim
max-reserved-bandwidth	config-local-site-router-pif	copy verbatim
max-reserved-bandwidth	config-site-router-if	copy verbatim
max-reserved-bandwidth	config-site-router-pif	copy verbatim
measure-bandwidth	config-nso-map	copy verbatim
measure-eq	config-nso-map	copy verbatim
measure-icmp	config-nso-map	copy verbatim
measure-microburst	config-nso-map	copy verbatim
measure-pnqm	config-nso-map	copy verbatim
nso-map	config	copy verbatim
one-way-latency	config-nso-map	copy verbatim
peer-interface	config-local-site-router	copy verbatim
peer-interface	config-site-router	copy verbatim
policy-map	config	copy verbatim
priority	config-pmap-c	copy verbatim
priority-level	config-pmap-c	copy verbatim
protect-packets	config-nso-map	copy verbatim
queue-limit	config-pmap-c	copy verbatim
queuing-targets	config-nso-map	copy verbatim
router	config-local-site	copy verbatim
router	config-site	copy verbatim
subnet	config-site	copy verbatim
subnet-filtering	config-site-router-if	copy verbatim
subnet-filtering	config-site-router-pif	copy verbatim
trace-events	config-pmap	copy verbatim
class	config-pmap	copy verbatim + copy referenced class-map
nso	config-pmap	copy verbatim + copy referenced nso-map
nso	config-pmap-c	copy verbatim + copy referenced nso-map
service-policy	config-local-site-router-if	copy verbatim + copy referenced policy-map

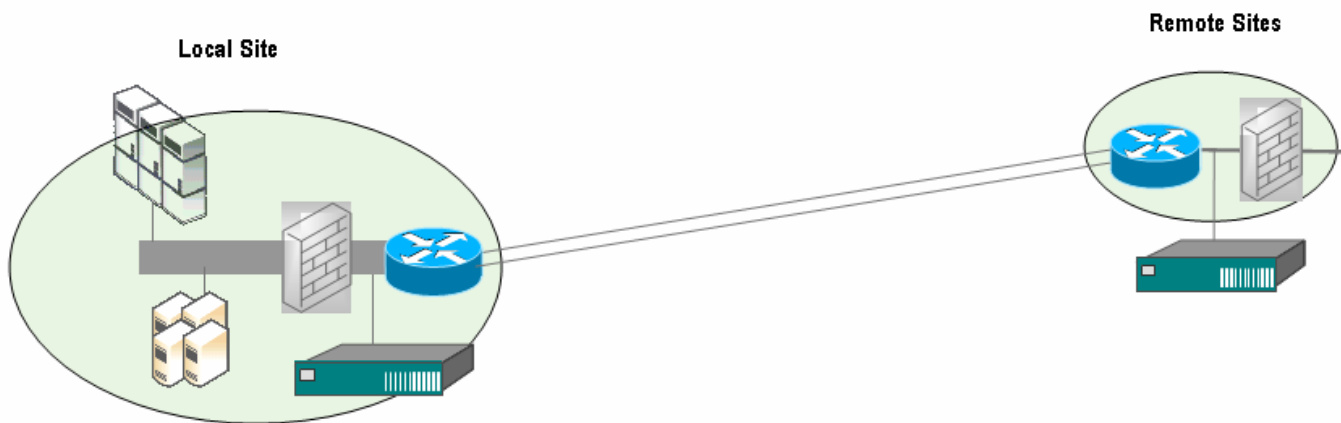
service-policy	config-local-site-router-pif	copy verbatim + copy referenced policy-map
service-policy	config-site-router-if	copy verbatim + copy referenced policy-map
service-policy	config-site-router-pif	copy verbatim + copy referenced policy-map
connects-to	config-site-router-if	form appropriate reverse connects-to command for the former local-site
attached-port	config-site-router	copy verbatim
filter-class	config-site-router-if	copy verbatim, and copy referenced class-map
site	config	replace site <name> with local-site <name>
local-site	config	replace local-site <name> with site <name>

Configuration Examples

The following example shows how a remote BQM configuration is derived from a local BQM configuration:

Local BQM Configuration:	Corresponding Remote BQM Configuration:
<pre> ! custom apps custom-application "CA-GOOGLE" match application HTTP url=*.google.* custom-application "CA-AMAZON" match application HTTP url=*.amazon.* ! class maps class-map match-any "MATCH-GOOGLE" match application "CA-GOOGLE" class-map match-any "MATCH-AMAZON" match application "CA-AMAZON" ! policy maps policy-map "HQ-P1" class "MATCH-GOOGLE" policy-map "ELY-P1" class "MATCH-AMAZON" policy-map "HOBART-P1" class "MATCH-AMAZON" ! ! local-site local-site "HQ" router "ROUTER-ELY" interface "ELY-Serial0/1" service-policy output "HQ-P1" ! ! remote branch site, direct connect site "ELY" router "ROUTER-DEFAULT" interface "Serial0/1" service-policy output "ELY-P1" pnqm-server 192.168.2.4 connects-to "HQ" "ROUTER-ELY" "ELY-Serial0/1" ! ! remote branch site, no BQM installed site "HOBART" router "HOBART-ROUTER" interface "SerialA" service-policy output "HOBART-P1" peer-interface "SerialA" </pre>	<pre> ! custom apps custom-application "CA-GOOGLE" match application HTTP url=*.google.* custom-application "CA-AMAZON" match application HTTP url=*.amazon.* ! class maps class-map match-any "MATCH-GOOGLE" match application "CA-GOOGLE" class-map match-any "MATCH-AMAZON" match application "CA-AMAZON" ! policy maps policy-map "HQ-P1" class "MATCH-GOOGLE" policy-map "ELY-P1" class "MATCH-AMAZON" ! ! policy-map "HOBART-P1" is not included since not referenced !rename local-site "ELY" local-site "ELY" router "ROUTER-DEFAULT" interface "Serial0/1" service-policy output "ELY-P1" site "HQ" router "ROUTER-ELY" interface "ELY-Serial0/1" service-policy output "HQ-P1" pnqm-server 10.4.2.12 connects-to "ELY" "ROUTER-DEFAULT" "Serial0/1" ! remote site "HOBART " is not included since there is no BQM installed there for PNQM measurement. </pre>

Figure 8-4 ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Two Directly Connected Interfaces



The following shows an example local site and remote site configuration when there are two directly-connected interfaces:

Local Site Configuration	Remote Site Manual Configuration
<pre> class-map match-any North_Out match ip dst=192.168.1.1 class-map match-any South_Out match ip dst=192.168.1.2 class-map match-any North_In match ip src=192.168.1.1 class-map match-any South_In match ip src=192.168.1.2 local-site Local-site router core1 interface Serial0/1 bandwidth 512 filter-class North_Out no subnet-filtering interface Serial0/2 bandwidth 512 filter-class South_Out no subnet-filtering remote-site RemoteSite1 router remotel interface Serial0/1 bandwidth 512 filter-class North_In no subnet-filtering connects-to Local-site core1 interface Serial0/2 bandwidth 512 filter-class South_In no subnet-filtering connects-to Local-site core1 </pre>	<pre> class-map match-any North_Out match ip dst=192.168.1.1 class-map match-any South_Out match ip dst=192.168.1.2 class-map match-any North_In match ip dst=192.168.5.1 class-map match-any South_In match ip dst=192.168.5.2 local-site Local-site router remotel interface Serial0/1 bandwidth 512 filter-class North_In interface Y2 bandwidth 512 filter-class South_In remote-site Remote_LocalSite router core1 interface Serial0/1 bandwidth 512 filter-class North_Out connects-to Local-site remotel interface Serial0/2 bandwidth 512 filter-class South_Out connects-to Local-site remotel </pre>

Configuring Manual PNQM - Example Scenario

The following example scenario describes how to set up local and remote BQM appliances for manual PNQM configuration. In this example, the MPLS VPN network consists of 50 sites and a single data center with a multi-class configuration consisting of a voice class, data class and class-default.

We want to measure PNQM, Corvil Bandwidth, and in particular we want to see Expected Queuing results for both directions of traffic for remote sites also deployed with BQM.

The data center BQM appliance includes the following configuration:

- PNQM measurements enabled in the network service objectives for each class
- Sampling is set to all in the voice class network service objective and 4 pps for each of the other classes
- PNQM IP addresses are configured for all remote BQM appliances
- Manual PNQM mode is specified
- The sampling rate is initially set to all packets on the interface, which overrides the network service objective per-class sampling rate to enable misclassification detection to help troubleshoot any potential issues with the configuration



Note In general, you should check the missing flows count. If the reported value is significant then you configure misclassification detection to help identify the problem.

Misclassification may be caused by a straightforward mis-configuration or configuration change on either BQM appliance.

Alternatively, the issue may be because of remarking of packets by some intermediate router. This remarking may be static, in the sense that all packets from a certain source are remarked by the router(s). The remarking may also be dynamic, for example, by a policer on an intermediate router or routers, depending on traffic conditions.

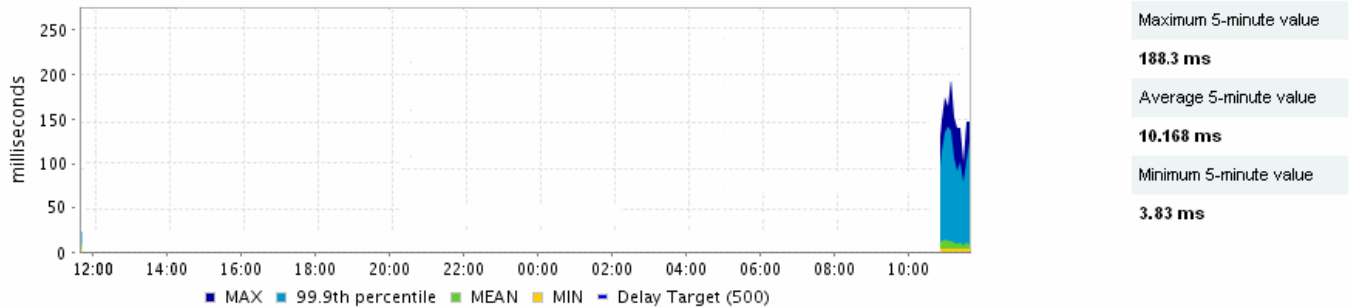
We use the PNQM manual configuration guidelines described in the preceding section to define the configurations for each remote BQM. The configurations are loaded onto each BQM and after five minutes we can examine the first PNQM results in each class for any of the remote sites.

In this example scenario the PNQM results are initially empty for both the voice and data class on all the sites with the GUI showing very high misclassification results.

Figure 8-5 Misclassification Results Reported in GUI

PNQM: Availability 100%, 11231 misclassified packets.

End to End Measured Delay ?



To view details on the misclassification results, the we use the CLI **show interfaces * pnqm** command:

```
host(config)# show interfaces * pnqm
site nyc
  router rtr
    interface ve0
      bandwidth 2500
      max-reserved-bandwidth 75
      subnet-filtering
      ping-address 192.168.2.85
      peer-interface dc rtr ve0
      pnqm-server 192.168.5.68
      service-policy output default
      Traffic Stats - 1000 bps mean, 58 Kbps 1s peak, 167 Kbps 5ms peak
                    - 67 Kbps 50ms peak (configured)
                    - 351 packets, 18,452 bytes
      PNQM Stats - 18992 packets sampled, 0 lost (0.00%), 10032 in
missing flows, 11231 misclassified
.
.
.
```

PNQM class mismatch:

Source	Destination	Prot	TOS	Local	Remote
10.1.0.2:35956	10.10.10.2:11200	tcp	46	voice	class-
default					
10.1.0.2:35956	10.10.10.2:11200	tcp	46	voice	class-
default					
10.1.0.2:35956	10.10.10.2:11200	tcp	46	voice	class-
default					
10.1.0.2:35956	10.10.10.2:11200	tcp	46	voice	class-
default					
10.1.0.2:35956	10.10.10.2:11200	tcp	46	voice	class-
default					

Using the Command Line Interface (CLI)

10.1.0.2:35956 default	10.10.10.2:11200	tcp	46	voice	class-
10.1.0.2:35956 default	10.10.10.2:11200	tcp	10	video	class-
10.1.0.2:35956 default	10.10.10.2:11200	tcp	10	video	class-
10.1.0.2:35956 default	10.10.10.2:11200	tcp	10	video	class-
10.1.0.2:35956 default	10.10.10.2:11200	tcp	10	video	class-

The summary results indicated the number of misclassified packets. Below the results for the individual classes, there is information showing the 6-tuple results for that last ten packets that have been misclassified. The information on these packets is from the point of view of the local BQM (that is, the one on which you are viewing the information.) In particular, the first five columns show information collected for each packet at the local BQM appliance. The class name displayed in the Remote column shows the class into which the remote BQM appliance put the misclassified packet.



Note Depending on the respective configurations on the remote BQM and the router it is monitoring, this may not necessarily be the same as the class into which the router put the packet.

In the example shown above, it may be that the router puts the remarked packets into a different class rather than class-default. In this example, the BQM configuration dictates that these packets are put in class-default on the BQM appliance.

In the example shown here, the TOS field for the misclassified packets in the voice class is shown as dscp=ef (dscp=46) and for the video class is dscp=af11 (dscp=10). So the class match rules for these classes are using IP precedence values but the packets have been remarked for the service provider.

The next task is to modify these match rules for all the remote BQM configuration files. The remote BQM appliances are then reloaded with the new configuration files using the **copy tftp://[hostname|A.B.C.D]/<filename> config** command:

```
host(config)$ copy tftp://192.168.17.3/cfg/ldn_branch.cfg config
```

After another five minutes we start examining the PNQM results for various sites. All results are now being reported with no misclassification. The system is left to run for a few hours and later in the day we use the CLI **show** command to scan the misclassification results for all the classes on all the sites.

```
class video
  Traffic Stats - 89 Kbps mean, 292 Kbps 1s peak, 378 Kbps 5ms
peak
                - 291 Kbps Corvil Bandwidth
                - 303 Kbps 50ms peak (configured)
                - 292 Kbps 600ms peak (delay-target)
                - 46,201 packets, 10,903,436 bytes
  PNQM Stats - 46201 packets sampled, 0 lost (0.00%), 0 in
                missing flows, 0 misclassified
```

```

class voice
  Traffic Stats - 868 Kbps mean, 1840 Kbps 1s peak, 2049 Kbps 5ms
peak
- 2801 Kbps Corvil Bandwidth
- 2983 Kbps 50ms peak (configured)
- 2772 Kbps 600ms peak (delay-target)
- 398,407 packets, 87,723,202 bytes
  PNQM Stats - 462045 packets sampled, 0 lost (0.00%), 0 in
missing flows, 0 misclassified

class class-default
  Traffic Stats - 1000 bps mean, 4 Kbps 1s peak, 290 Kbps 5ms
peak
- 5 Kbps Corvil Bandwidth
- 29 Kbps 50ms peak (configured)
- 8 Kbps 500ms peak (delay-target)
- 30 packets, 2,109 bytes
  PNQM Stats - 30 packets sampled, 0 lost (0.00%), 0 in
missing flows, 0 misclassified

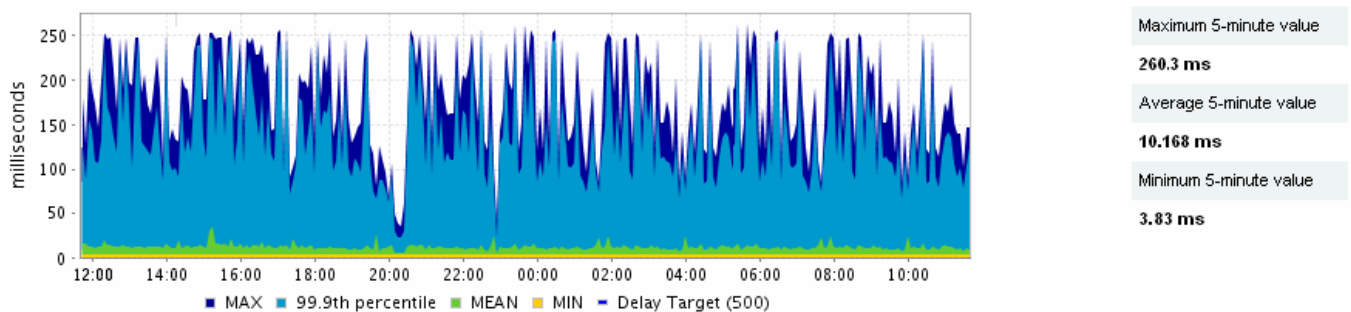
```

No misclassification is now being reported so the data center PNQM configuration is modified so that the interface sampling rate is disabled and the sampling rates set back to those specified in the relevant network service objectives. To do this from the GUI we edit each interface and select **Use class sample rate from NSO map**. From the CLI we edit each interface and use the **pnqm-server** command without specifying a sampling override rate.

The system in this example, is now operating correctly and we can view PNQM results alongside Expected Queuing results for both directions of traffic.

Figure 8-6 Expected Queuing Results from Remote BQM

Expected Queuing Delay (data retrieved from remote BQM 192.168.11.12) ?



In this example, the data for the Expected Queuing Latency graph is successfully retrieved from the manually configured remote BQM and displayed in the GUI on the local BQM. Data for the other Expected Queuing graphs is also retrieved and displayed.

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
```

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 separate text editor, save it with the `.cfg` file extension and copy it to the appliance to become the current configuration. In the following example, the file is copied from a tftp server:

```
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 appliance when logged in as either the admin or config users.

Default BQM Configuration

The following section lists the default configuration of network service objectives, class-maps, policy-maps, sites, routers, and interfaces present on the BQM when first installed. The list represents the set of CLI commands required to re-establish any of the objects in the default configuration, if necessary.

```
class-map class-default
  match any
class-map unknown-applications
  match application Unknown
nso-map high-speed
  measure-microburst milliseconds 20
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 50
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
nso-map low-latency
  measure-microburst milliseconds 10
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 5
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
nso-map low-speed
  measure-microburst milliseconds 100
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period minutes 5
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
  one-way-latency milliseconds 750
  measure-pnqm packets-per-second 10 event-thresholds latency latency-variation loss
nso-map network-service-objective-default
  measure-microburst milliseconds 50
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
  protect-packets percent 99.90000 busy-period hours 4
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-icmp interval-milliseconds 10000 size 36 event-thresholds delay loss
  one-way-latency milliseconds 500
  measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
nso-map real-time
  measure-microburst milliseconds 10
  queuing-targets delay-milliseconds use-one-way protect-packets use-one-way
```

```
protect-packets percent 99.90000 busy-period minutes 5
measure-eq event-thresholds delay loss
measure-bandwidth event-threshold percent 100
measure-icmp interval-milliseconds 1000 size 40 event-thresholds delay loss
one-way-latency milliseconds 120 variation milliseconds 30
measure-pnqm packets-per-second 100 event-thresholds latency latency-variation loss
policy-map default
  nso network-service-objective-default
  trace-events
  class class-default
    nso network-service-objective-default
    queue-limit 64
local-site Local-site
  description "site in which BQM is deployed"
  router bqm
    interface PortA
      attached-port PortA
      bandwidth 1000000
      max-reserved-bandwidth 75
      no subnet-filtering
      service-policy output default
    interface PortAB
      bandwidth 2000000
      max-reserved-bandwidth 75
      no subnet-filtering
      service-policy output default
    interface PortB
      attached-port PortB
      bandwidth 1000000
      max-reserved-bandwidth 75
      no subnet-filtering
      service-policy output default
    interface "Unknown Applications"
      bandwidth 1000000
      max-reserved-bandwidth 75
      no subnet-filtering
      filter-class unknown-applications
      service-policy output default
  router default
    interface default
      bandwidth 2000000
      max-reserved-bandwidth 75
      subnet-filtering
      service-policy output default
    peer-interface default
      bandwidth 2000000
      max-reserved-bandwidth 75
      subnet-filtering
      service-policy output default
site "Unmatched Traffic"
  description "Unmatched traffic"
  subnet unmatched-remote
  router default
    interface default
      bandwidth 1000000
      max-reserved-bandwidth 75
      subnet-filtering
      service-policy output default
    peer-interface default
      bandwidth 1000000
      max-reserved-bandwidth 75
      subnet-filtering
      service-policy output default
```

For more information on using any of these commands, see the “Command Reference” section of this document.

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.

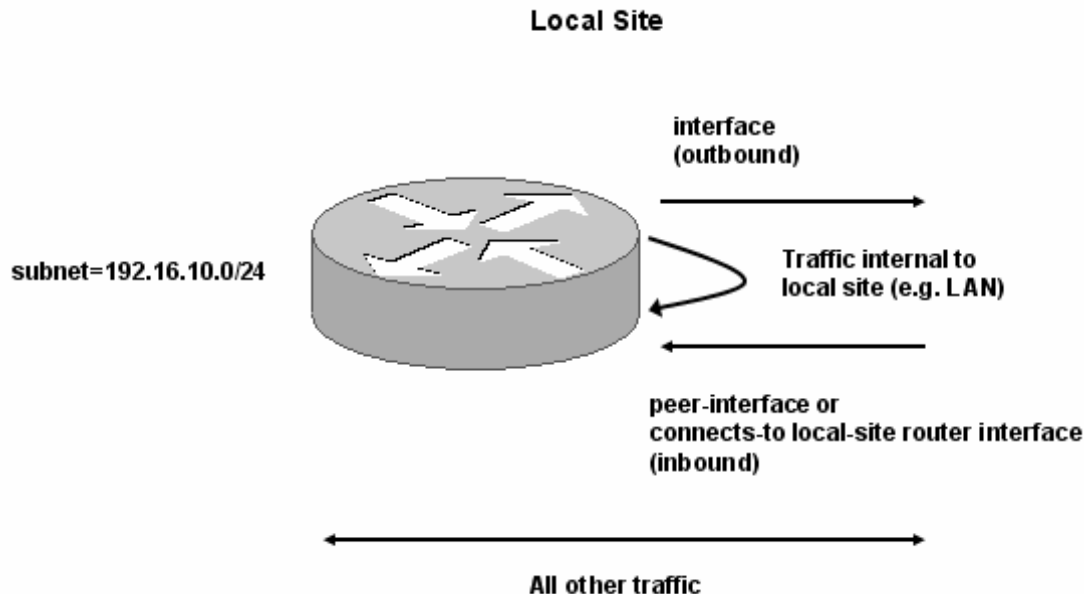
Defining sites with subnets is optional in the BQM configuration. Using **no subnet-filtering** indicates that you intend to ignore site subnets when matching traffic. So this is used when you are

- using the **attached-ports** command to establish traffic filtering with the physical Cisco ADE 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

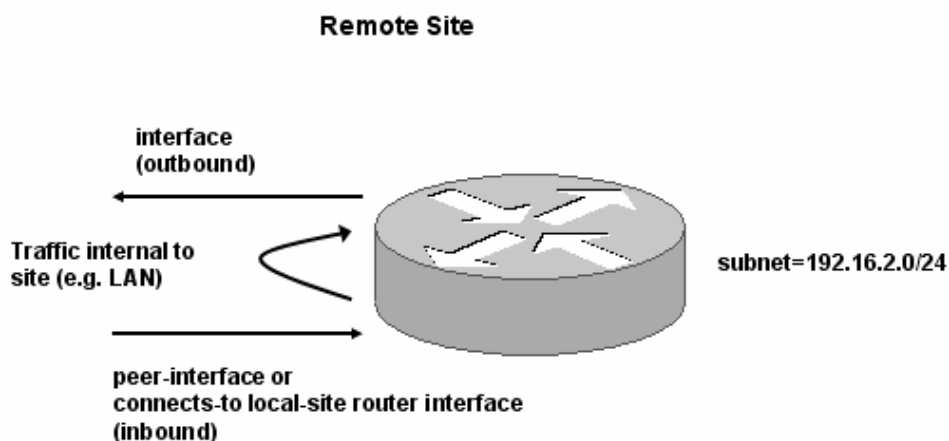
The use of the Cisco ADE physical ports (such as PortA, PortB and so on) in the default first day of service configuration requires subnet filtering to be explicitly disabled. So the default BQM configuration includes a **no subnet-filtering** command on each relevant interface. Note that the default 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 8-7 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 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.

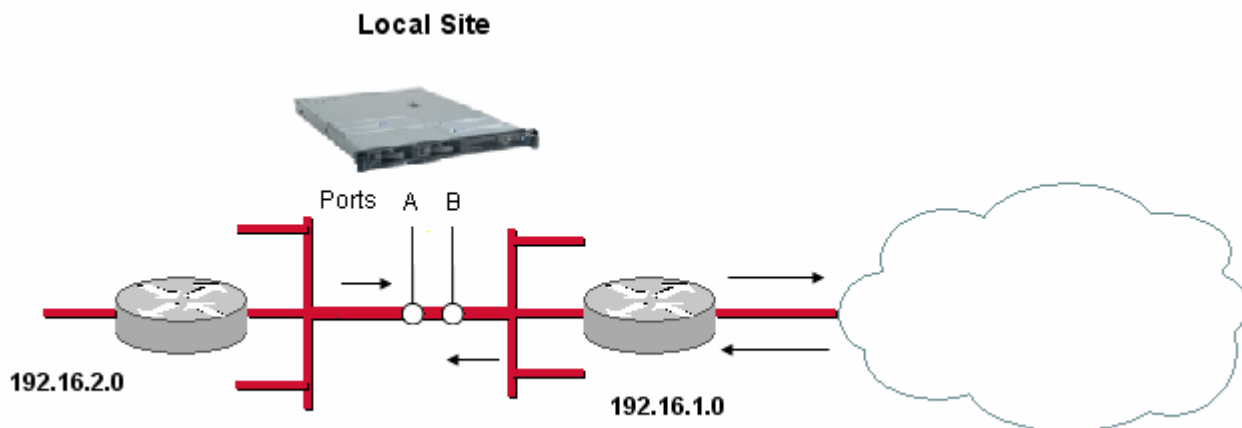
Figure 8-8 Subnet Filtering – Exclude Local Traffic

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, 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 physical port PortA is used to measure outbound traffic and PortB is used to measure inbound traffic:

Figure 8-9 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 mpls tags
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 mpls tags
```

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.

Viewing CLI Results

When you completed BQM configuration, you can view selected results on the CLI using the **show** command. To view results for a specific interface, you use the **show interface** command:

```
show interface <site> <router> <interface> [ { pnqm [class <class>] } |
{ [ stats [class <class>] [top <n>]
[applications|conversations|listeners|talkers]
[ascending|descending] } ]
```

You specify a particular interface by qualifying it with the site and router names. As well as the configuration details for that interface, the CLI also displays summary traffic, PNQM, and ICMP statistics, assuming they are enabled. All values displayed are cumulative since the last time the statistics counters were cleared (using the **clear counters** command, or due to a reboot or a configuration change.)

```

host(config)# show interface nyc rtr ve0
site nyc
  router rtr
    interface ve0
      bandwidth 2500
      max-reserved-bandwidth 75
      subnet-filtering
      ping-address 192.168.2.85
      connects-to sj rtr ve0
      pnqm-server 192.168.2.68
      filter-class nyc.out
      service-policy output default
        Traffic Stats - 1000 bps mean, 12 Kbps 1s peak, 167 Kbps 5ms peak
                      - 58 Kbps 50ms peak (configured)
                      - 122,767 packets, 6,387,484 bytes
        PNQM Stats   - 48050 packets sampled, 3 lost (0.01%), 0 in
missing flows
      class class-default
        Traffic Stats - 1000 bps mean, 12 Kbps 1s peak, 167 Kbps 5ms
peak
                      - Corvil Bandwidth not configured
                      - 58 Kbps 50ms peak (configured)
                      - 24 Kbps 500ms peak (delay-target)
                      - 122,767 packets, 6,387,484 bytes
        PNQM Stats   - 48050 packets sampled, 3 lost (0.01%), 0 in
missing flows
        ICMP monitoring - 9691 packets sent, 0 lost (0.00%)

```

In the example shown here you can see the traffic statistics reported includes the mean, one-second peak and 5-millisecond peak values measured for the traffic. The traffic statistics also include the user-specified millisecond peak rate, as configured in the network service objective, as well as the packet and byte counts.

The displayed summary PNQM statistics include the number of packets for which PNQM latency and loss measurements have been made, along with the number of packets lost and those attributed to missing flows, that is, flows that were detected by a BQM appliance at one end of the PNQM channel, but not at the other. The results are also displayed for each class on the interface. In the example shown here, there is a single-class configuration showing class-default.

The interface-level ICMP monitoring results display the number of ICMP responder packets sent and the number lost.

You can use the **show interface <site> <router><interface> pnqm** command to view more PNQM information for the interface and all its classes, or in a multiclass configuration, you can specify a particular class name.

```

!
.
class class-default
  Traffic Stats - 0 bps mean, 8 Kbps 1s peak, 120 Kbps 5ms peak
                - 101 Kbps Corvil Bandwidth
                - 47 Kbps 50ms peak (configured)
                - 15 Kbps 500ms peak (delay-target)
                - 136,048 packets, 7,078,696 bytes
  PNQM Stats   - 53112 packets sampled, 4 lost (0.01%), 0 in
missing flows
                - PNQM availability: 100%
                - 10.956 ms min, 11.992 ms mean, 13.774 ms max

```

```

(0.129 ms max error)
- Channel status: OK
- 53112 signature lookups (4 failures),
current sample rate: 1-in-2
- attempting sample rate change to: 1-in-1
- src: 172.18.2.68:5100,
  rt-class/branch1/bl-r/bl-
r.ve0/output/class-default
- OK, received 10 signatures in
778.866451 seconds (0.01 sigs/sec)
- 0.000% hash collisions, 0 signatures in
  history
- dest: 127.0.0.1:5100,
  rt-class/branch1/bl-r/bl-
r.ve0/output/class-default
- OK, received 10 signatures in
782.570943
seconds (0.01 sigs/sec)
- 0.000% hash collisions, 0 signatures
in
  history
- internal clock stats: o=-81.637s
o_err=0.000s
  skew=-0.000138334 maxdrift=1.23372e-06
- Reverse Channel:
  rt-class/server-
1/cloudrtr/cloudrtr.ve0/output/class-default

```

As well as the summary statistics displayed in the general case, you now get an indication of PNQM availability. The displayed percentage represents the proportion of time since the statistics were last cleared that PNQM measurement has been operating successfully.



Note If GPS is configured for the system, there is also a similar indication of GPS availability.

The next results displayed are the maximum, mean and minimum end-to-end measured latency results in milliseconds. The maximum calculated error on these results is also displayed. This figure is usually small but because of the cumulative nature of the displayed results, early peaks in the error value when the system is started may persist and therefore be misleading when compared to the other values.

The channel status is displayed as OK as long as PNQM measurement is operating successfully. The status is shown as Down if there is a problem with the channel, usually because of either a connectivity issue or a configuration mis-match between the two BQM appliances.

The signature lookups reflect the number of packets that have been processed, along with the count of lookup failures. The displayed current sampling rate shows the one-in-N sampling rate that the system is using to most closely match the configured packets-per-second sampling rate. Depending on the changing traffic patterns on the network, the system may detect a significant difference between these rates, in which case a message is displayed here indicating that the system is attempting to change the one-in-N sampling rate to a rate that more closely reflects the current packets per second rate. The system will attempt a similar correction if a significant different in rates is detected between the two endpoints of the PNQM channel.

The remaining information is largely for debugging purposes for support and covers the internal system definition of the PNQM channel endpoints and internal clocking statistics.



Note If you are using PNQM auto-configuration mode the detailed PNQM results are presented at the interface level as opposed to the class level.

Alternatively, you can use **show interface** *<site>* *<router>* *<interface>* **stats** to view top applications, conversations, listeners, or talkers results. You can also choose to view these results for a particular class on the interface. To see results for peer-interfaces in PVN deployments, you use the **show peer-interface** command.

To view results for all interfaces, or for all interfaces with the given name, you use the **show interfaces** command:

```
show interfaces [<name> [*]] [ { pnqm [class <class>] } |
                             { [ stats [class <class>] [top <n>]
                               [applications|conversations|listeners|talkers]
                               [ascending|descending] } ]
```

To see the equivalent results for peer-interfaces in PVN deployments, you use the **show peer-interfaces** command.

Configuring Network Model Deployments with the CLI

This section describes how to take knowledge of the existing network design, which 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

Assuming that all the remote site traffic is to or from the local site, these network model deployments provide the full range of BQM measurements and results - PNQM, EQ (Inbound and Outbound), Corvil Bandwidth, Microburst and Top N - unless otherwise noted. Example configuration details are provided for the main network model deployment types. The following alternate network deployment scenarios, where BQM results may be impacted, are also outlined:

- MPLS VPN deployment with redundant local site connectivity
- MPLS VPN deployment with redundant remote site connectivity
- MPLS VPN deployment with any-to-any traffic
- MPLS VPN deployment with remote site internet traffic via local site
- MPLS VPN deployment with local site connected to remote site via two WANs
- Dual data center deployment
- Point-to-point across a firewall deployment



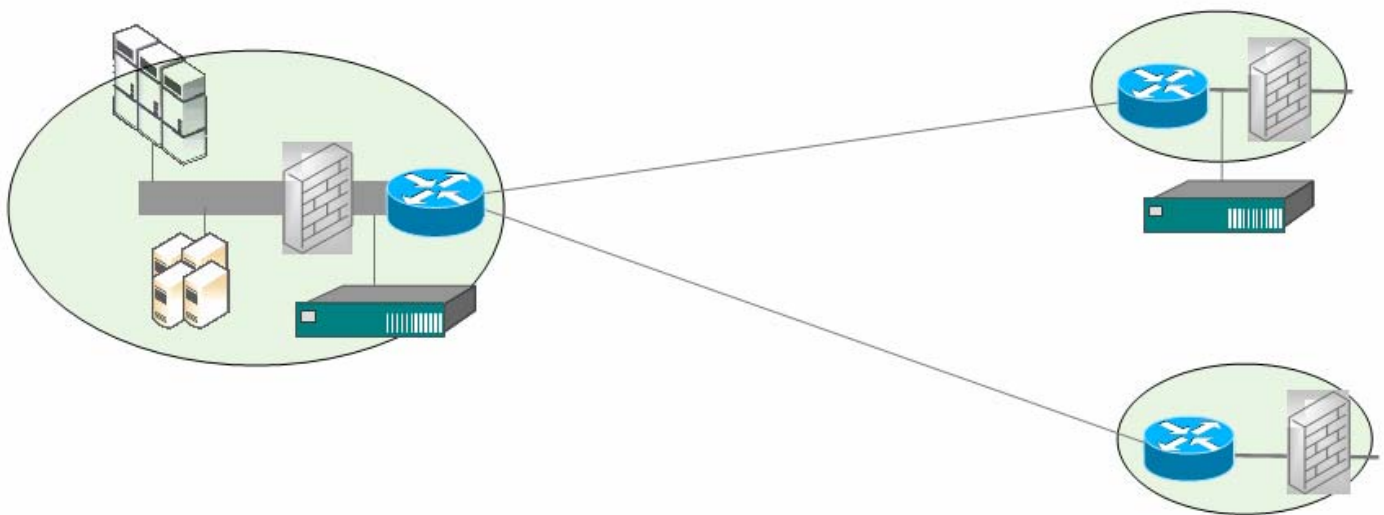
Note PNQM measurement is not supported in Network Address Translation (NAT) environments.

Expected Queuing and Corvil Bandwidth for pre-queuing interfaces and microburst are supported.

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

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' represents the physical installation site.

Figure 8-10 *Network Model - Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment*



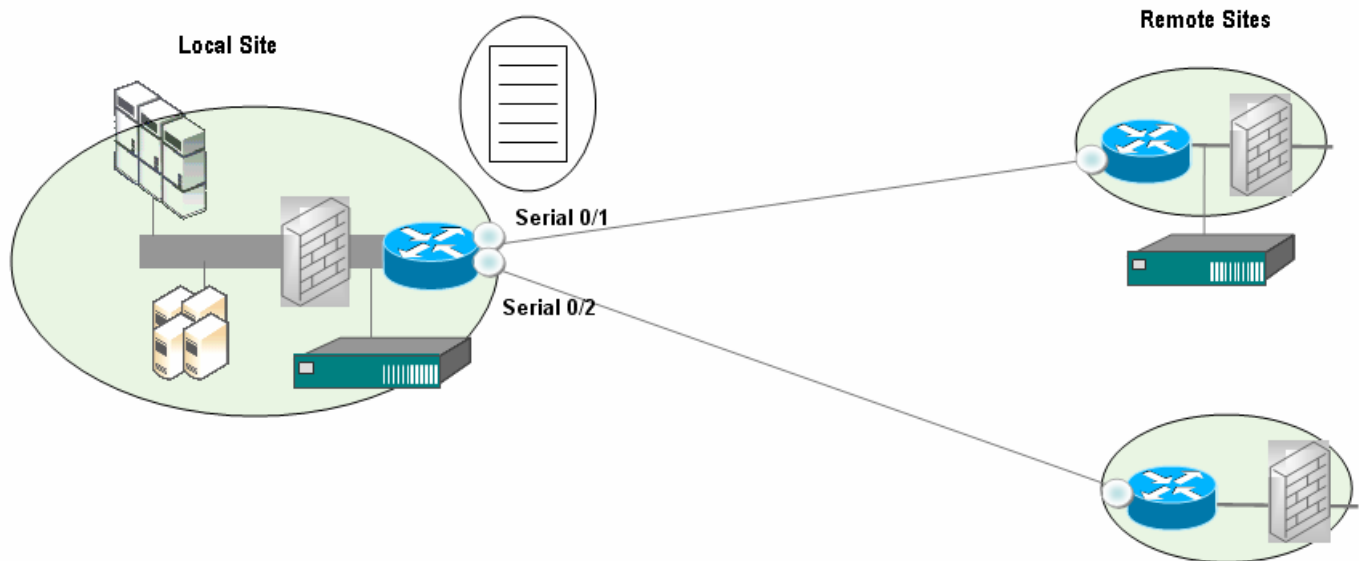
To configure the network model for this example deployment, you configure the following:

- Local site
 - Default site in model that contains a Cisco ADE; the name is editable
 - Subnet
 - Router
 - Interfaces specifying bandwidth configuration and policy-maps
- Remote Site with Cisco ADE installed for PNQM measurement
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map, address of Cisco ADE for PNQM measurement
- Remote Site (no Cisco ADE installed, no PNQM measurement)
 - Name
 - Subnet
 - Router
 - Interface with link to local site-router-interface, bandwidth, policy-map

In this example single-class configuration, we do not explicitly configure class-maps, policy-maps, or network service objectives. The system then uses the default class-map, policy-map and network service objective. Also we do not configure a BQM IP address for remote site interfaces for which PNQM measurement is not required.

When you define interfaces without explicitly defining a policy-map or network service objective, the default policy-map and therefore the default network service objective are automatically assigned to the interface. You can also define a policy-map and an associated (non-default) network service objective, and apply them to a configured interface.

Figure 8-11 Basic 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:

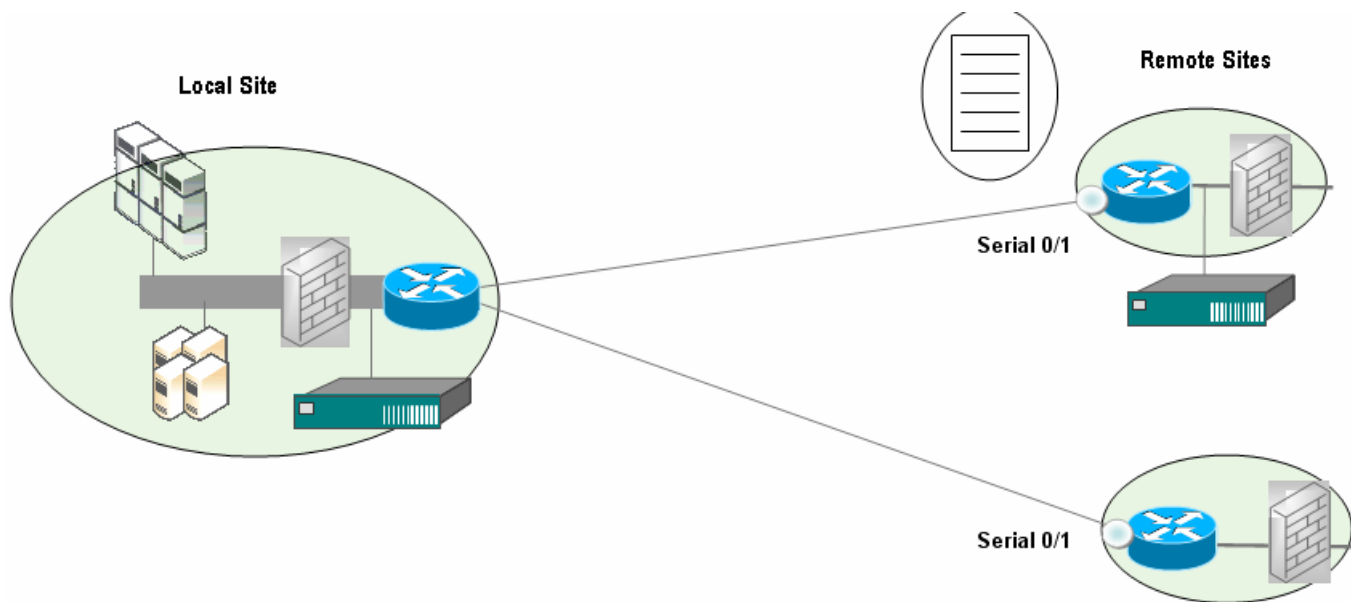
Step 1 Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and the local site router, named core1 has two interfaces, Serial0/1 and Serial0/2, with both connected to links of 512 kbps:

```
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-if)$ 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)$ interface Serial0/2
host(config-local-site-router-if)$ description "Link to Remote Site 2"
host(config-local-site-router-if)$ bandwidth 512
```

When you define interfaces without explicitly defining a policy-map or network service objective, the default policy-map and therefore the default network service objective are automatically assigned to the interface. If you have defined a policy-map and an associated

(non-default) network service objective, you can apply them to the interface at this point using the **service-policy output** *<policy-map name>* command.

Figure 8-12 Basic ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Remote Site Configuration



Step 2

Define the configuration remote sites with a Cisco ADE installed and requiring PNQM measurement. This remote site has its own subnet has a well-known ping address at 192.168.1.3 for ICMP measurement. The physical site represented by the remote site in the network model has a Cisco ADE installed and running BQM. In this example, the Cisco ADE has the following IP address: 192.168.1.2. PNQM measurement is effectively enabled at interface level using the **pnqm-server** command. This remote site has a site router, whose interface connection back to the 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)$ router remotel
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ ping-address 192.168.1.3
host(config-site-router-if)$ connects-to Local-site core1
Serial0/1
```




Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” for guidelines on how to create a matching BQM configuration to enable PNQM measurement on a remote Cisco ADE given a certain configuration on the local Cisco ADE.

- Step 3** Define the configuration for remote sites without a Cisco ADE installed. In this example, the remote site has its own subnet, a well-known ping address at 192.168.1.3 for ICMP measurements, and a site router, whose interface connections back to the local site interface is made explicit in the configuration using the **connects-to** command:

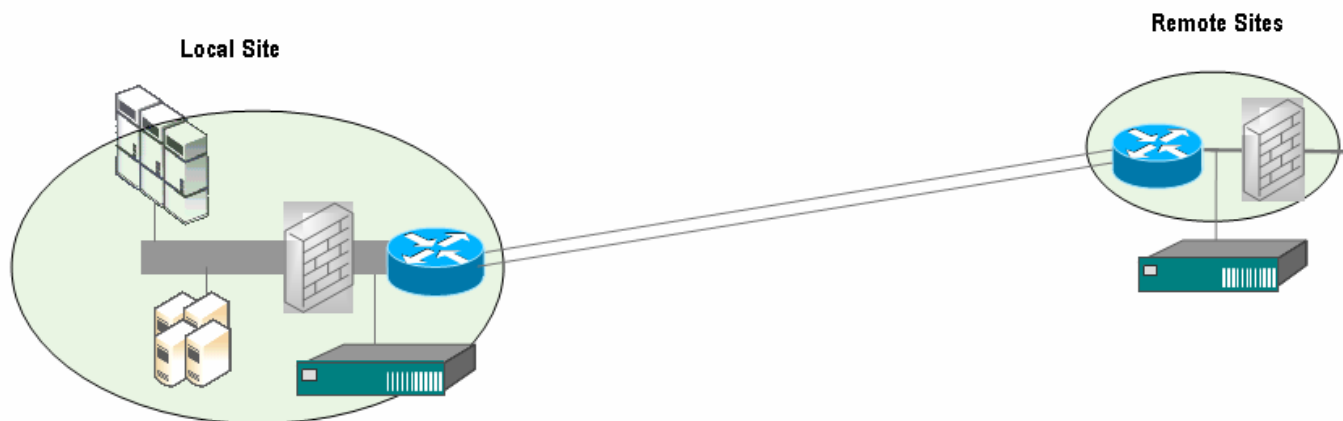
```
host(config-site-router-if)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
host(config-site)$ router remote2
host(config-site-router)$ interface Serial0/1
host(config-site-router-if)$ description "Link to Local Site"
host(config-site-router-if)$ bandwidth 512
host(config-site-router-if)$ connects-to Local-site core1
Serial0/2
```

- Step 4** Check the configuration with the **show config** command:

- Step 5** When you have satisfied with the configuration, you can save your changes. To back up the new configuration, you use the copy command:

```
host(config)$ copy config
```

If there are two interface connections between the local site and a remote site, you must model the separate remote site interfaces using filter classes and disable subnet filtering with the **no subnet-filtering** command. For more information on subnet filtering and filter classes, see the sections “Working with Subnet Filtering” and “Using Filter Classes.”

Figure 8-13 Configuring the Network Model for Two Directly Connected Interfaces

The following shows an example configuration when there are two directly connected interfaces between a local and remote site where each has a Cisco ADE installed for PNQM measurement. For automatic PNQM configuration to work, you must model the remote interfaces as two separate sites, each defined by subnets:

```
!
class-map match-any North_Out
  match ip dst=10.1.20.1
class-map match-any North_In
  match ip src=10.1.20.1
!
!
local-site Local-site
  router core1
    interface Serial0/1
      bandwidth 512
    interface Serial0/2
      bandwidth 512
    interface Serial1/0
      bandwidth 512
      filter-class North_Out
      no subnet-filtering

remote-site RemoteSite1a
  subnet 192.168.1.1
  router remotel
    interface Serial0/1
      bandwidth 512
      connects-to Local-site core1 Serial0/1
      pnqm-server 192.168.1.3 autoconf

remote-site RemoteSite1b
  subnet 192.168.1.2
  router remotel
    interface Serial0/2
      bandwidth 512
      connects-to Local-site core1 Serial0/2
      pnqm-server 192.168.1.3 autoconf
```

For remote sites for which there is no Cisco ADE installed and no PNQM measurement is required, you use filter classes to identify the traffic for each interface and turn off subnet filtering:

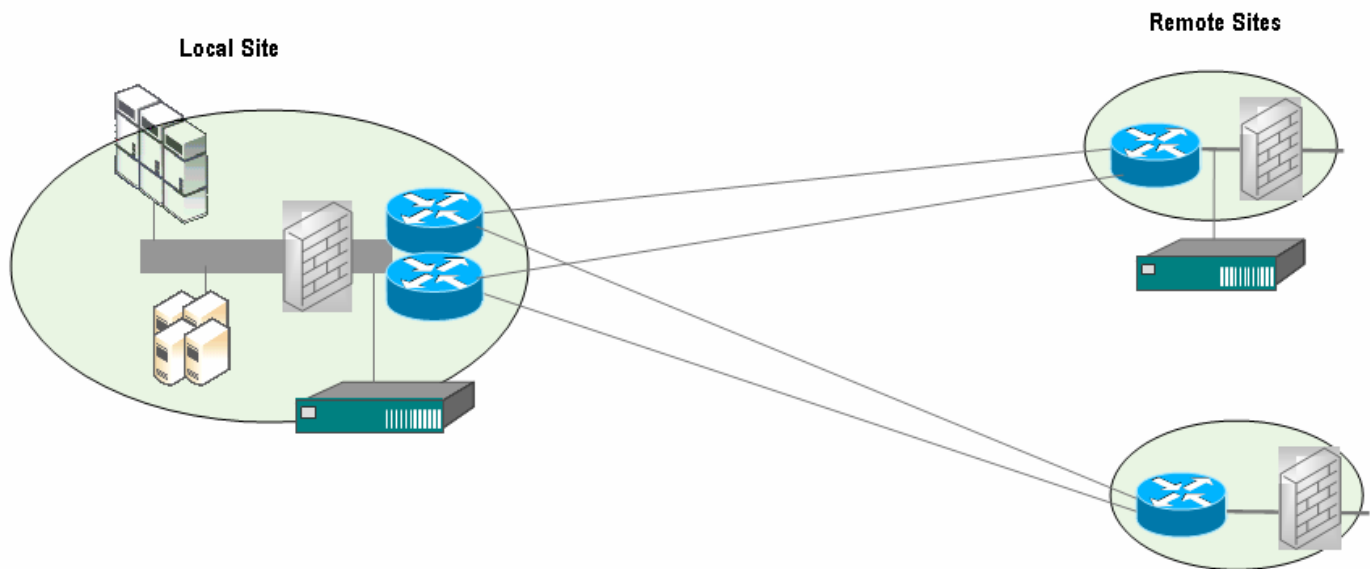
```
remote-site RemoteSite2
router remote2
interface Serial0/1
bandwidth 512
filter-class North_In
no subnet-filtering
connects-to Local-site core1 Serial1/0

!
```

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

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. For PNQM measurement, another Cisco ADE is installed at the relevant remote site. All measurements are made and viewed from the perspective of the local site. Each local site router must be bound to specific physical measurement ports using the **attached-port** command.

Figure 8-14 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:

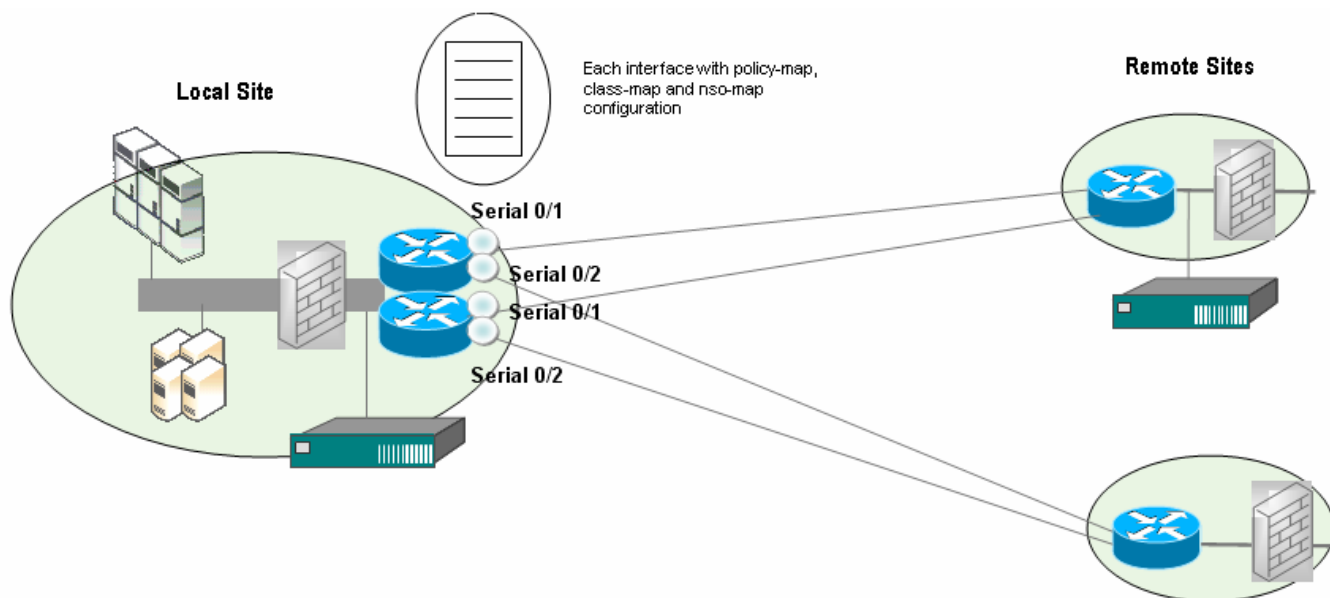
- Local site
 - Default site in model that contains a Cisco ADE; the name is editable
 - Subnet
 - Router
 - Two interfaces specifying bandwidth configuration and policy-maps
 - Mapping of physical measurement ports to routers

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

In this example single-class configuration, we do not explicitly configure class-maps, policy-maps, or network service objectives. The system then uses the default class-map, policy-map and network service objective. Also we do not configure a BQM IP address for remote site interfaces for which PNQM measurement is not required.

When you define interfaces without explicitly defining a policy-map or network service objective, the default policy-map and therefore the default network service objective are automatically assigned to the interface. You can also define a policy-map and an associated (non-default) network service objective, and apply them to a configured interface.

Figure 8-15 *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

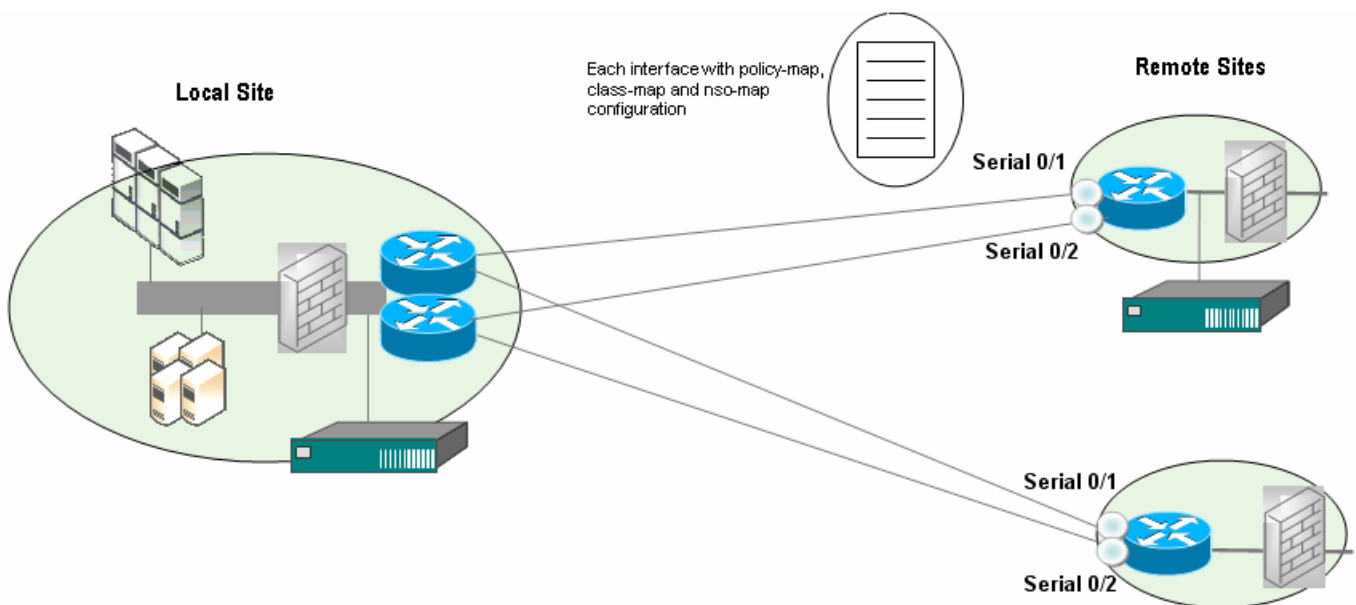
Define the local site details for the configuration. In this example, the local site has subnet 192.168.5.0/24 and two local site routers, named core1 and core2, each with two interfaces, Serial0/1 and Serial0/2, with all interfaces connected to links of 512 kbps and all using the FIFO policy-map. For this type of deployment, either a two or four-port Cisco ADE 2120 is required, so at least one physical measurement port is mapped to the core1 local site router, and at least one is 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)$ attached-port PortA
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)$ 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
host(config-local-site-router-if)$ router core2
host(config-local-site-router)$ attached-port PortB
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)$ 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 8-16 *Dual-homed ATM PVC, Frame Relay PVC, Metro Ethernet, Leased Line Deployment – Remote Site Configuration*



Step 2 Define the configuration for remote sites with a Cisco ADE installed and requiring PNQM measurement. This remote site has its own subnet has a well-known ping address at 192.168.1.3 for ICMP measurement. The physical site represented by the remote site in the network model has a Cisco ADE installed and running BQM. In this example, the Cisco ADE has the following IP address: 192.168.17.2. PNQM measurement is effectively enabled at interface level using the **pnqm-server** command. This remote site has a site router, whose interface connection back to the 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)$ router remotel
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ ping-address 192.168.1.3
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ ping-address 192.168.1.3
host(config-site-router-if)$ connects-to Local-site core2
Serial0/1

```



Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” for guidelines on how to create a matching BQM configuration to enable PNQM measurement on a remote Cisco ADE given a certain configuration on the local Cisco ADE.

PNQM results are restricted in this case to the aggregate of both links.

Step 3

Define the configuration for remote sites without a Cisco ADE installed. In this example, the remote site has its own subnet, a well-known ping address at 192.168.1.3 for ICMP measurements, and a site router, whose interface connections back to the local site interface is made explicit in the configuration using the **connects-to** command:

```

host(config-site-router-if)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
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)$ ping-address 192.168.2.3
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)$ ping-address 192.168.2.3
host(config-site-router-if)$ connects-to Local-site core2
Serial0/2
host(config-site-router-if)$

```

Step 4 Check the configuration with the **show config** command:

Step 5 When you have satisfied with the configuration, you can save your changes. To back up the new configuration, you use the copy command:

```

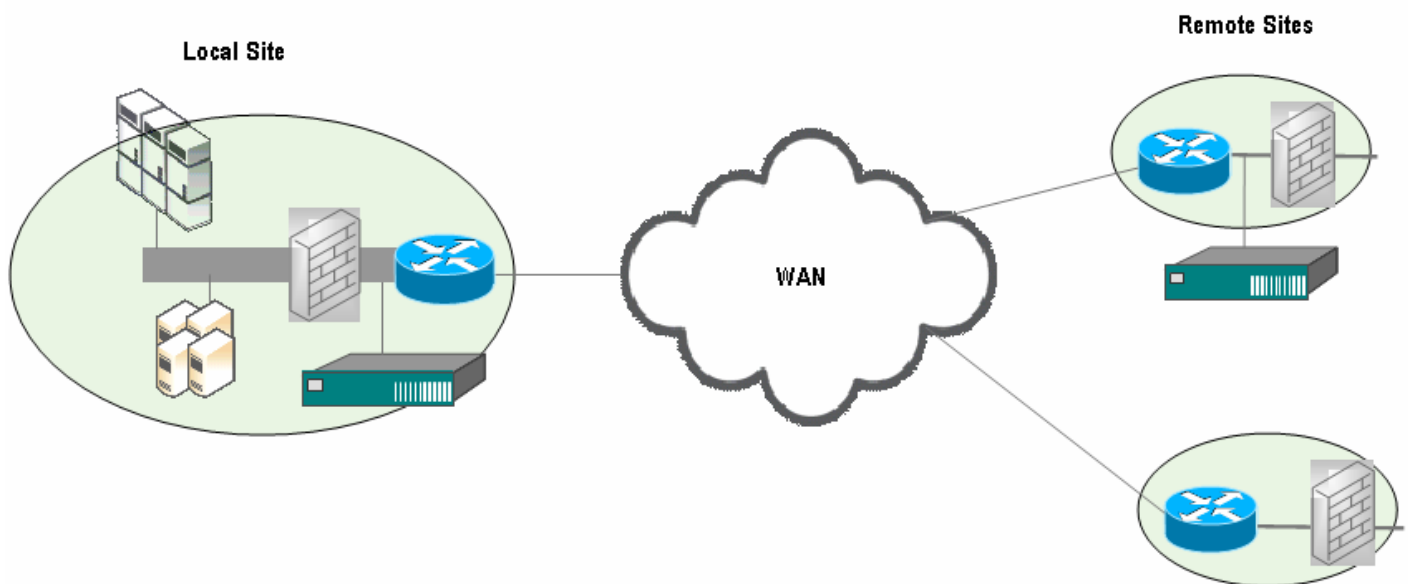
host(config)$ copy config

```

Basic MPLS VPN, Internet VPN, Private VPN Deployment

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. The 'Local Site' represents the physical installation site 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. To enable PNQM measurements, another Cisco ADE is installed (via tap or spanning) at one of the remote sites. Ideally you use the Service Provider Network policy-map for the remote site QoS policies.

Figure 8-17 Network Model – Basic MPLS VPN, Internet VPN, Private VPN Deployment

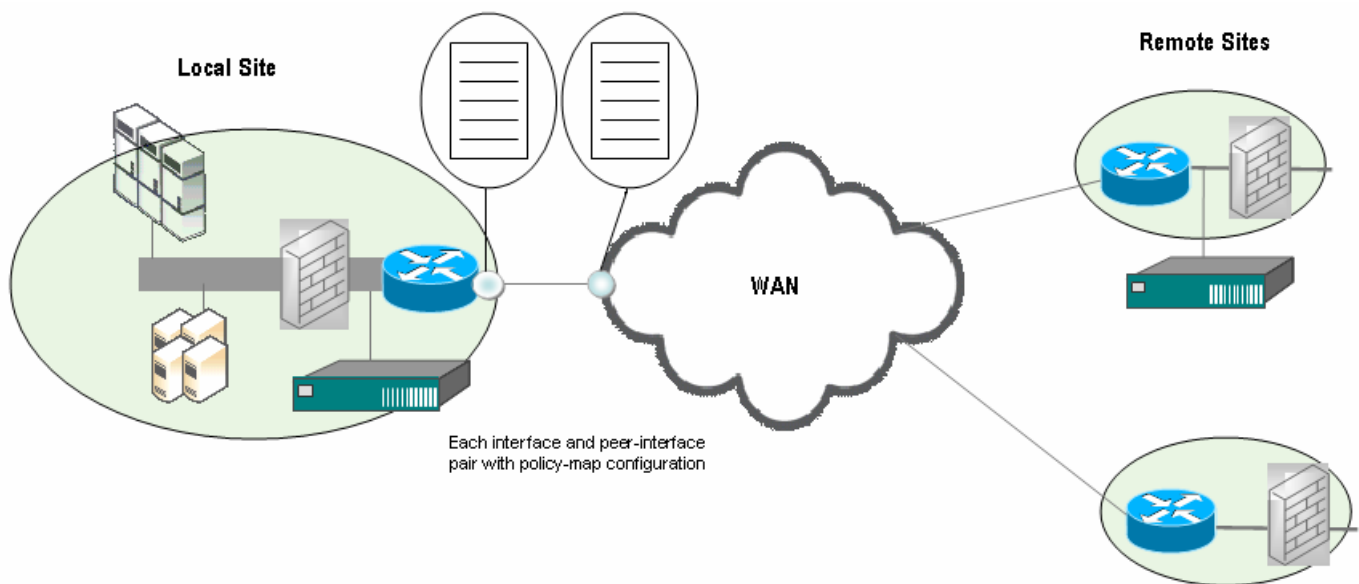


To configure the network model for this deployment, you configure the following:

- Local site
 - Default site in model that contains a Cisco ADE; the name is editable
 - Subnet
 - Router
 - Local site interface/SPN peer-interface pair with bandwidth configuration and policy-maps
- Remote Site (Cisco ADE installed for PNQM measurement)
 - Name
 - Subnet
 - Router
 - Remote site interface/SPN peer-interface pair with bandwidth configuration, policy-maps, and address of Cisco ADE for PNQM measurement
- Remote Site (No Cisco ADE installed, no PNQM measurement)
 - Name
 - Subnet
 - Router
 - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

In this example multiclass configuration, multiple network service objectives, class-maps, and policy-maps are defined.

Figure 8-18 Basic MPLS VPN, Internet VPN, Private VPN Local Site Configuration



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

Step 1

Define the network service objectives for classes. In this example network service objective configuration, the following parameters are configured:

- One-way latency target in milliseconds
- Packet protection target
- PNQM measurement is enabled
- Expected Queuing calculation is enabled with events triggered if latency exceeds one-way latency value or packet loss is detected
- Corvil Bandwidth measurement is enabled with events triggered if bandwidth measurement exceeds the configured interface capacity
- Microburst measurement is enabled down to a resolution of 150 milliseconds

Queuing delay targets are not explicitly defined, so the one-way latency value and the packet protection target are used by default for a delay target and as a basis for a packet loss target of 0.1% respectively.

```
host(config)$ nso-map realtime
host(config)$ description "Network service objectives for
remote site - no PNQM"
host(config-nso-map)$ one-way latency milliseconds 500
host(config-nso-map)$ protect-packets percent 99.9 busy-period
hours 4
host(config-nso-map)$ measure-pnqm packets-per-second 100
event-thresholds latency latency-variation loss
host(config-nso-map)$ measure-bandwidth event-threshold percent
100
host(config-nso-map)$ measure-eq event-thresholds delay loss
host(config-nso-map)$ measure-microburst milliseconds 150
```

You can configure different network service objectives to apply to each class. For more information on defining network service objectives, see the section “Defining a Network Service Objective” and the **network service objective**, **one-way-latency**, **protects-packets**, **measure-bandwidth**, **measure-eq**, **measure-microburst**, and **queuing-targets** 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 network service objective values specified above are applied to each policy-map class:

```
host(config-nso-map)$ policy-map mpls_policy
host(config-pmap)$ class realtime
host(config-pmap-c)$ nso realtime
host(config-pmap-c)# bandwidth percent 25
host(config-pmap-c)# class critical
host(config-pmap-c)$ nso critical
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class video
host(config-pmap-c)$ nso video
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class bulk
host(config-pmap-c)$ nso bulk
host(config-pmap-c)# bandwidth percent 10
host(config-pmap-c)# class besteffort
```

The other policy-maps are configured in the same way.



Note Because there is no explicit network service objective configuration made for the policy-map or the individual classes, the default network service objective is applied. See the section “Defining a Network Service Objective” for more information on the default network service objective.

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:

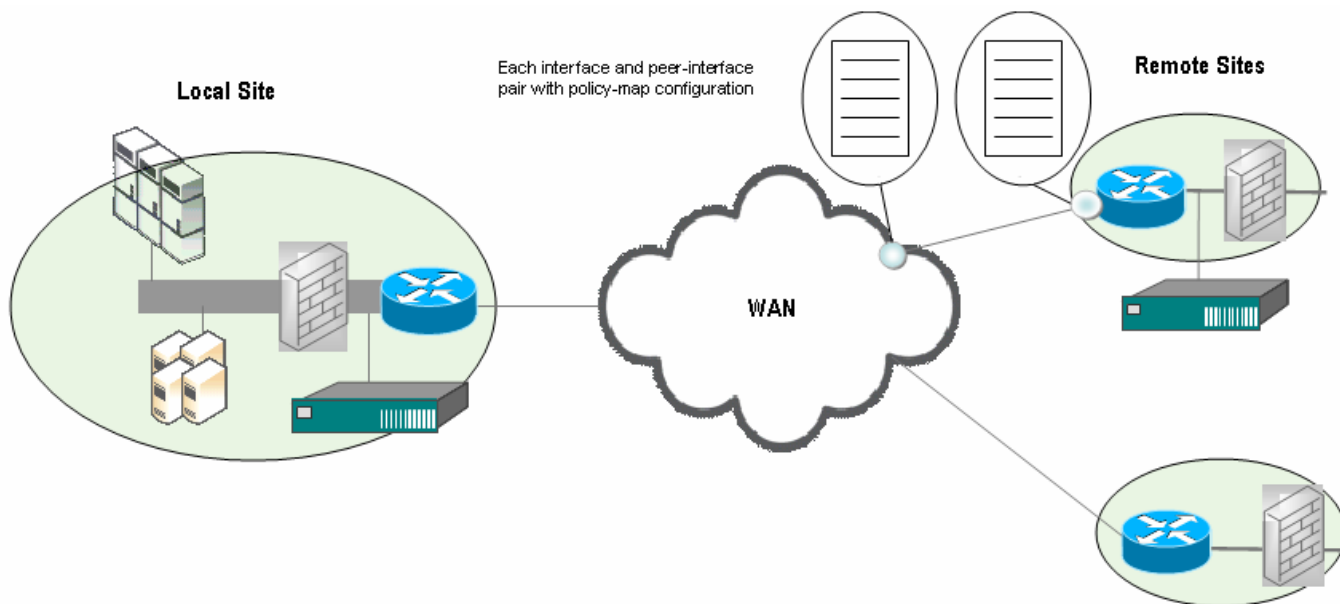
```
host(config)$ local-site Local-Site
host(config-site)$ subnet 192.168.5.0/24
host(config-local-site)$ router core1
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to SPN
MPLS"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
mpls_policy
host(config-local-site-router-if)$ peer-interface Serial0/1
host(config-local-site-router-pif)$ description "interface on
PE"
host(config-local-site-router-pif)$ bandwidth 512
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 8-19 Basic MPLS VPN, Internet VPN, Private VPN Deployment – Remote Site Configuration



- Step 5** Define the configuration remote sites with a Cisco ADE installed and requiring PNQM measurement. This remote site has its own subnet has a well-known ping address at 192.168.1.3 for ICMP measurement. The physical site represented by the remote site in the network model has a Cisco ADE installed and running BQM. In this example, the Cisco ADE has the following IP address: 192.168.17.2. PNQM measurement is effectively enabled at interface level using the **pnqm-server** command. This remote site has a site router, whose interface connection back to the peer-interface is made explicit in the configuration using the **peer-interface** command:

```

host(config-local-site-router-if)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ router remotel
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ ping-address 192.168.1.3
host(config-site-router-if)$ service-policy output mpls_policy
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

```



Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” for guidelines on how to create a matching BQM configuration to enable PNQM measurement on a remote Cisco ADE given a certain configuration on the local Cisco ADE.



Note You need only configure PNQM for the remote site interface of interest. You do not need to configure PNQM details for the associated peer-interface.

- Step 6** Define the configuration for remote sites without a Cisco ADE installed. In this example, the remote site has its own subnet, a well-known ping address at 192.168.1.3 for ICMP measurements, and a site router, whose interface connections back to the service provider network peer-interface is made explicit in the configuration using the **peer-interface** command:

```

host(config-site-router-pif)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
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 mpls_policy
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 7** Check the configuration with the **show config** command:

- Step 8** When you have satisfied with the configuration, you can save your changes. To back up the new configuration, you use the copy command:

```

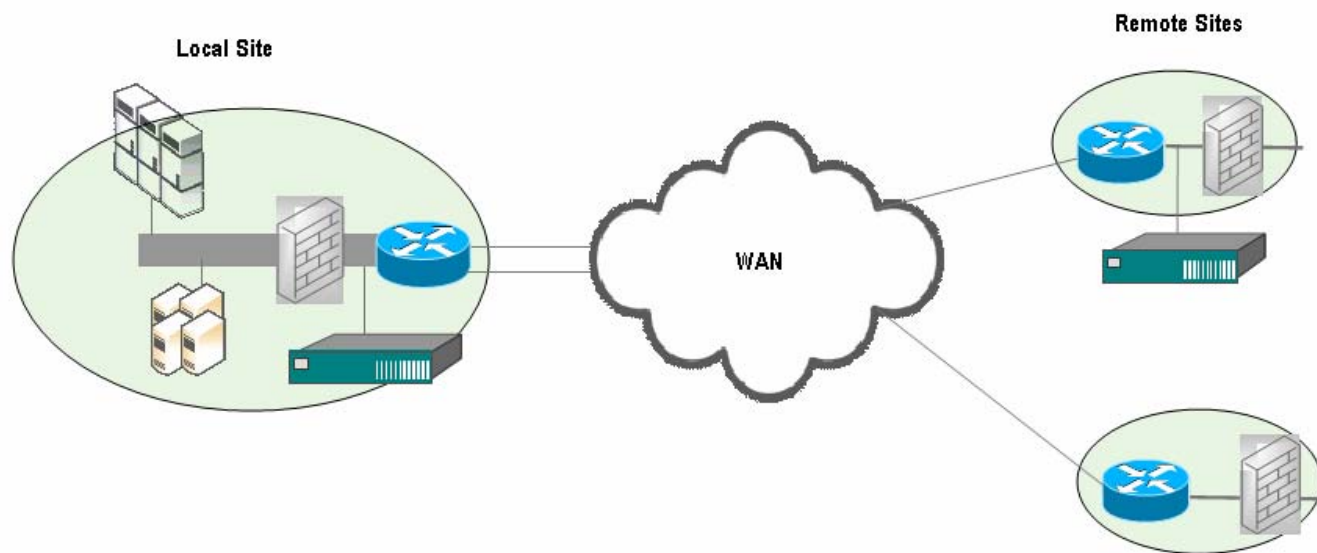
host(config)$ copy config

```

MPLS VPN Deployment with Redundant Local Site Connectivity

The BQM network model can be configured to model this deployment. However, if the links from the local site to the service provider network are load balanced, and therefore the same traffic is split over both links,

Figure 8-20 *Network Model – MPLS VPN, Internet VPN, Private VPN Deployment with Redundant Local Site Connectivity*

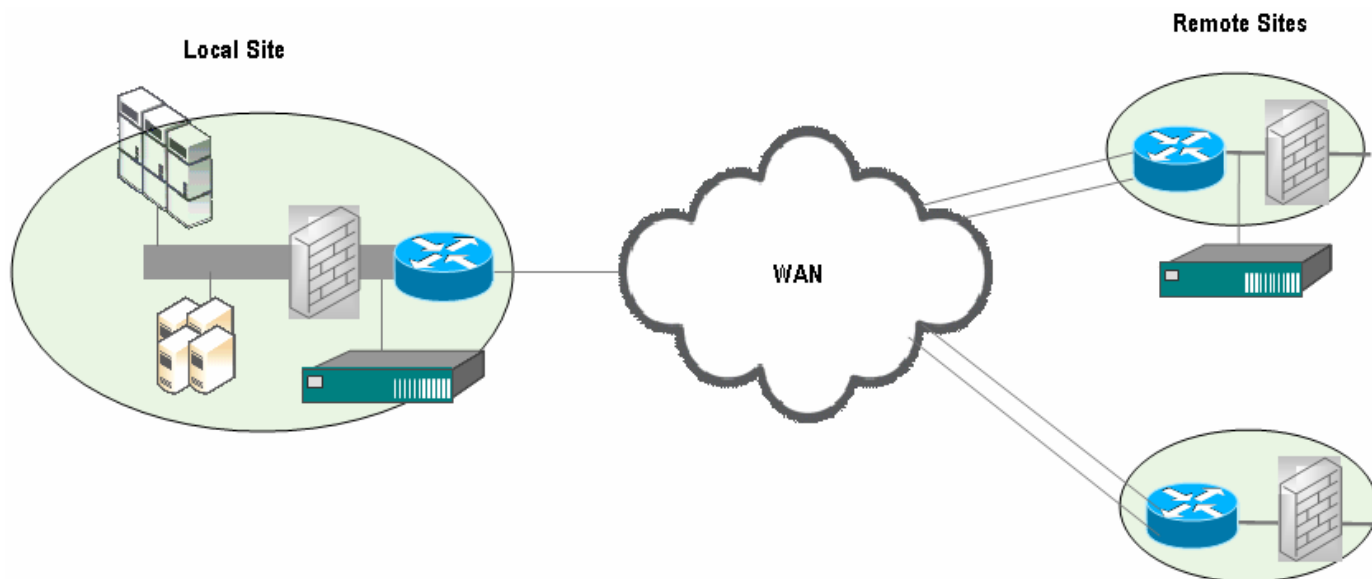


BQM does not present accurate traffic statistic results for the individual local site interfaces in this case. You must monitor the local WAN access as an aggregate of both interfaces. Likewise, PNQM results are only supported for the aggregate of both interfaces.

MPLS VPN Deployment with Redundant Remote Site Connectivity

The BQM network model can be configured to model this deployment. However, if the links from the remote site to the service provider network are load balanced, and therefore the same traffic is split over both links,.

Figure 8-21 *Network Model –MPLS VPN, Internet VPN, Private VPN Deployment with Redundant Remote Site Connectivity*

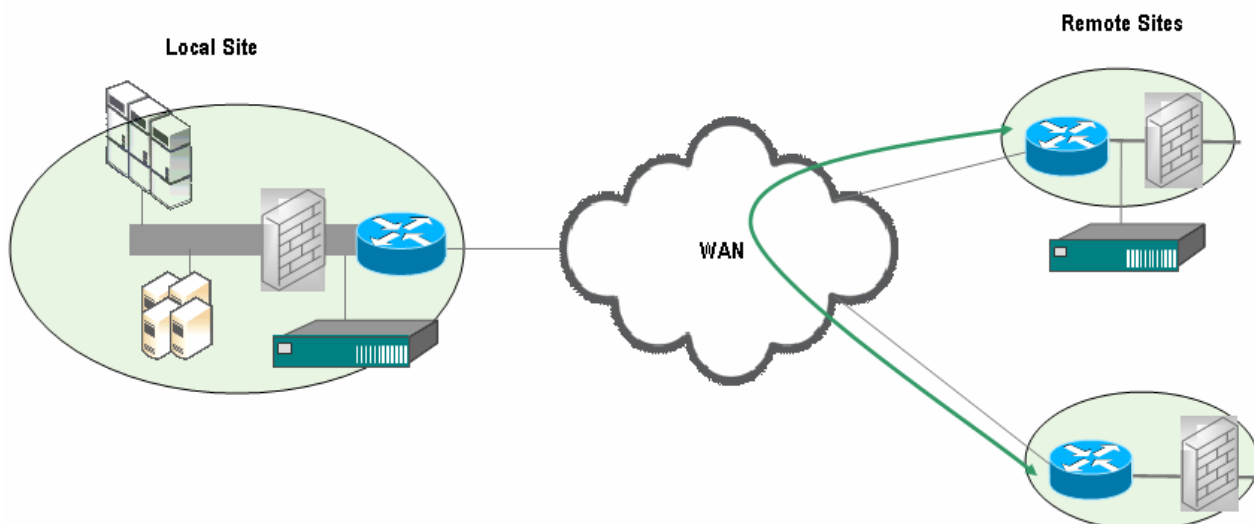


BQM does not present accurate traffic statistic results for the individual remote site interfaces in this case. You must monitor the local WAN access as an aggregate of both interfaces. Likewise, PNQM results are only supported for the aggregate of both interfaces.

MPLS VPN Deployment with Any-to-Any Traffic

In this case most of the traffic is between remote sites and a single local site, but there is also some traffic between remote sites.

Figure 8-22 *Any-to-Any Traffic Between Remote Sites*



PNQM and EQ and Corvil Bandwidth (for pre-queuing interfaces) results may be impacted but for the most part congestion at a remote site WAN access point is likely to be caused by local site traffic on its own. Post-queuing EQ results are not impacted.

Microburst results are impacted to some extent but provide useful information. You may not see whether a given remote site interface is being saturated by all the traffic arriving there, but only whether the saturation is caused by local site traffic. If the remote site is instrumented, you can see all the traffic at that remote Cisco ADE.

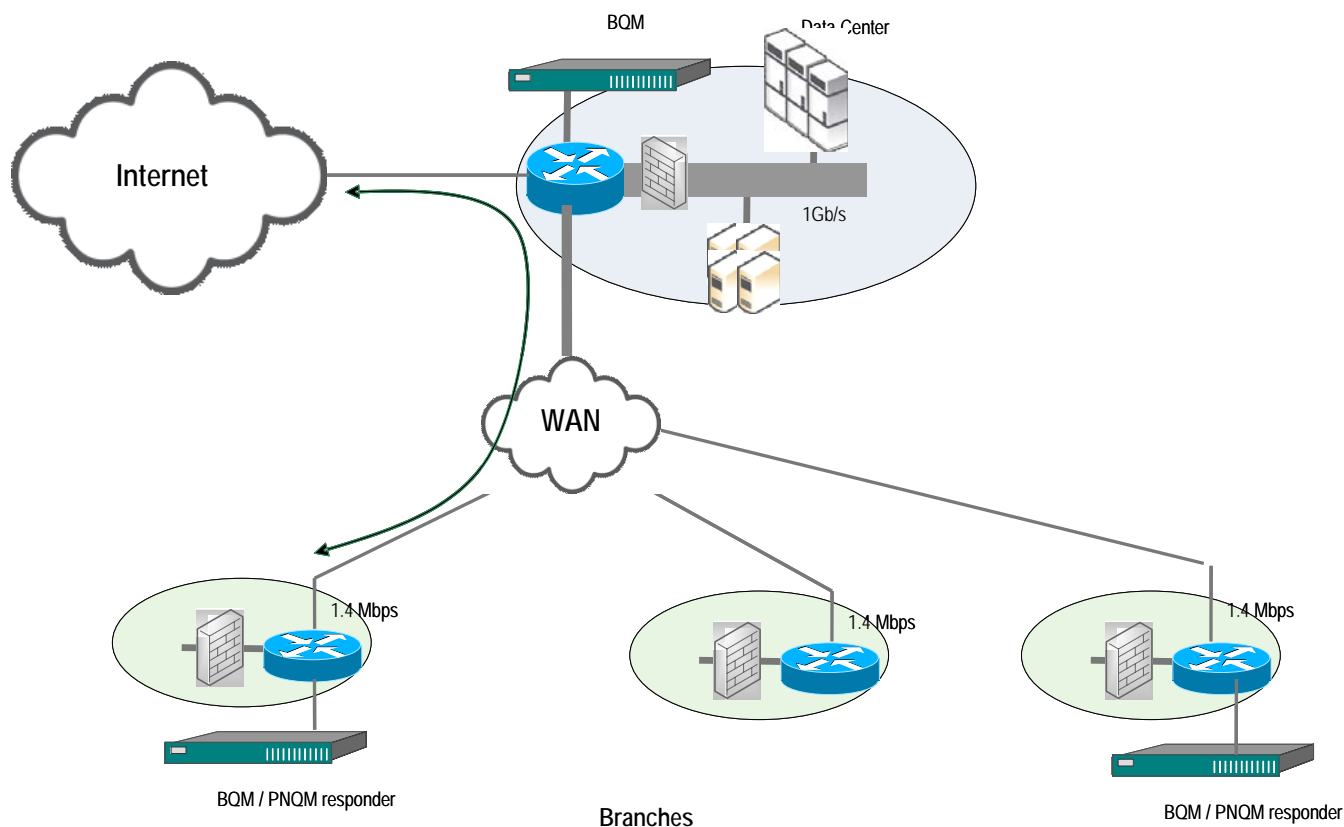
Top N results are also impacted. You only see Top N results for local site-to-remote site traffic, not all the remote site traffic. If the remote site is instrumented, you can see all the traffic at the remote Cisco ADE.

MPLS VPN Deployment with Remote Site Internet Traffic via Local Site

In the deployment example described here, the BQM sees all Internet traffic for all remote sites, assuming there is no proxying. (If non-transparent proxying is used, then proxied traffic will not be distinguished from any other local site-remote site traffic). All branches access the internet through the data center. The internet link in the data center is through a separate router with no proxy server. All traffic mostly dominates in the downstream direction with insignificant amounts of any to any traffic

A Cisco ADE is deployed in the data center to measure EQ, Corvil Bandwidth and PNQM to all remote sites. Cisco ADEs are deployed in all remote sites as PNQM responders and auto-configuration mode is used.

Figure 8-23 Remote Site Internet Traffic via Local Site



If internet traffic is bursting and experiencing large delays (for example, one site might have EQ results showing occasional large spikes of excessive queuing latency), the PNQM results will not show the excessive latency because PNQM is not measuring the internet traffic. It is impractical to configure the internet subnets in the local site. The PNQM results are not based on the internet traffic.

In general for this type of deployment, PNQM will not provide results for traffic from remote sites to the Internet, because this traffic doesn't come from the local site. The traffic will instead be counted as re-routed. A remote site will only see all of the traffic if it has a Cisco ADE installed and manually configured to mirror the local site configuration, and this remote site is directly connected to the local site and can identify local site-bound traffic (using attached ports, or some non-subnet based method that includes the Internet traffic).

The "Unmatched traffic" interface should contain local site-to-Internet traffic, but won't include remote site-to-Internet traffic, because that traffic isn't "Unmatched" – it's already matched to/from a remote site. Remote site interface results will include Internet traffic. So, PNQM results will contain non-Internet remote site traffic. EQ and Corvil Bandwidth results for pre-queuing interfaces will include all remote site traffic, and so can be used to investigate remote site WAN-access congestion.

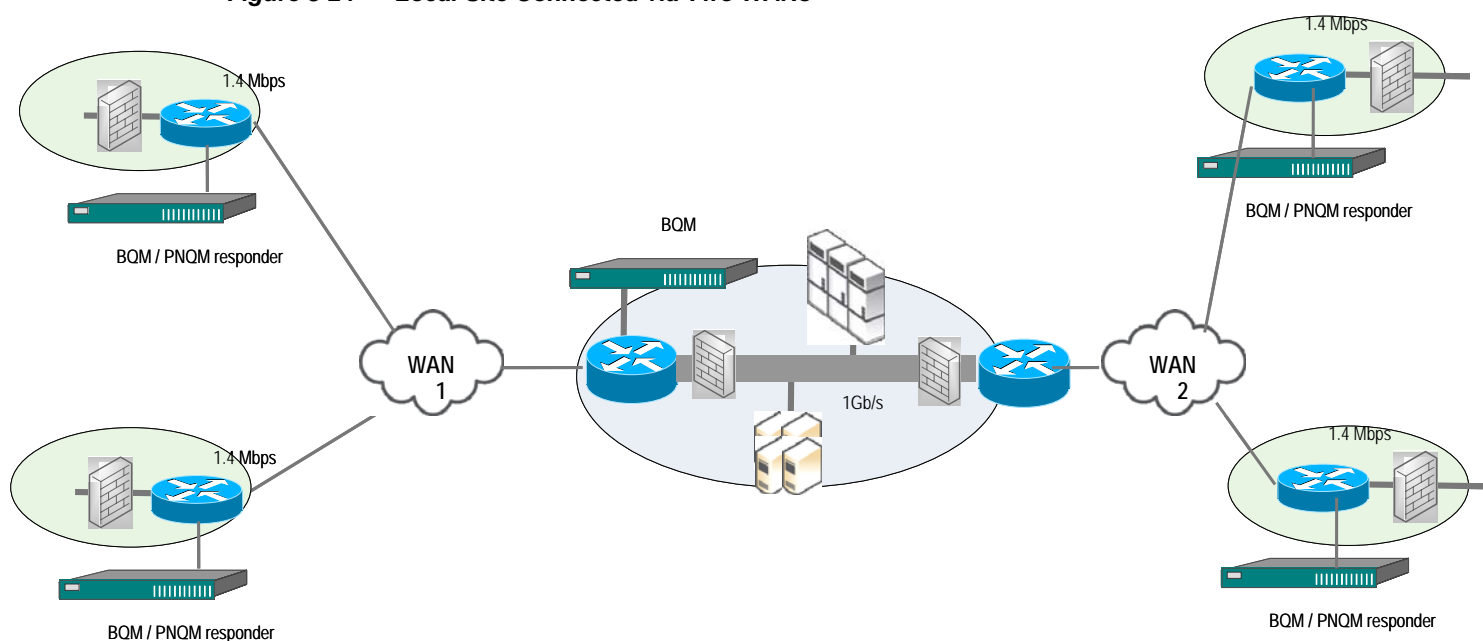
To get EQ for post-queuing interfaces from Cisco ADEs installed at remote sites, the remote site BQM configuration must identify all traffic bound for the local site using some non-subnet based method that includes the Internet traffic. This could be done using attached-ports and uni-directional traffic acquisition, or filter-classes that match all incoming/outgoing traffic using destination/source subnets in the remote site.

Remote site interface microburst and Top N results will include remote site-to-Internet traffic, but results for the local site WAN-access interface will not.

MPLS VPN Deployment with Local Site Connected to Remote Sites via Two WANs

In this scenario, the remote sites are divided across two WANs, and the local site Cisco ADE sees traffic flowing between the two WANs. This scenario also applies to deployments in which all remote sites are in a single WAN but have two or more routers and the traffic between remote sites is brought back to a switch and is measured by the Cisco ADE.

Figure 8-24 Local Site Connected via Two WANs



PNQM are impacted here because you can't monitor remote site-to-remote site traffic. The remote site will not include the traffic because the traffic won't match local site subnets.

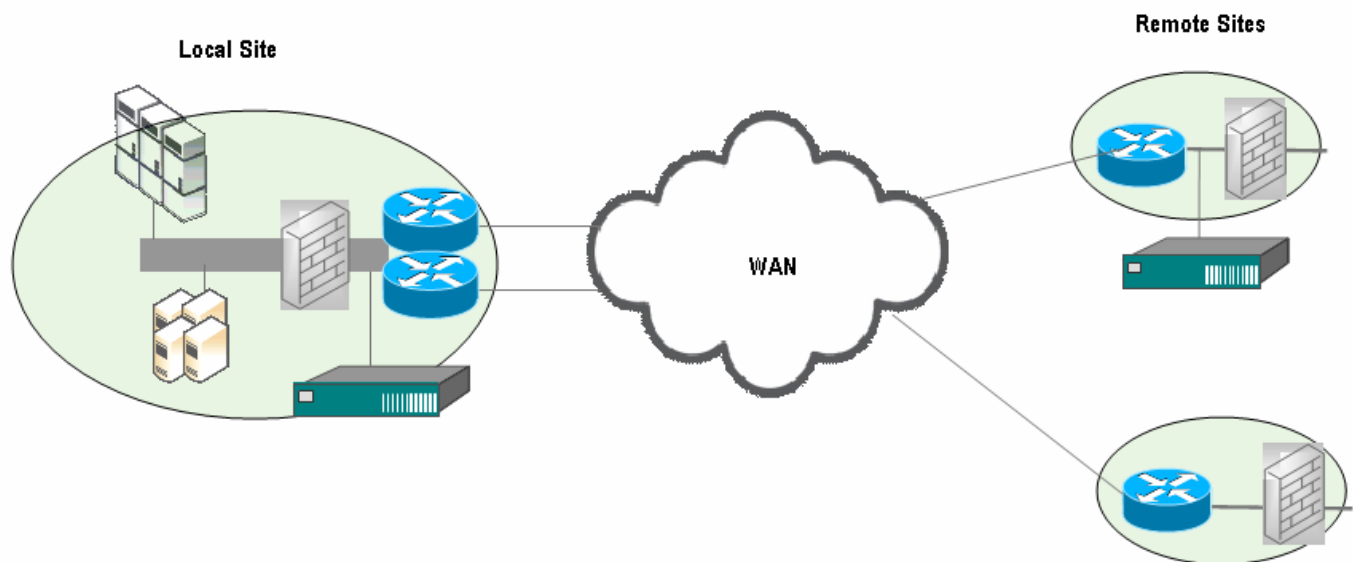
EQ and Corvil Bandwidth results for pre-queuing interfaces will include the measured remote site-to-remote site traffic, unless you specifically filter it out using filter-classes. EQ results for post-queuing interfaces are not impacted. For directly-connected sites you could add subnets to the remote site configuration that represents the local site subnets, so that the remote site configuration will match all local site-bound traffic, including through traffic.

Microburst and Top N results will include measured remote site-to-remote site traffic, unless specifically filtered out using filter-classes.

Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment

The Cisco ADE is installed via either tap or spanning configuration on the LAN interface of the local site router. For PNQM measurement, another Cisco ADE is installed at the relevant remote site. All measurements are made and viewed from the perspective of the local site. If the two WAN router interfaces at the local site are managed by a load balancer, then PNQM measurement is supported only on the aggregate of both interfaces. 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 8-25 Network Model – Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment



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

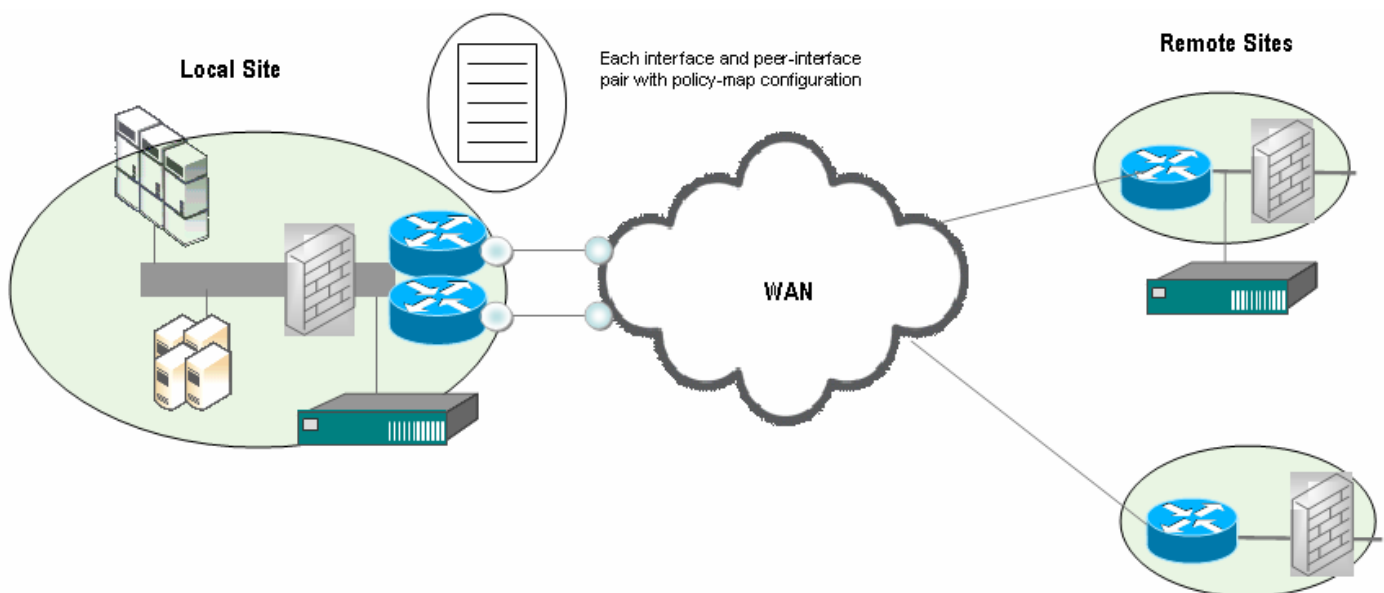
- Local site
 - Default site in model that contains a Cisco ADE; the name is editable
 - Subnet
 - Router
 - Local site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

- Remote Site (Cisco ADE installed for PNQM measurement)
 - Name
 - Subnet
 - Router
 - Remote site interface/SPN peer-interface pair with bandwidth configuration, policy-maps, and address of Cisco ADE for PNQM measurement
- Remote Site (No Cisco ADE installed, no PNQM measurement)
 - Name
 - Subnet
 - Router
 - Remote site interface/SPN peer-interface pair with bandwidth configuration and policy-maps

In this example multiclass configuration, multiple network service objectives, class-maps, and policy-maps are defined.

To configure the network model for this deployment from the CLI, you do the following

Figure 8-26 *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 network service objective for remote sites without a Cisco ADE installed for PNQM measurement. In this example network service objective configuration, the following parameters are configured:

- One-way latency target in milliseconds
- Packet protection target
- PNQM measurement is explicitly disabled
- Expected Queuing calculation is enabled with events triggered if latency exceeds one-way latency value or packet loss is detected
- Corvil Bandwidth measurement is enabled with events triggered if bandwidth measurement exceeds the configured interface capacity
- Microburst measurement is enabled down to a resolution of 150 milliseconds

Queuing delay targets are not explicitly defined, so the one-way latency value and the packet protection target are used by default for a delay target and as a basis for a packet loss target of 0.1% respectively.

```
host(config)$ nso-map low_speed
host(config)$ description "Network service objectives for
remote site - no PNQM"
host(config-nso-map)$ one-way latency milliseconds 500
host(config-nso-map)$ protect-packets percent 99.9 busy-period
hours 4
host(config-nso-map)$ no measure-pnqm
host(config-nso-map)$ measure-bandwidth event-threshold percent
100
host(config-nso-map)$ measure-eq event-thresholds delay loss
host(config-nso-map)$ measure-microburst milliseconds 150
```

You can configure different network service objectives to apply to each class. For more information on defining network service objectives, see the section “Defining a Network Service Objective” and the **network service objective**, **one-way-latency**, **protects-packets**, **measure-bandwidth**, **measure-eq**, **measure-microburst**, and **queuing-targets** 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 network service objective values specified above are applied to each policy-map class:

```

host(config-nso-map)$ policy-map mpls_policy
host(config-pmap)$ class realtime
host(config-pmap-c)$ nso realtime
host(config-pmap-c)# bandwidth percent 25
host(config-pmap-c)# class critical
host(config-pmap-c)$ nso critical
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class video
host(config-pmap-c)$ nso video
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class bulk
host(config-pmap-c)$ nso bulk
host(config-pmap-c)# bandwidth percent 10
host(config-pmap-c)# class besteffort

```

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)$ attached-port PortA PortB
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to SPN
MPLS"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
mpls_policy
host(config-local-site-router-if)$ peer-interface Serial0/1
host(config-local-site-router-pif)$ description "interface on
PE"
host(config-local-site-router-pif)$ bandwidth 512

```

```

host(config-local-site-router-pif)$ service-policy output pe-
policy
host(config-local-site-router-pif)$ router core2
host(config-local-site-router)$ attached-port PortC PortD
host(config-local-site-router)$ interface Serial0/1
host(config-local-site-router-if)$ description "Link to SPN
MPLS"
host(config-local-site-router-if)$ bandwidth 512
host(config-local-site-router-if)$ service-policy output
mpls_policy
host(config-local-site-router-if)$ peer-interface Serial0/1
host(config-local-site-router-pif)$ description "interface on
PE"
host(config-local-site-router-pif)$ bandwidth 512
host(config-local-site-router-pif)$ service-policy output pe-
policy

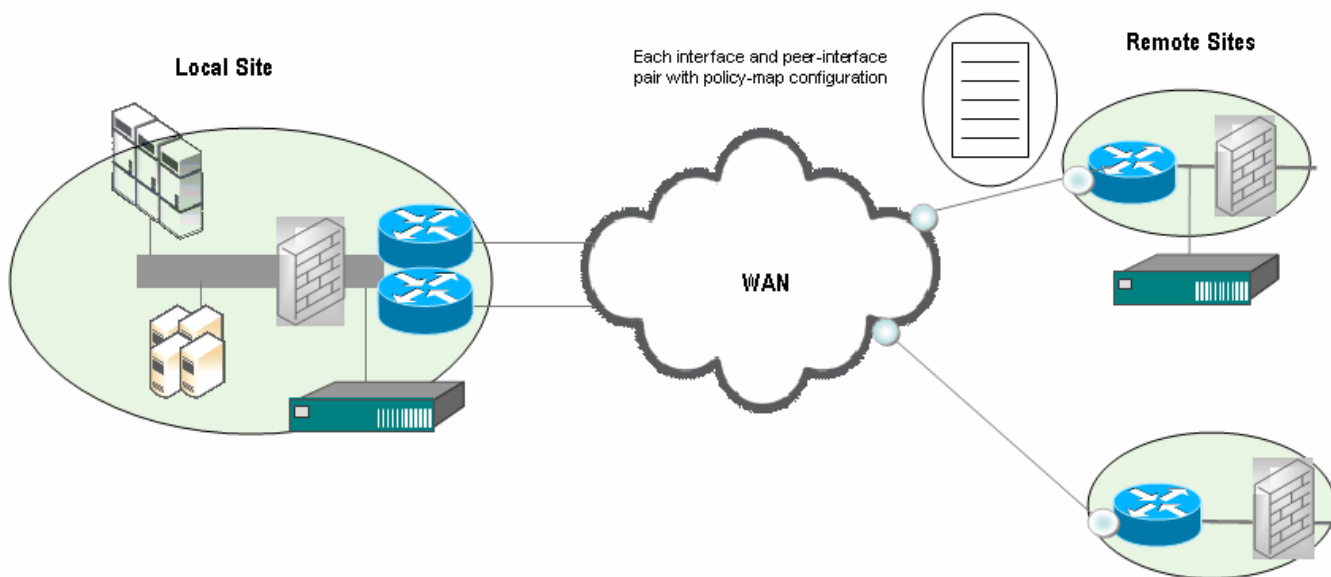
```



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 8-27 *Dual-homed MPLS VPN, Internet VPN, Private VPN Deployment – Remote Site Configuration*



Step 5

Define the configuration remote sites with a Cisco ADE installed and requiring PNQM measurement. This remote site has its own subnet has a well-known ping address at 192.168.1.3 for ICMP measurement. The physical site represented by the remote site in the network model has a Cisco ADE installed and running BQM. In this example, the Cisco ADE has the following IP address: 192.168.17.2. PNQM measurement is effectively enabled at

interface level using the **pnqm-server** command. This remote site has a site router, whose interface connection back to the peer-interface is made explicit in the configuration using the **peer-interface** command:

```
host(config-local-site-router-if)$ site "Remote Site 1"
host(config-site)$ subnet 192.168.1.0/24
host(config-site)$ router remotel
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ ping-address 192.168.1.3
host(config-site-router-if)$ service-policy output mpls_policy
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
```



Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” for guidelines on how to create a matching BQM configuration to enable PNQM measurement on a remote Cisco ADE given a certain configuration on the local Cisco ADE.



Note You need only configure PNQM for the remote site interface of interest. You do not need to configure PNQM details for the associated peer-interface.

Step 6

Define the configuration for remote sites without a Cisco ADE installed. In this example, the remote site has its own subnet, a well-known ping address at 192.168.1.3 for ICMP measurements, and a site router, whose interface connections back to the service provider network peer-interface is made explicit in the configuration using the **peer-interface** command:

```
host(config-site-router-pif)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
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 mpls-policy
```

```

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 7 Check the configuration with the **show config** command:

Step 8 When you have satisfied with the configuration, you can save your changes. To back up the new configuration, you use the copy command:

```

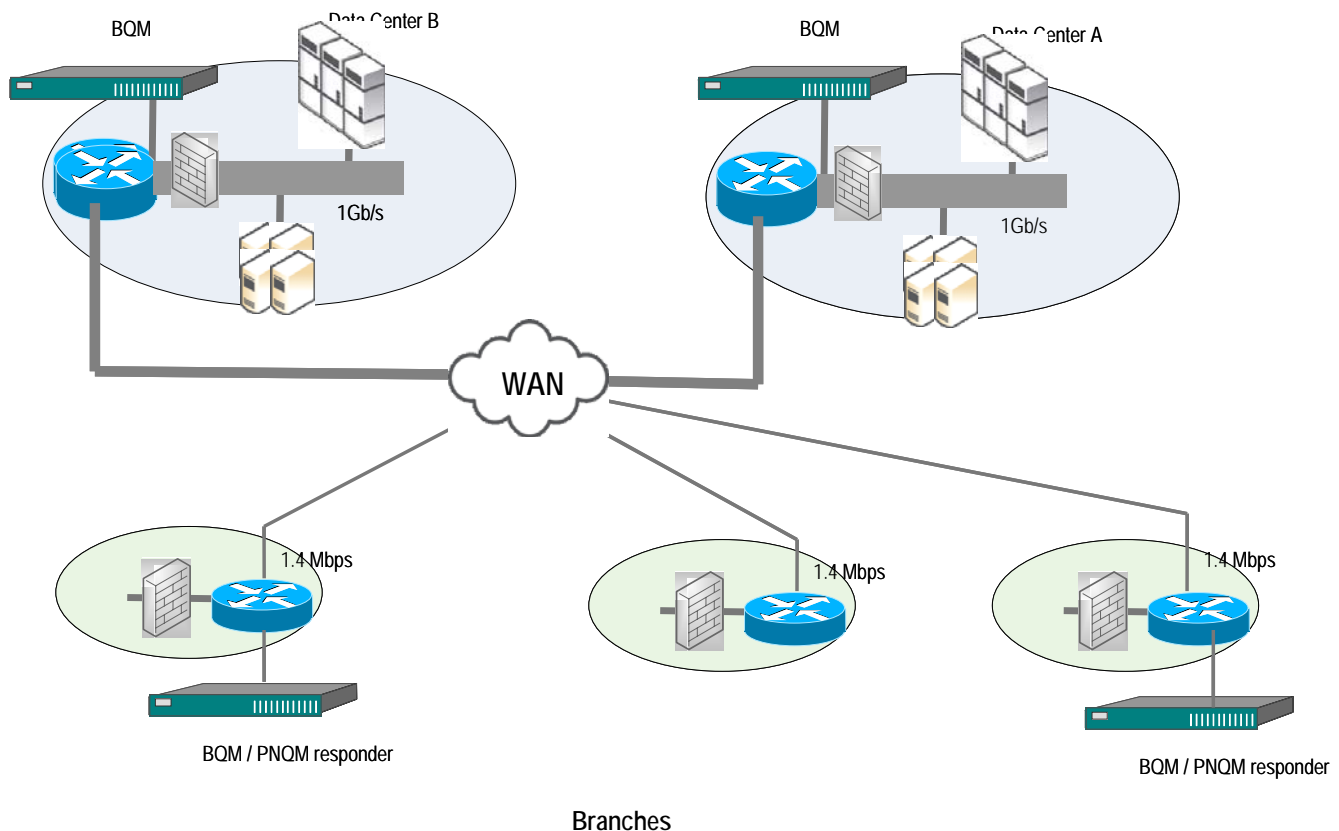
host(config)$ copy config

```

Dual Data Center Deployment

The network model deployments discussed in the preceding sections are based on having the single local site configuration represent the physical installation of a Cisco ADE at a data center. However, it is possible to get some insight into network quality issues using BQM when the deployment involves two data centers.

Figure 8-28 Deployment with Two Data Centers



In the example deployment shown in the preceding figure, Cisco ADEs running BQM are deployed in the two data centers and are configured to report PNQM and auto-configuration mode is used because remote EQ results are not required. PNQM responders are deployed at a number of remote sites. The Cisco ADEs also measure EQ and Corvil Bandwidth for all the interfaces on the remote sites, but there is some doubt about these results due to the presence of potentially significant any-to-any traffic between these sites. Data mostly dominates in the downstream direction from the two data centers.

The combination of traffic from the two data centers may create issues at remote sites that cannot be measured by EQ. For example, users might report intermittent application performance issues at a couple of remote sites. EQ and Corvil Bandwidth might not report any issues with the sites experiencing the application performance issues, but PNQM might report larger delays downstream (and perhaps some loss) to all the sites then can be explained from the current EQ results and active ping results.

If PNQM shows issues for the same remote sites but not for any others, the problem is unlikely to be the service provider. In this case, the most likely solution would be to upgrade the WAN links at the relevant remote sites.

In general, if all branch traffic is to the data centers, you can get reliable PNQM results, but if there are significant traffic loads to each data center you cannot tell if PNQM quality outages for traffic to remote sites is due to the other data center or to the service provider. If there is a Cisco ADE installed at the other data center, you could configure the remote site Cisco ADE with PNQM channels to each data center, and compare PNQM and local WAN access congestion (Microburst and EQ) results on the remote site Cisco ADE.

EQ and Corvil Bandwidth for pre-queuing interfaces are impacted, but the results are likely to be useful when remote site WAN access traffic is dominated by one data center at a time. EQ results for post-queuing interfaces is not affected.

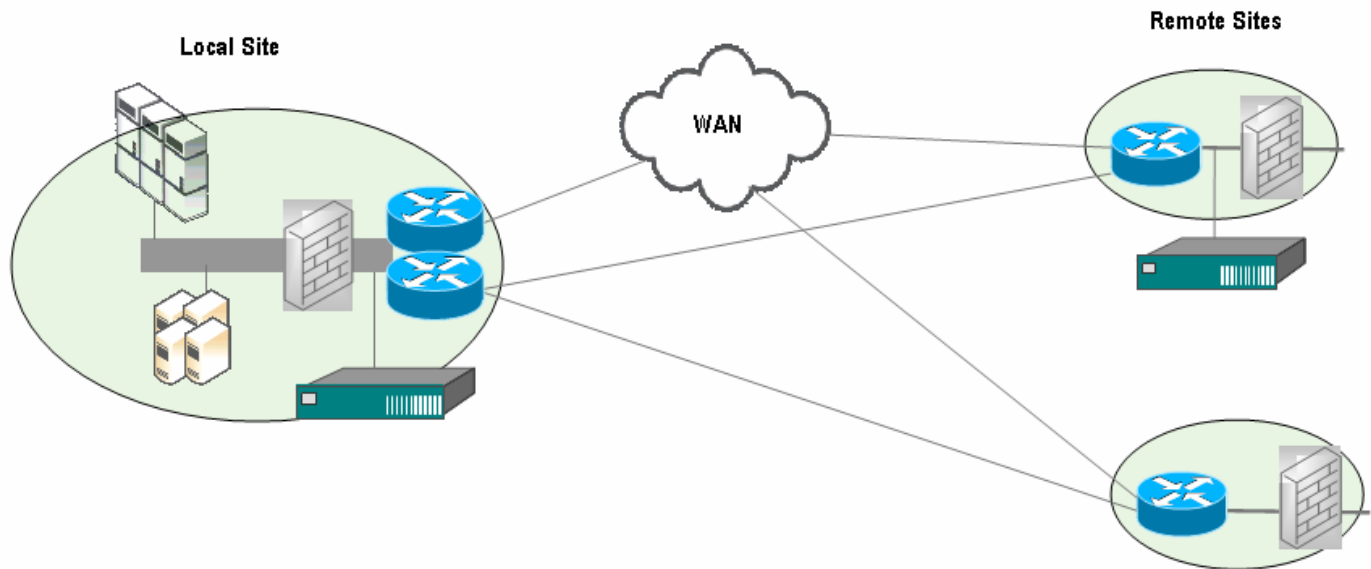
Microburst results are impacted to some extent but still provide useful information. However, you are not seeing whether a given remote site interface is being saturated by all the traffic arriving there, but only whether the saturation is caused by data center traffic. If the remote site is instrumented, you can see all the traffic at that remote Cisco ADE.

Top N results are also impacted. You only see Top N results for local site-to-remote site traffic, not all the remote site traffic. If the remote site is instrumented, you can see all the traffic at the remote Cisco ADE.

Hybrid Deployment

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

Figure 8-29 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 Cisco ADE; 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 physical measurement ports to routers
- Remote Site (Cisco ADE installed for PNQM measurement)
 - Name
 - Subnet
 - Router
 - Remote site interface/SPN peer-interface pair with bandwidth configuration, policy-maps, and address of Cisco ADE for PNQM measurement
 - Remote site interfaces in point-to-point connection with local site router with bandwidth configuration and policy-maps
- Remote Site (No Cisco ADE installed, no PNQM measurement)
 - 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 network service objective and monitor end2end map for the configuration. In this example network service objective 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)$ network service objective low_speed
host(config-nso-map)$ measure-bandwidth
host(config-nso-map)$ measure-microburst milliseconds 150
host(config-nso-map)$ queuing-targets delay-milliseconds 150
```

For more information on defining network service objectives, see the **network service objective**, **measure-bandwidth**, **measure-microburst**, and **queuing-targets** 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 network service objective values specified above are applied to each policy-map class:

```
host(config-nso-map)$ policy-map mpls_policy
host(config-pmap)$ class realtime
host(config-pmap-c)$ nso low_speed
host(config-pmap-c)# bandwidth percent 25
host(config-pmap-c)# class critical
host(config-pmap-c)$ nso low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class video
host(config-pmap-c)$ nso low_speed
host(config-pmap-c)# bandwidth percent 20
host(config-pmap-c)# class bulk
host(config-pmap-c)$ nso low_speed
host(config-pmap-c)# bandwidth percent 10
host(config-pmap-c)# class besteffort
host(config-pmap-c)$ nso 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 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)$ router remotel
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ ping-address 192.168.2.5
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)$ pnqm-server 192.168.1.2 autoconf
host(config-site-router-if)$ pnqm-server-test
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic
(notice), 0 could not be established (error).
Test completed...
host(config-site-router-if)$ connects-to Local-site core2
Serial0/1
```



Note If you want to be able to view Expected Queuing results as measured from the remote Cisco ADE, you need to perform manual configuration of PNQM on that remote Cisco ADE, setting up a full network model from the perspective of that machine. See the section “Manual PNQM Configuration” for guidelines on how to create a matching BQM configuration to enable PNQM measurement on a remote Cisco ADE given a certain configuration on the local Cisco ADE.



Note You need only configure PNQM for the remote site interface of interest. You do not need to configure PNQM details for the associated peer-interface.

Step 6

Define the configuration for remote sites without a Cisco ADE installed. In this example, the remote site has its own subnet and a site router with interface connections back to both the service provider network peer-interface, made explicit in the configuration using the **peer-interface** command, and the local site, using the **connects-to** command:

```
host(config-site-router-pif)$ site "Remote Site 2"
host(config-site)$ subnet 192.168.2.0/24
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 7

Check the configuration with the **show config** command:

```
host(config-site-router-pif)$ show config
network service objective low_speed
  queuing-targets delay-milliseconds 150
  measure-microburst milliseconds 150
  measure-bandwidth
!
```

```
!  
  
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  
    nso low_speed  
    bandwidth 25  
  class critical  
    nso low_speed  
    bandwidth 20  
  class video  
    nso low_speed  
    bandwidth 20  
  class bulk  
    nso low_speed  
    bandwidth 10  
  class besteffort  
    nso low_speed  
  class class-default  
  
policy-map mpls_policy  
  class realtime  
    nso low_speed  
    bandwidth 25  
  class critical  
    nso low_speed  
    bandwidth 20  
  class video  
    nso low_speed  
    bandwidth 20  
  class bulk  
    nso low_speed  
    bandwidth 10  
  class besteffort  
    nso low_speed  
  class class-default  
  
policy-map pe_policy  
  class realtime  
    nso low_speed  
    bandwidth 25  
  class critical  
    nso low_speed  
    bandwidth 20  
  class video
```

```
nso low_speed
bandwidth 20
class bulk
  nso low_speed
  bandwidth 10
class besteffort
  nso 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 remotel
    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--

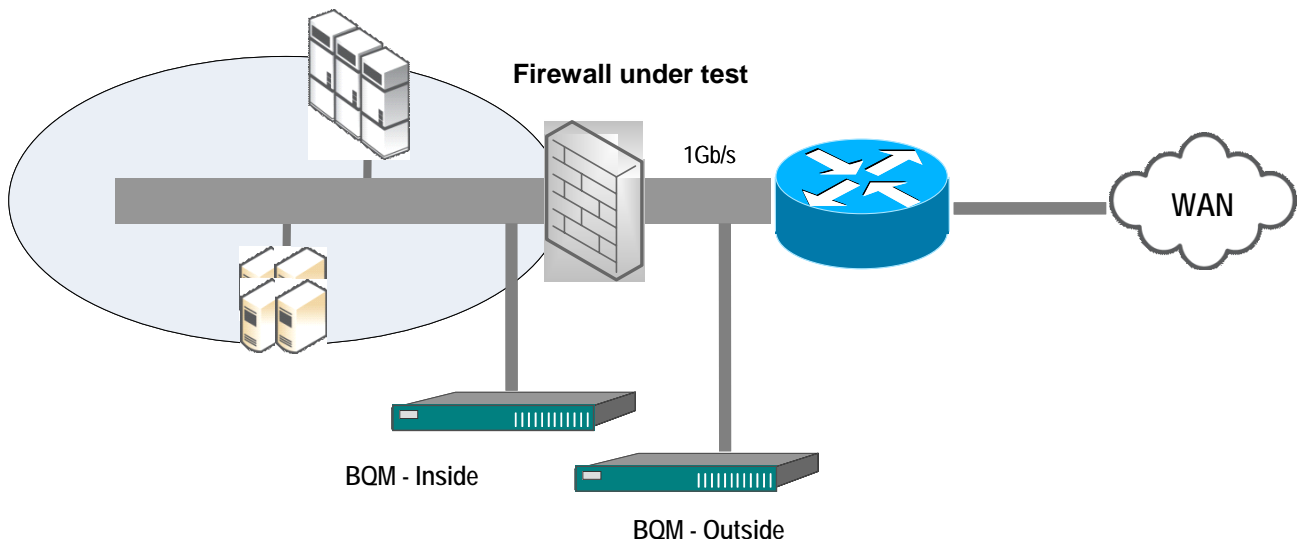
Step 7 When you have satisfied with the configuration, you can save your changes. To back up the new configuration, you use the copy command:

```
host(config)$ copy config
```

Point-to-Point Firewall Deployment

You can measure the latency experienced through a firewall using BQM PNQM technology. Packets must not be modified by the firewall device - compression, encryption, and several WAN acceleration techniques are not supported.

Figure 8-30 PNQM Measurement Across a Firewall



In the example deployment shown in the preceding figure, the firewall is connected between two switches in the DMZ, the second switch is connected to the WAN router.

Two Cisco ADEs running BQM are deployed, the first (BQM - Inside) measuring the traffic between the first switch and the firewall, the second (BQM - Outside) measuring the traffic between the firewall and the second switch connected to the WAN router.

BQM – Inside is configured as follows:

- A local site is configured with an interface with a filter-class matching all traffic with a source IP address of the data center subnets
- A remote site is configured as directly connected with a filter-class on the interface to match all traffic with a destination IP address of the data center subnets
- PNQM is configured on the remote site interface with the IP address of BQM - Outside and set to manual configuration mode
- Corvil Bandwidth and EQ measurements are disabled for all interfaces because these values are not relevant to the firewall; a single-class policy map is used on all interfaces

BQM - Outside must be manually configured with the mirror configuration. See the section “Manual Remote BQM Configuration” for more information on manual configuration.

PNQM latency results can now be viewed for the interface in the remote site. You can optionally set thresholds to trigger packet captures and examine the traffic that is experiencing the excessive delays in the firewall.

This example deployment does not support WAN-acceleration, or other effects that modify the packets. To support WAN-acceleration, you would need to measure PNQM between points outside the firewall and then, separately, measure PNQM between points inside the firewall. You could then compare the results to see the differences introduced by the inside-outside acceleration boundary.

Configuring a Custom Dashboard

You can configure a custom dashboard to monitor the network service level being achieved by a defined set of classes. The newly defined custom dashboard is displayed as a new tab in **Bandwidth Quality Manager** mode in the GUI.

You define a custom dashboard in the CLI using the **custom-dashboard** command.

Only one custom dashboard may be defined at any time, so to check if a custom dashboard has already been defined (for example, by another user via the GUI), you can use the **show custom-dashboard** command. In the following example, there is no custom dashboard already defined:

```
host(config)# show custom-dashboard
host(config)#
```

If you attempt to use the **custom-dashboard** command when there is already a custom dashboard defined, you get the following error message:

```
host(config)# custom-dashboard EMEA
Error: number of custom-dashboards exceeded limit '1'
host(config)#
```

To define a custom dashboard using the CLI, you do the following:

Step 1 Define the custom dashboard with a unique name.

```
host(config)# custom-dashboard TelePresence
host(config-custom-dashboard)#
```



Note The name you specify here will be displayed as the name of the new tab in **Bandwidth Quality Manager** mode. In this case there will be seven tabs displayed in the GUI, so we recommend that you use a concise name for the tab. The maximum allowable length is 15 characters.

Step 2 Specify the classes to be monitored using the custom dashboard using the **class** command.

```
host(config-custom-dashboard)# class class-default
host(config-custom-dashboard)# class nyc_video
host(config-custom-dashboard)# class ldn_video
host(config-custom-dashboard)# class syd_video
```

Step 4 Specify the graph and chart results to be displayed for each selected class using the **graph-order** command to enter graph order mode and then using the **graph** command.

```
host(config-custom-dashboard)# graph-order
host(config-custom-dashboard-go)# graph ?
  5 minute Network Service Index      graph name
  Average Rate                        graph name
  Corvil Bandwidth - Delay             graph name
  Corvil Bandwidth - Queue Length     graph name
  End-to-end Jitter                   graph name
  End-to-end Loss                     graph name
  End-to-end Delay                    graph name
  EQ Delay                           graph name
  EQ Delay variation                  graph name
  EQ Loss                            graph name
  Interface ICMP Round-trip Delay     graph name
  Microburst-detection                graph name
  Packet Rate                         graph name
  Packet Size distribution (by bytes)  graph name
  Packet Size distribution (by packets) graph name
  Peak-to-mean                       graph name
  Top 10 Applications                 graph name
  Top 10 Conversations                graph name
  Top 10 Listeners                    graph name
  Top 10 Talkers                      graph name

host(config-custom-dashboard-go)# graph "End-to-end Delay"
host(config-custom-dashboard-go)# graph "End-to-end Loss"
host(config-custom-dashboard-go)# graph "EQ Delay"
host(config-custom-dashboard-go)# graph "EQ Loss"
```



Note Graph names comprising more than one word must be enclosed in quotes ("").

Graphs are displayed in the GUI custom dashboard in the same order that they are defined here. You can use the **up** and **down** commands to change the order, or use the **graph** command to add or remove graphs.

Step 5 When you leave graph order mode, the changes you have defined are saved.

```
host(config-custom-dashboard-go)# end
```

The new custom dashboard is displayed as a new tab in the GUI **Bandwidth Quality Manager** mode to the right of the **Network Service Quality** tab. You may have to refresh the browser screen to see the new tab. When the next data summarization period elapses (as per the selected reporting period), results are available for each monitored class.

You can use the **show custom-dashboard** and **show config custom-dashboard** commands to review the current custom dashboard configuration.

```
host(config)# show custom-dashboard
custom-dashboard TelePresence
  class nyc_video
  class ldn_video
  class syd_video
  graph-order
  ! graph order list
  graph "End-to-end Delay"
  graph "End-to-end Loss"
  graph "EQ Delay"
  graph "EQ Loss"
```

```
host(config)# show config custom-dashboard
!
custom-dashboard TelePresence
  class nyc_video
  class ldn_video
  class syd_video
  graph-order
  graph "End-to-end Delay"
  graph "End-to-end Loss"
  graph "EQ Delay"
  graph "EQ Loss"
```

```
host(config)#
```




9 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



Note For information on system upgrade, see the Release Notes.

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 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 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
- gps
- 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 BQM as the admin user, you have the ability to change both the admin and config user account passwords. If you log in as the config user you may only change the config user password.



Note You should change both passwords on the first day of use, as soon as you have set up BQM. Valid, good passwords comprise a mixture of at least eight upper and lowercase, alphanumeric and non-alphanumeric characters. The system enforces a minimum length of five characters.

For example, to change the config user account password, you use the **password** command:

```
host(config)# password config
```

```
Changing password for config
config's password:
New password:
Re-enter new password:
Password changed.
```

```
host(config)#
```

Password Recovery

To restore the original default passwords shipped with BQM, you do the following:

Log in at the console port using the username `restorepasswords`. No password is needed.

This can only be done from the console port, 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  7 09:10   -
admin          GUI          Sep  7 09:18   -
host(config)#
```

Table 9-1 **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 console port, the Host column displays <code>serial-line</code> .

System Setup

The basic system setup operations include:

- Installing a License
- Viewing and Configuring Network Settings
- Configuring PNQM Settings
- Restricting SNMP Access
- Restricting IP Address Access
- System Time Settings

Installing a License

If 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. The System ID may be retrieved using the **status** command.

```
host(config)$ status
Cisco Bandwidth Quality Manager software: Version 4.0)
CorvilMeter software: CDK_3_0_BUILD_42 (conf Jun 23 17:42:17 2007)
Application Recognition Module: ARM (full) v3.15.1
System type: 50c
Logging: <off>
Access control: unrestricted
host uptime is 9 days, 1 hour, 8 minutes, 57 seconds

License system id: 03d2d7a29546c28c90
License status:  ** missing **
License features: Sites: 100, Packet Capture: enabled
License evaluation time total: unlimited
License evaluation time remaining: unlimited

cpu #0: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
37%
cpu #1: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
38%
cpu #2: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
37%
cpu #3: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
40%
5-minute average load (all CPUs): 20%
```

In this example, BQM is unlicensed and the license system id is displayed.

Licenses consist of a plain text file (file extension `.lic`) that must be installed. If there is an attempt to install an invalid license, or a license that doesn't match the 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 the 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, the following 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 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://sshhwindows.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 appliance, 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 Cisco ADE network settings, involving the setup of the 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 the 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 9-2 Setup Information

IP address	Specify an IP address for the appliance. 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 appliance.
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 appliance.

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 appliance 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 host name resolution:

```
host(config)$ domain name-server 192.16.24.2
```

Passive Network Quality Monitoring (PNQM) Communication Port Settings

For Passive Network Quality Monitoring (PNQM) to operate correctly between two Cisco ADEs, the BQM communication port settings on every Cisco ADE must match. The first port is for the PNQM protocol (default port: 5100) and the second is for the application layer to retrieve data from a remote BQM appliance (default port: 5101). If the default port settings are acceptable, you do not need to take any action.

To change the PNQM port parameters to different values, use the **pnqm-settings** command.

pnqm-settings port <port> [app-port <app-port>] [max-overhead percent <percentage>]

In this example, the PNQM port settings are adjusted from the default values:

```
host(config-site-router-if) # pnqm-settings port 5105 app-port 5108
```

The same port settings must be applied on all devices that will participate in PNQM measurement.

There is also an optional parameter available to adjust the global per-interface maximum limit on PNQM-generated traffic, if necessary. The default setting is 5% of interface capacity.

Restricting SNMP Access

If you are logged in as the admin user, you can restrict SNMP access to the appliance 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 is 'public'. This community string is not configurable.

Restricting IP Address Access

By default, all IP addresses are allowed to connect to the Cisco ADE. 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 appliance. 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 appliance, you type the following command:

```
host(config)$ allow 192.168.128.5
host(config)$
```



Note Restricting IP address access impacts PNQM operation. You need to make sure that any configured set of allowed IP addresses includes those of every appliance participating with the local machine in PNQM measurement.

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 appliance:

```
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 appliance:

```
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 using the **show clock** or **clock** commands.

```
host(config)$ show clock
10:42:56  7 December 2006 UTC    (UTC)
host(config)$
```

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 appliance being rebooted to ensure consistency.

clock set *hh:mm:ss day month year*

Table 9-3 **Clock Command Settings**

<i>hh:mm:ss</i>	Specify the current time in hours (24-hour format), minutes, and seconds.
<i>day</i>	Specify the current day (by number) in the month.
<i>month</i>	Specify the current month (by full name).
<i>year</i>	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 9-4 Clock Timezone Command Settings

<i>zone</i>	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 9-5 NTP Server Command Settings

<i>IP address</i>	Specify the IP v4 dotted decimal address of the server providing the clock synchronization.
<i>hostname</i>	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 information about the system, such as the software version, CPU information, and memory usage details.

```

host(config)# status
Cisco Bandwidth Quality Manager software: Version 4.0
CorvilMeter software: CDK_3_0_BUILD_42 (conf Jun 23 17:42:17 2007)
Application Recognition Module: ARM (full) v3.15.1
System type: 50c
Logging: <off>
Access control: unrestricted
host uptime is 9 days, 1 hour, 8 minutes, 57 seconds

License system id: 03d2d7a29546c28c90
License features: Sites: 100, Packet Capture: enabled
License evaluation time total: unlimited
License evaluation time remaining: unlimited

cpu #0: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
37%
cpu #1: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
38%
cpu #2: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
37%
cpu #3: "Intel(R) Xeon(R) CPU           E5335  @ 2.00GHz", 4096 KB cache,
40%
5-minute average load (all CPUs): 20%

disk #0: "Slot 0 [FUJITSU MAX3147RC      0104] Slot 1 [FUJITSU MAX3147RC
0104]", total=279662344 KB, used=6553224 KB (2%)
disk #1: "Slot 2 [FUJITSU MAX3147RC      0104] Slot 3 [FUJITSU MAX3147RC
0104]", total=280680376 KB, used=25753456 KB (9%)

6 fan component(s), 0 alert(s)
1 power supply component(s), 0 alert(s)
7 temperature sensor component(s), 0 alert(s)
BIOS date: 08/18/06

Xyratex firmware revision: 0xf500329a

Last Backup/Restore operation 'no status available for the last
backup/restore operation'
Memory: total=4138988 KB, cached=1097756 KB, used=2862536 KB (69%)
       5-minute average usage: 69%

NIC buffer usage: 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
    network service objectives: 11
    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 9-6 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	<p>Displays the following license information:</p> <p>License system id: the unique system id number required when applying for a license</p> <p>License features: the features available with the current license (100 or more sites, packet capture enabled/disabled)</p> <p>License evaluation time total: the duration of the current license</p> <p>License evaluation time remaining: the time remaining until the current license expires</p> <p>A license status is displayed when the current license is invalid.</p>
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 logical disk. See the following section “Physical and Logical Disks” for more information on how the logical disk details (disk #0, disk #1) reported map to the arrangement of physical disks in the Cisco ADE.
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.
Backup/Restore information	Displays information about the status of the most recent backup or restore attempts.

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.

Physical and Logical Disks on the Cisco ADE 2130 and 2140

The Cisco ADE 2130 uses four physical disks as two logical disks. The Cisco ADE 2140 uses six physical disks as two logical disks. Logical disk #0 is used by the system and database, and Logical disk #1 stores packet capture files.

Each physical disk denotes a single hard drive in a particular slot. On the Cisco ADE 2130 the slots are numbered as follows:

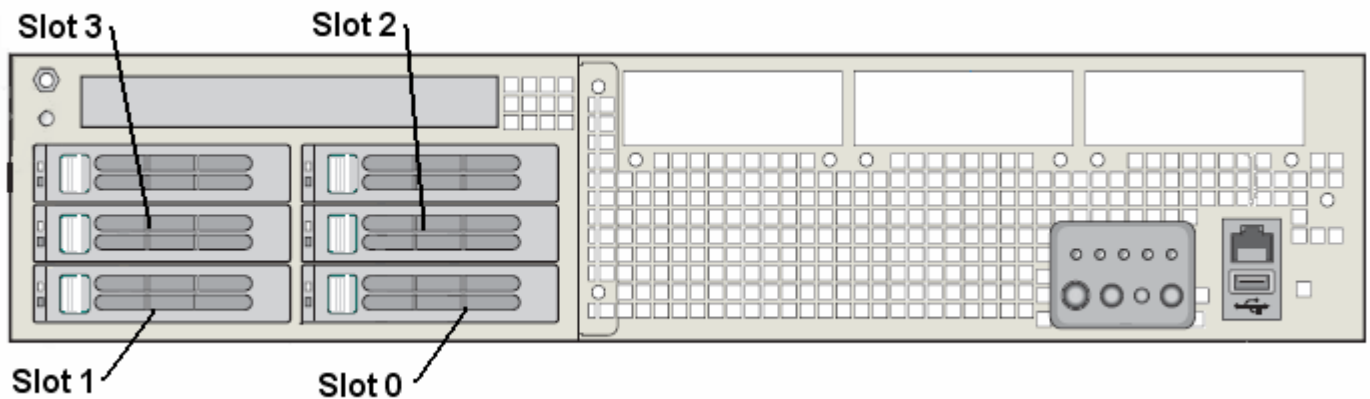
- slot 0: lower-right
- slot 1: lower-left
- slot 2: center-right
- slot 3: center-left

On the Cisco ADE 2140 the slots are numbered as follows:

- slot 0: lower-right
- slot 1: lower-left
- slot 2: center-right
- slot 3: center-left
- slot 4: upper-right
- slot 5: upper-left

The following figure show the relative positions of the physical disks on the front panels of the Cisco ADE 2130.

Figure 9-1: Cisco ADE 2130 Physical Disks



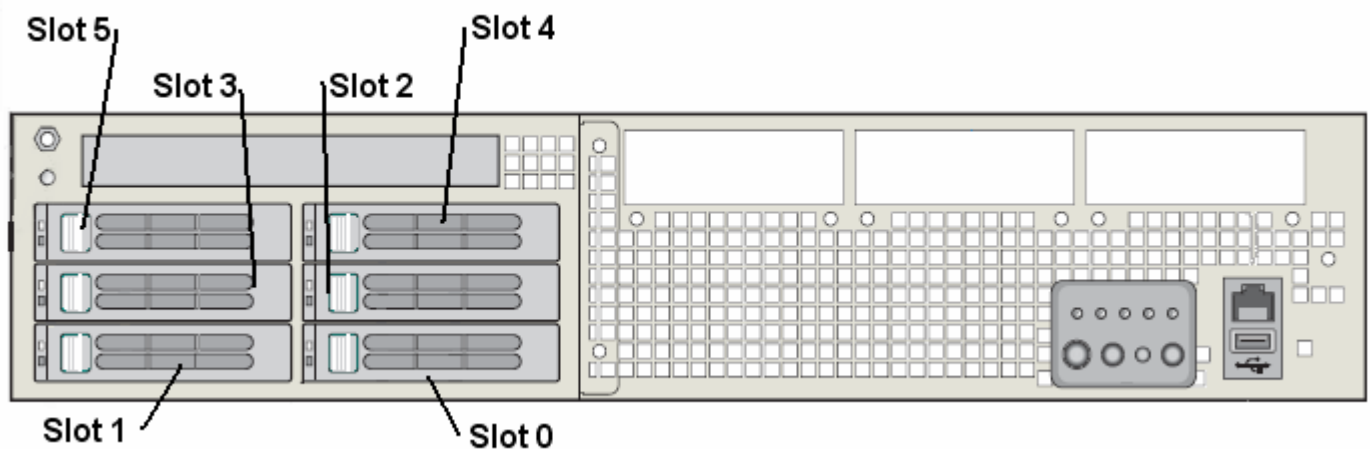
Logical disk #0, as reported in the **status** command, is a RAID volume comprising the physical disks in slot 0 and slot 1.

Logical disk #1 is a RAID volume comprising the physical disks in slot 2 and slot 3.

The top left and top right drives are not populated on the Cisco ADE 2130.

The following figure show the relative positions of the physical disks on the front panels of the Cisco ADE 2140.

Figure 9-2: Cisco ADE 2140 Physical Disks



Logical disk #0, as reported in the **status** command, is a RAID volume comprising the physical disks in slot 0 slot 1, and slot 2.

Logical disk #1 is a RAID volume comprising the physical disks in slot 3, slot 4, and slot 5.

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)

Backup and restore of data is supported within the same product version only. So a backup performed using release 4.0 can be restored using release 4.0 only.



Note We recommend that you back up your system regularly.

Restoring System Software

In general, restoring the system image involves the following steps:

1. Backup current configuration file and database
2. Perform restore – copy or ssh
3. Perform recovery mechanism and verify the restore

The system software restore can be done from the local BQM using the **copy** command from the CLI, directly from the serial console, or from a remote machine using ssh. During a restore operation, the current IP address, login settings, and configuration information are all persisted.

As a precaution, you can backup the configuration, the database and packet capture files to an FTP server or using scp. The following section describes the tasks involved in upgrading the system software. To back up the configuration and database (and optionally packet capture) data to a specified directory on an FTP server with the specified relative path, you use the **backup** 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 you can use ssh from a remote machine. To do so, you do the following:

```
ssh admin@bqm_hostname retrieve config > [file path/]file
```

In this example the BQM configuration and database (but no packet capture files) are backed up:

```
host(config)$ backup data scp://192.168.128.2/backup/1155756573_2006-08-16-192933 admin adminp4sswd
```

To restore a specified system image file from the TFTP directory on a TFTP server with the specified relative path to the appliance, 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 appliance. 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-v3.1=_trunk.22987_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 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 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
```



Note In general, we recommend that, when you have verified an upgrade of system image, you repeat the procedure to copy the chosen system image to the standby system image in order to avoid a subsequent accidental reload of an older version of the system image. Reloading an older build number will result in loss of data.



Note When restoring a backup, the backed up license file replaces the current system license. If you are restoring from a different Cisco ADE platform, you may end up with an unlicensed BQM, even if you were licensed before the restore operation. In both cases you need to re-install the required license. For more information, see the section “Installing a License.”

To restore the system image using ssh, you can do the following:

```
ssh admin@bqm_hostname install system < [file path/] file
```

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 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.



Note If you perform a BQM backup for one Cisco ADE and restore this backup to a second Cisco ADE, the restore operation overwrites the IP address settings on this second device. However, the changed IP address settings do not take effect until the next reboot of the system. So after the next reboot of the second device you will have two Cisco ADE appliances with the same IP address on the network. Similarly, a remotely-initiated restore to a Cisco ADE on a different subnet may result in this Cisco ADE becoming inaccessible after its next reboot.

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 data-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 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 Cisco ADE with host name sanfran_dc:

```
host(config)$ ssh admin@sanfran_dc install arm < arm39.arm.tar.gz
```

If you attempt to update the Cisco ADE 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:

```
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:

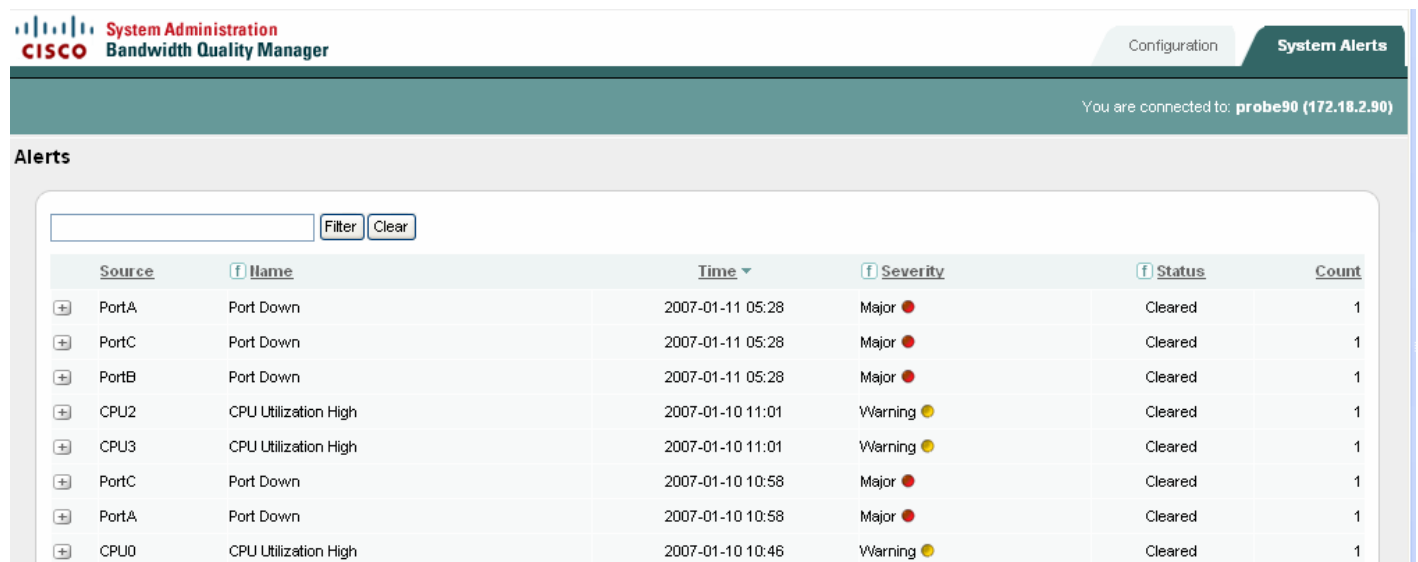
- Viewing System Alerts
- Viewing the Audit Trail
- Generating System Technical Support Diagnostic Information
- Reviewing the System Log
- Storing System Log Messages
- Watchdog Operation
- System Recovery

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 9-3 System Alerts Tab



Source	Name	Time	Severity	Status	Count
PortA	Port Down	2007-01-11 05:28	Major	Cleared	1
PortC	Port Down	2007-01-11 05:28	Major	Cleared	1
PortB	Port Down	2007-01-11 05:28	Major	Cleared	1
CPU2	CPU Utilization High	2007-01-10 11:01	Warning	Cleared	1
CPU3	CPU Utilization High	2007-01-10 11:01	Warning	Cleared	1
PortC	Port Down	2007-01-10 10:58	Major	Cleared	1
PortA	Port Down	2007-01-10 10:58	Major	Cleared	1
CPU0	CPU Utilization High	2007-01-10 10:46	Warning	Cleared	1

By default the **System Alerts** tab lists all active alerts triggered due to system events on the Cisco ADE itself. 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 BQM:

System Shutdown - indicates that the system is about to be shut down.

System Startup - indicates that the system has started up.

Database Fault - indicates a problem with the BQM database.

Fan Failure - indicates a problem with the system fan.

GPS Fault - indicates a problem with the connected GPS system, if configured

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 Utilization High - indicates that the CPU utilization is running over the 90% threshold.

System Throughput High - indicates that the average network card 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 Exceeded - indicates that the data storage disk is over 80% full.

Hard Disk Threshold Exceeded - 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. 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

Status – indicates whether the alert is active or has cleared. You can use the filter to view only active or only cleared alerts.

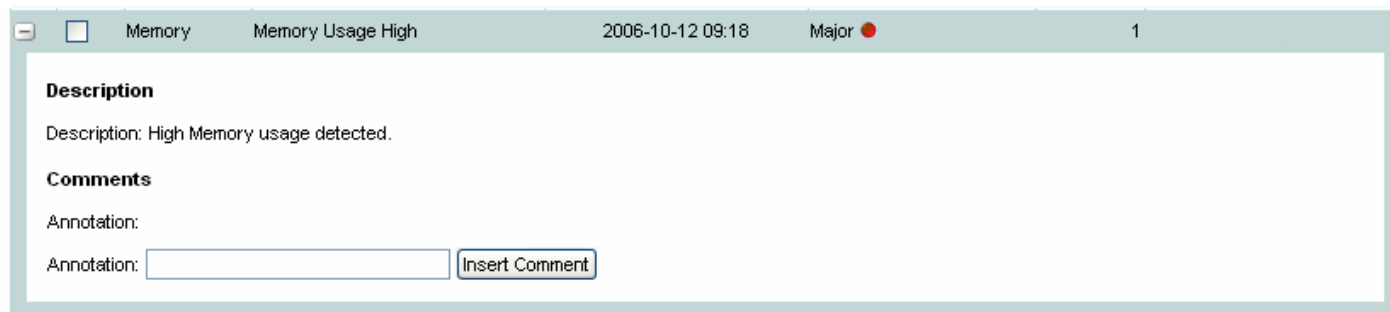
Count - the system employs a 30-minute sliding window event coalescing period to avoid the system becoming flooded with alerts. This number displays the number of individual coalesced alert triggers comprising this reported alert since an alert of this type was last cleared.

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 9-4 *Commenting a System Alert*



Step 2 Enter the comment text in the **Comments** field and click **Insert Comment**.

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.

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 2007	class	class-default	System	Adding class
Thu Sep 7 09:28:33 2007	nso-map	Inter-continent	System	Adding nso-map
Thu Sep 7 09:28:33 2007	nso-map	Internet VPN	System	Adding nso-map
Thu Sep 7 09:28:33 2007	nso-map	Metro Area	System	Adding nso-map
Thu Sep 7 09:28:33 2007	nso-map	Short Haul WAN	System	Adding nso-map
Thu Sep 7 09:28:33 2007	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, 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

BQM uses a circular log on the local system to store log messages. 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

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 BQM every three seconds. If the watchdog determines that the system is unresponsive, or that it is no longer running then the watchdog will generate an alarm and cause the system to reboot. The Cisco ADE reboots, and returns to its last known good state.

System Recovery

In the event of serious software or hardware problems that prevent you from using BQM, you should contact your sales representative. Depending on the nature of the problem, the options available to recover the system are as follows:

- Software upgrade
- Software re-installation
- Return the Cisco ADE

This section describes the procedure to perform a recovery upgrade. If you want to re-install the software using the product release CD, see the Installation Guide for instructions.



Note Performing a CD re-installation will result in all previously collected data being lost.

To perform a recovery upgrade you do the following:

Step 1 Contact your sales representative and obtain the 4.0 upgrade image.

Step 2 Locate the source of the last known good backup of the system.

Step 3 Use the following command to start the upgrade:

```
ssh admin@probe_name install system < image_name
```

So, for example to load the image file named CBQM-v4.0_RELEASE.upgrade on to a Cisco ADE named data_center you would use the following:

```
ssh admin@data_center install system < CBQM-  
v4.0_RELEASE.upgrade
```

Step 4 The machine reboots. When the Cisco ADE restarts, you are prompted to log in. You now have a running system.

Step 5 Restore the last known good backup of system data to the appliance:

```
restore data  
[scp://[hostname | IP address]/[path] username password]  
[ftp://[hostname | IP address]/[path] username password]
```



Note For details on performing backup and restore operations, see the section “Backup and Restore” in this chapter.

Configuring Fault Notification

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 Cisco ADE. This includes communications and resource faults which occur where Cisco ADE resources have degraded availability or capacity to provide the essential data.

Overview

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. 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 9-7 Quality Faults

Fault	Description	Syslog Severity	SNMP Severity	Frequency	Clear
Corvil Bandwidth Threshold Exceeded	The Corvil Bandwidth measurement indicates the class bandwidth threshold has been exceeded.	Alert	Major	Every	Yes
E2E Availability Issue	An issue with completing ICMP roundtrip measurements has been detected.	Alert	Major	Every	Yes
E2E Delay Threshold Exceeded	The ICMP Roundtrip Delay exceeded the configured threshold	Alert	Major	Every	Yes
ICMP Loss Detected	Loss of ICMP packets was detected.	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
ICMP Failure Detected	ICMP end-to-end measurement is not operating.	Error	Warning	Every	Yes
Microburst Detected	Microbursts exceeding the configured bandwidth threshold have been detected.	Alert	Major	Every	Yes
Network Service Threshold Exceeded	The Network Service Index has crossed the configured threshold.	Alert	Major	Every	Yes
PNQM Failure Detected	PNQM end-to-end measurement is not operating.	Error	Warning	Every	Yes
PNQM Latency Threshold Cleared	PNQM latency measurements have returned below the configured threshold.	Error	Warning	Every	Yes
PNQM Latency Threshold Exceeded	PNQM latency measurements are exceeding the	Error	Warning	Every	Yes

	configured threshold.				
PNQM Latency Variation Threshold Cleared	PNQM latency variation measurements have returned below the configured threshold.	Error	Warning	Every	Yes
PNQM Latency Variation Threshold Exceeded	PNQM latency variation measurements are exceeding the configured threshold.	Error	Warning	Every	Yes
PNQM Loss Threshold Cleared	PNQM loss measurements have returned below the configured threshold.	Error	Warning	Every	Yes
PNQM Loss Threshold Exceeded	PNQM loss measurements are exceeding the configured threshold.	Error	Warning	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 9-8 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	Emergency	Severe	Hourly	Yes
CPU Utilization High	Consistently high CPU usage detected.	Emergency	Warning	Hourly	No
Database Fault	Problem with the BQM database	Alert	Major	Every	No
Fan Failure	Fan failure detected.	Critical	Major	Daily	Yes
Hard Disk Threshold Exceeded	Hard disk threshold violation detected.	Emergency	Severe	Hourly	Yes
Hard Drive Failure	Hard drive failure detected.	Emergency	Severe	Daily	Yes

Port Down	Physical interface down detected.	Alert	Major	Hourly	Yes
License Expired	License expired detected.	Critical	Major	Daily	Yes
License Invalid	License invalid detected.	Critical	Major	Daily	Yes
License Near Expiration	License is near expiration.	Warning	Warning	Daily	Yes
Memory Usage High	High Memory usage detected.	Critical	Major	Every	Yes
System Throughput High	Average network card buffer utilization over 80% for a period of time.	Alert	Major	Every	Yes
Temperature High	System temperature is too high.	Alert	Major	Daily	Yes
Power Supply Failure	Power supply failure detected.	Critical	Major	Daily	Yes
Soft Disk Threshold Exceeded	Soft disk threshold violation detected.	Warning	Warning	Daily	Yes
Watchdog Restart	Watchdog has restarted.	Notification	Warning	Every	No



Note Names containing spaces must be delimited by quotes, for example: “CPU Utilization High”

You can configure different settings for any given fault using the appropriate commands. For more information, see the section “Configuring Alert Settings.”

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
snmp-server enable traps syslog destination 127.0.0.1
snmp-server fault "System Shutdown" traps Informational
report-traps syslog Informational report-syslog report-
email
freq Every

snmp-server fault "System Startup" traps Informational
report-traps syslog Informational report-syslog report-
email
freq Every

```

```
snmp-server fault "Fan Failure" traps Major report-traps
                  syslog Critical report-syslog report-email freq Daily

snmp-server fault "Power Supply Failure" traps Major
report-traps syslog Critical report-syslog report-email
freq
                  Daily

snmp-server fault "Hard Drive Failure" traps Severe
report-traps syslog Emergency report-syslog report-email
freq
                  Hourly

snmp-server fault "Port Down" traps Major report-traps syslog
Alert report-syslog report-email freq Hourly

snmp-server fault "Database Fault" traps Major report-traps
syslog Alert report-syslog report-email freq Every

snmp-server fault "System Throughput High" traps Major
report-traps syslog Critical report-syslog report-email
freq
                  Every

snmp-server fault "License Near Expiration" traps Warning
report-traps syslog Warning report-syslog report-email
freq
                  Daily

snmp-server fault "License Expired" traps Major report-traps
syslog Critical report-syslog report-email freq Daily

snmp-server fault "License Invalid" traps Major report-traps
syslog Critical report-syslog report-email freq Daily

snmp-server fault "Memory Usage High" traps Major report-traps
syslog Critical report-syslog report-email freq Every

snmp-server fault "Soft Disk Threshold Exceeded" traps Warning
report-traps syslog Warning report-syslog report-email
freq
                  Daily

snmp-server fault "Hard Disk Threshold Exceeded" traps Severe
report-traps syslog Emergency report-syslog report-email
freq
                  Hourly

snmp-server fault "Watchdog Restart" traps Warning
report-traps syslog Notification report-syslog report-
email
                  freq Every

snmp-server fault "CPU Utilization High" traps Warning
```

```

report-traps syslog Warning report-syslog report-email
freq
Every

snmp-server fault "CPU Failure" traps Severe report-traps
syslog Emergency report-syslog report-email freq Hourly

snmp-server fault "Temperature High" traps Major report-traps
syslog Alert report-syslog report-email freq Daily

snmp-server fault "GPS Fault" traps Major report-traps syslog
Alert report-syslog report-email freq Daily

snmp-server fault "E2E Delay Threshold Exceeded" traps Major
report-traps syslog Alert report-syslog freq Every

snmp-server fault "E2E Loss Detected" traps Major report-traps
syslog Alert report-syslog freq Every

snmp-server fault "E2E Availability Issue" traps Major
report-traps syslog Alert report-syslog freq Every

snmp-server fault "Network Service Threshold Exceeded" traps
Major report-traps syslog Alert report-syslog freq Every

snmp-server fault "Micro-Burst Detected" traps Major
report-traps syslog Alert report-syslog freq Every

snmp-server fault "Corvil Bandwidth Threshold Exceeded" traps
Major report-traps syslog Alert report-syslog freq Every

snmp-server fault "Expected Queuing Loss Detected" traps Major
report-traps syslog Alert report-syslog freq Every

snmp-server fault "Expected Queuing Delay Threshold Exceeded"
traps Major report-traps syslog Alert report-syslog freq
Every

snmp-server fault "Expected Policing Threshold Exceeded" traps
Major report-traps syslog Alert report-syslog freq Every

snmp-server fault "ICMP Failure Detected" traps Warning
report-traps syslog Error report-syslog freq Every

snmp-server fault "PNQM Failure Detected" traps Warning
report-traps syslog Error report-syslog freq Every

snmp-server fault "PNQM Latency Threshold Cleared" traps
Warning report-traps syslog Error report-syslog freq
Every

snmp-server fault "PNQM Latency Threshold Exceeded" traps
Warning report-traps syslog Error report-syslog freq
Every

```

```
snmp-server fault "PNQM Latency Variation Threshold Cleared"
                  traps Warning report-traps syslog Error report-syslog
freq
                  Every

snmp-server fault "PNQM Latency Variation Threshold Exceeded"
                  traps Warning report-traps syslog Error report-syslog
freq
                  Every

snmp-server fault "PNQM Loss Cleared" traps Warning
                  report-traps syslog Error report-syslog freq Every

snmp-server fault "PNQM Loss Detected" traps Warning
                  report-traps syslog Error report-syslog freq Every
```

```
cnse2(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.



10 CLI Command Reference

This chapter provides information on each of the CLI commands available on the BQM.

Configuration Mode

The following table lists the configuration and administration commands available in global configuration mode when you log in to the device initially. Typically commands that are available in global configuration mode are also available in a 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 v4 addresses or subnets to access the Cisco ADE 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	Creates a packet capture instance. This will automatically move you into capture configuration mode.
capture-settings	Configures global packet capture parameters: disk space quota and capture file password
class-map	Creates a class-map. This will automatically move you into class-map configuration mode.
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.
custom-application	Configures a custom application.
custom-dashboard	Configures a custom dashboard for display in the GUI.
delete	Deletes packet capture files from the file system.

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.
exit	Quit the current configuration mode. If used in configuration mode, you are logged out.
gps	Enables or resets operation of a connected GPS system.
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
local-site	Configures a representation of the local site.
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.
more	Lists the contents of a file.
no	Deletes an object or entry. An object that is being used by another object cannot be deleted.
nso-map	Creates a network service objective. This will automatically move you into network service objective configuration mode.
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.
pnqm-settings	Sets the port and application port parameters that must match on each pair of BQM appliances participating in PNQM measurement. Also sets the upper limit on the amount of signature traffic generated per interface during PNQM operation.
policy-map	Creates a policy-map. This will automatically move you into Policy-map configuration mode.
port	Specifies the Ethernet operation of the selected Cisco ADE physical 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 network service objectives.
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.
site	Creates a representation of a remote site, defined at a minimum by specifying network subnets. Interfaces are then defined under sites and their routers.
snmp-server	Specifies the SNMP community strings (passwords) for SNMP set and get commands to restrict SNMP access to the Cisco ADE. Supports configuration of BQM fault notification.
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.
status	Reports the current BQM status.
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 for BQM configuration:

- 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 (..)

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
<code>description</code>	Adds a text description to a class-map.
<code>match</code>	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.

Custom-Dashboard Configuration Mode

You use custom-dashboard configuration mode to define the contents of a custom dashboard for display in the GUI. The following lists the commands available when defining a custom dashboard.

Command	Description
<code>class</code>	Adds a class to a custom dashboard.
<code>display</code>	Enables display of a defined custom dashboard in the GUI.
<code>graph-order</code>	Defines the order in which graphs are displayed for classes in the custom dashboard.

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
<code>class</code>	Creates a policy-map entry that matches a previously configured class-map.
<code>description</code>	Adds a text description to a policy-map.
<code>down</code>	Moves a class down in the list of policy-map classes.
<code>nso</code>	Creates a policy-map entry that matches a previously configured network service objective.
<code>trace-events</code>	Enables rolling event detection packet capture for a policy-map.
<code>up</code>	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
<code>bandwidth</code>	Specifies or modifies bandwidth allocated for a policy-map class.
<code>class-adjust</code>	Modifies the size of packets which match this class. The size is specified in bytes and can be either a specific number or an identifier with optional modifier.
<code>nso</code>	Creates a class entry that matches a previously configured network service objective.
<code>priority</code>	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.

Network Service Objective Configuration Mode

When you define a network service objective using the **nso-map** command, you are brought directly into this mode.

Command	Description
description	Adds a text description for a network service objective.
measure-eq	Enables Network Service Index and Expected Queuing calculations for a class. The optional keywords enable detection of events using the configured one-way latency or queuing-target as the delay threshold, and the configured protect-packets percentage as the basis for the loss threshold (For example, protect-packets percent 99.9 implies a loss threshold of 0.1% of packets).
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-icmp	Enables ICMP ping measurement and associated event detection thresholds.
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.
measure-pnqm	Specifies passive network quality monitoring measurements, and sets optional event detection thresholds.
one-way-latency	Specifies the maximum tolerable one-way packet delay for end-to-end measurements, with an option to specify a maximum one-way latency variation.
protect-packets	Specifies the packet protection target and busy period values for network service index and bandwidth sizing calculation. The configured percentile value is also used to display graph data.
queuing-targets	Specifies the delay and loss queuing targets to override one-way latency and packet protection target settings for Expected Queuing and Corvil Bandwidth for 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
<code>description</code>	Adds a text description to the default local site.
<code>router</code>	Creates a router for the default local site.
<code>subnet</code>	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
<code>description</code>	Adds a text description to a class-map.
<code>router</code>	Creates a router for a given site.
<code>subnet</code>	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
<code>attached-port</code>	Specifies which physical ports (PortA, PortB, PortC, PortD) to use for traffic measurement for a local site only.
<code>description</code>	Adds a text description to a router.
<code>interface</code>	Creates a model interface for a router. An interface is used to measure traffic outbound from the perspective of a given site.
<code>peer-interface</code>	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 physical interfaces: PortA, PortB, PortC, and PortD. These interfaces cannot be renamed or deleted.

Command	Description
<code>bandwidth</code>	Specifies a bandwidth allocation for the interface.
<code>connects-to</code>	Specifies the local site interface to which the chosen remote site interface is connected in a point-to-point deployment.
<code>description</code>	Adds a text description to an interface.
<code>filter-class</code>	Specifies a class-map on which to base interface traffic filtering.
<code>link-adjust</code>	Specifies a packet size adjustment value for an interface.
<code>max-reserved-bandwidth</code>	Specifies the maximum reserved bandwidth value for an interface.
<code>ping-address</code>	Specifies the ICMP responder address for end-to-end ping measurements from this interface.
<code>ping-address-test</code>	Sends test packets to the configured ICMP responder address to verify connectivity.
<code>pnqm-server</code>	Defines a PNQM measurement channel between the interface and a remote site interface.
<code>pnqm-server-test</code>	Sends test traffic to the remote site interface to verify PNQM connectivity.
<code>ppp</code>	Specifies that link fragmentation and interleaving is enabled for an interface.
<code>service-policy</code>	Adds a service-policy for the output direction of an interface.
<code>subnet-filtering</code>	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 physical interfaces: PortA, PortB, PortC, and PortD. These interfaces cannot be renamed or deleted.

Command	Description
<code>bandwidth</code>	Specifies a bandwidth allocation for the peer-interface.
<code>description</code>	Adds a text description to a peer-interface.
<code>filter-class</code>	Specifies a class-map on which to base interface traffic filtering.
<code>link-adjust</code>	Specifies a packet size adjustment value for an interface.
<code>max-reserved-bandwidth</code>	Specifies the maximum reserved bandwidth value for an interface.
<code>ppp</code>	Specifies that link fragmentation and interleaving is enabled for an interface.
<code>service-policy</code>	Adds an input service-policy for the output direction of a peer-interface.
<code>subnet-filtering</code>	Specifies that interface packet filtering is based on the associated site subnet(s).

You do not need to explicitly configure PNQM for peer-interfaces as long as the corresponding interfaces are correctly configured.

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 capture configuration mode:

Command	Description
<code>attach interface</code>	Attaches the relevant packet capture instance to a specific, named interface.
<code>duration</code>	Sets the maximum duration for the packet capture. When the configured time is reached, packet capture is stopped automatically.
<code>start</code>	Starts packet capture. Use the no start command to stop packet capture.
<code>size</code>	Sets the maximum file size for the packet capture. When the configured file size is reached, packet capture is stopped automatically.
<code>snaplength</code>	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), 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)$ ?
(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
  custom-dashboard Configure a custom-dashboard
  delete          Delete files and/or directories from a filesystem
  dir             List files on a specified filesystem
  domain          Configures DNS Name Servers.
  end             Return to base context
  exit            Exit configuration mode or EXEC
  gps             Enable or disable USB-based GPS clock
  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.
-- More --	

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 Cisco ADE 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 Cisco ADE, that is different from the IP address you are currently using to access the appliance.

The IP address you are currently using to access the Cisco ADE might be different from the device from which you are logged in to BQM. This is usual in the case where you are logged in via a proxy device.

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 Cisco ADE.
<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 BQM. The **allow** command is used to allow devices 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 Cisco ADE. 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 Cisco ADE:

```
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

<i>site name</i>	Specify the name of the site in which the interface is configured.
<i>router name</i>	Specify the name of the router for which the interface is configured.
<i>interface-name</i>	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

<i>port</i>	Specifies the name of the measurement port: Port A, PortB, PortC, PortD.
<i>inbound</i>	Specifies inbound traffic to the local site.
<i>outbound</i>	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 they are not specified.

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 most recent backup operation.
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 must 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 an error is displayed and the service policy is not attached to that interface.
- 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

<i>bandwidth-kbps</i>	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 – 20,000,000 kbps
remaining percent <i>percentage</i>	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%
<code>percent <i>percentage</i></code>	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
```

Mode

Site router interface configuration
`host(config-site-router-if)#`

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

<i>bandwidth-kbps</i>	Specifies the bandwidth of the model interface, in kilobits per second (kbps). Range: 1 – 20,000,000 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

<i>name</i>	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 Cisco ADE employs a separate logical hard disk configuration 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

Custom dashboard configuration

host(config-pmap)#

host(config-custom-dashboard)#

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.

You can also use the **class** command when defining the class-maps to be monitored in a custom dashboard. There is no limit to the number of class-maps that can be used in a custom dashboard definition, but a given class-map can be used only once.

class {*class-map name* | class-default}

no class {*class-map name* | class-default}

Syntax Description

<i>class-map name</i>	Specify the name of the previously configured class-map (case-sensitive) to be referenced in the policy-map, or monitored in the custom dashboard.
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'.

Examples

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
```

In this example, a custom dashboard is defined and a number of class-maps are specified. Results for these class-maps will be monitored in the new tab defined in the GUI:

```
host(config)# custom-dashboard Telepresence
host(config-custom-dashboard)# class video_tp
host(config-custom-dashboard)# class video
host(config-custom-dashboard)# class video_all
host(config-custom-dashboard)# class voice
host(config-custom-dashboard)# class class-default
```

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

<i>adjust identifier</i>	Specifies an identifier to use. Currently the only identifier supported is cRTP, which maps to a class-adjust value of -36.
<i>modifier</i>	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.
<i>class-map name</i>	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 <i><interface-name></i>	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 timezone** command.

Setting the clock results in the Cisco ADE being rebooted to ensure consistency.

clock set [*hh:mm:ss day month year* | *ntp*]

Syntax Description

<i>hh:mm:ss</i>	Specify the current time in hours (24-hour format), minutes, and seconds.
<i>day</i>	Specify the current day (by number) in the month.
<i>month</i>	Specify the current month (by full name).
<i>year</i>	Specify the current year (four digits, no abbreviation).
<i>ntp</i>	Specify that the clock is to be synchronized by NTP time source.

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

<i>zone</i>	<p>Name of the time zone, as per Java. The complete list of available Java time zone names is as follows:</p> <ul style="list-style-type: none"> 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, Europe/CET_CEST_Bel (GMT+02:00) Belgrade, Bratislava, Budapest,. 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, 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
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.
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

<i>local-site</i>	Specify the name of the local site to which the chosen remote site interface is connected.
<i>router</i>	Specify the name of the local site router to which the chosen remote site interface is connected.
<i>interface</i>	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 Data center 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 Cisco ADE.

Configuration Files

The file system contains a time stamped copy of each BQM configuration file at user login or the last time the current active configuration was explicitly saved to a configuration file. Note configuration changes are implicitly saved after syntax and semantic validation. The configurations due to login are automatically generated, current active configuration changes are explicitly saved to a configuration file 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 28 th 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> | tftp://[hostname|A.B.C.D]/<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 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.
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 file system. The file is identified by [file path/]<filename>.
arm	Specifies that the file being copied by tftp to the Cisco ADE 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 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

<i>name</i>	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" network service objective. In the CLI you see:

```
class-map market-data
  match application market-data

policy-map low-speed
  class market-data
    bandwidth percent 20
  nso 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
```

custom-dashboard

Mode

Configuration
host(config)#

Usage Guidelines

To define a custom dashboard to be displayed in a new tab in the GUI, you use the **custom-dashboard** command. Only one custom dashboard can be defined at any one time. Using this command brings you directly into custom-dashboard configuration mode, where you define the contents of the custom dashboard.

When you are in custom dashboard configuration mode you can specify which classes to monitor, the graphs to display, and the order in which the chosen graphs should be shown. An empty defined custom dashboard is valid. There is no default list of displayed graphs when a custom dashboard is first defined. See the command reference information for the **class**, **graph** and **graph-order** commands for more information. To remove a custom dashboard you use the **no** form of the command.

There is no limit to the number of named class-maps that can be defined for a custom dashboard, but a given class-map can be used only once.

custom-dashboard <name>
no custom-dashboard <name>

Syntax Description

<i>name</i>	Specify a unique name for the custom dashboard. The name specified here will be displayed as the name of the GUI tab for the custom dashboard. Because there can be a total of seven tabs displayed in the GUI, it is recommended that you use a concise name. The maximum length allowable is 15 characters.
-------------	---

Example

For example, you can define a new tab in the GUI named TelePresence as follows:

```
host(config)# custom-dashboard TelePresence
host(config-custom-dashboard)#
```

decapsulate

Mode

Configuration

```
host(config)#
```

Usage Guidelines

To enable protocol decapsulation for the GRE protocol, use the **decapsulate** command.

When using the BQM in WAAS WAN acceleration environments, in which the accelerated traffic seen arriving at a branch is GRE-encapsulated, enabling GRE decapsulation will strip off a single layer of GRE encapsulation from IP-GRE packets, presenting the GRE payload packet to the higher level layers in the stack.

When GRE decapsulation is enabled, you can define a class-map match rule to match GRE-decapsulated traffic using the **match gre** command.

Use **no decapsulate gre** to disable GRE protocol decapsulation. This is the default BQM setting. When GRE protocol decapsulation is disabled, any configured class-map match rules using the **match gre** command will not match any traffic.

The purpose of GRE decapsulation is, primarily, to support the deployment of PNQM in situations where the BQM at one end of the PNQM channel sees GRE-encapsulated packets, and the BQM at the other end sees the very same packets but without GRE encapsulation.

GRE-decapsulation is controlled via the **decapsulate gre** command, which is applied at the top level in the configuration file. When enabled, GRE-encapsulated packets will have the GRE header stripped off before the packet is presented to the higher layers in the BQM packet processing stack.

In particular, when **decapsulate gre** is enabled:

1. Layer-7 application recognition examines the GRE-payload packet. Thus, unless the GRE-payload happens to contain another layer of GRE-encapsulation, the top applications statistics will not show any GRE traffic.
2. class-map match rules operate on the GRE-payload, that is, they will match the IP/TCP/UDP headers within the GRE-encapsulated packet. This includes matching on configured subnets, for example.
3. PNQM hash calculations are based on the GRE-encapsulated packet.
4. Event Analysis reporting is based on the GRE-encapsulated packet.
5. If there is a non-zero snaplength applied to manual captures, the capture files will include the packet as seen on the wire – that is, the capture files will include the layer-2 header, the outer IP header, the GRE header and the payload packet, assuming sufficient snaplength.
6. Flows that appear both GRE-encapsulated and non GRE-encapsulated will be counted as separate flows (for example, in new flow accounting and top conversations lists). This could mean that there are two apparently identical flows in the top-conversations list.

There is a related **(no) match gre** rule available to the class-map classification rules. The semantics of **match gre** are that it matches traffic that has been GRE-decapsulated. Note that **match gre** will not match any traffic unless **decapsulate gre** is enabled.

The purpose of the **match gre** rule is to support environments in which the BQM sees packets both before and after GRE-encapsulation. The **match gre** rule makes it possible to distinguish these flows, avoiding PNQM hash collisions.

PNQM only supports GRE-encapsulation of IP packets – that is, where the GRE payload type is 0x0800. In particular, the current release does not support packets forwarded via WCCP over GRE.

decapsulate gre **no decapsulate gre**

Syntax Description

This command has no parameters.

Example

In this example, GRE decapsulation is enabled:

```
host(config)# decapsulate gre  
host(config)#
```

In this example, GRE decapsulation is disabled:

```
host(config)# no decapsulate gre  
host(config)#
```

In this example configuration fragment, the BQM sees packets before and after a GRE tunnel. We want to monitor the traffic inside the GRE tunnel:

```
decapsulate gre  
  
class-map gre-tunnel  
  match gre  
  
site branch1  
  subnet 10.1.0.0/24  
  ! note that the GRE-payload must have IP addresses in the  
  ! 10.1.0.0/24 subnet. The IP address of the outer IP header  
  ! will be ignored.  
  router default  
    interface default  
      filter-class gre-tunnel !ignore non GRE-encapsulated traffic
```

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 `arm:`, `backup:`, `capture:`, `cfg:`, `license:`, or `log:` 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 Cisco ADE 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] {**arm:** | **backup:** | **capture:** | **cfg:** | **license:** | **log:**} <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)
Network service objective configuration
host(config-nso-map)
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, nso-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

<i>text</i>	A single word, without double quotes, describing the class-map, custom application, policy-map, nso-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 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: backup:, 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

<i>file-url</i>	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_2007-09-13-131852-416015.cfg
      1164  bqm_2007-09-13-131853-023456.cfg
      1164  bqm_2007-09-13-131856-423457.cfg
      1164  bqm_2007-09-13-131900-043456.cfg
      1164  bqm_2007-09-13-131922-023336.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)$
```

display

Mode

Custom-dashboard configuration

`host(config-custom-dashboard)`

Usage Guidelines

To enable display of a custom-dashboard in the GUI use the **display** command. Use **no display** to disable display of a custom-dashboard.

display
no display

Syntax Description

This command has no parameters.

Example

In this example, display of a defined custom-dashboard is enabled:

```
host(config-custom-dashboard)$ display
```

domain

Mode

Configuration
`host(config)`

Usage Guidelines

To define DNS Name Servers that can be used by the Cisco ADE 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 be 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

<i>ip-address</i>	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 Cisco ADE host name resolution:

```
host(config)$ domain name-server 192.16.24.2
```

down

Mode

Policy-map configuration
(`config-pmap`)

Usage Guidelines

To move a class down in the list of defined classes in a policy-map, use the **down** command in policy-map configuration mode. By default the specified class is moved down one place. This can be changed by specifying the number of places, for example to move a class down three places. See the **up** command for information on moving classes up in a policy-map list.

Order of classes is important in 'match-first' policy-maps whereby only the first matching class matches traffic and subsequent classes further down the list are not matched.

down [*<number places>*] *<class name>*

Syntax Description

<i>number places</i>	Specifies the number of places down the list by which the specified graph is moved. By default the specified graph is moved down one place.
<i>class name</i>	Specifies the name of the class to be moved.

Example

In this example, the video class moved down the list of classes by one place:

```
host(config-pmap)# down video
```

In this example, the bulk class moved down the list of classes by two places:

```
host(config-pmap)# down 2 bulk
```

Mode

Custom dashboard graph order configuration
host(`config-custom-dashboard-go`)

Usage Guidelines

To move a specified graph down in the display order list for a defined custom dashboard tab in the GUI, use the **down** command in policy-map configuration or custom dashboard configuration mode respectively. See the **up** command for information on moving graphs up the display order list.

When you re-order the list of displayed graphs, the changes are displayed in the GUI tab following the next data summarization update for the chosen GUI reporting period. For example, if the 24-hour reporting period is selected in the GUI, the changes will be updated in the GUI tab after five minutes.

down [*<number places>*] *<graph name>*

Syntax Description

<i>number places</i>	Specifies the number of places down the list by which the specified graph is moved. By default the specified graph is moved down one place.
<i>graph name</i>	<p>Specifies the name of the graph to be moved.</p> <p>The list of available graphs is as follows (in the default order):</p> <ul style="list-style-type: none"> Microburst-detection "Average Rate" "Packet Rate" Peak-to-mean "Packet Size distribution (by bytes)" "Packet Size distribution (by packets)" "Top 10 Applications" "Top 10 Talkers" "Top 10 Listeners" "Top 10 Conversations" "Corvil Bandwidth - Delay" "Corvil Bandwidth - Queue Length" "5 minute Network Service Index" "End-to-end Delay" "End-to-end Jitter" "End-to-end Loss" "EQ Delay" "EQ Delay variation" "EQ Loss" "Interface ICMP Round-trip Delay" <p>Graph names with spaces between words must be enclosed in quotes (" ") when being specified in a command.</p>

Example

In this example, the Top 10 Conversations chart is moved down the list of displayed graphs by one place:

```
host(config-custom-dashboard-go)# down "Top 10 Conversations"
```

In the following example, the GUI End-to-End Latency graph is moved down the list of displayed graphs by three places:

```
host(config-custom-dashboard-go)# down 3 "End-to-end Delay"
```

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

<i>time</i>	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
```

ethernet

Mode

Port configuration

```
host(config-port)#
```

Usage Guidelines

To configure the Ethernet operation for 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 auto-negotiation 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

<i>class-map name</i>	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 mpls tags
```

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 vls tags  
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 vls tags  
host(config-site-router-pif)$ end
```

gps

Mode

```
host(config)$
```

Usage Guidelines

The Passive Network Quality Monitoring (PNQM) feature will give the BQM platform the ability to passively measure one-way latency for every packet. This will enable the analysis and presentation required to manage end-to-end network service quality. However, the current presentation of the one-way latency measurements plots a Max Directional Offset due to the unknown asymmetry in the end to end measured latency. The optional GPS-enabled solution will remove this uncertainty from the measurements.

To enable and start polling a GPS clock connected to the USB port, use the **gps** command. You must be logged in as admin to use this command.

Use **no gps enable** to disable GPS clock.

Use **gps reset** to reconfigure the GPS device with the factory default configuration.

gps enable | reset
no gps enable

Example

In this example, the USB-connected GPS clock is enabled:

```
host(config)$ gps enable
```

In the following example, the factory default settings are restored:

```
host(config-custom-dashboard-go)$ gps reset
```

graph

Mode

Custom dashboard graph order configuration
host (config-custom-dashboard-go)

Usage Guidelines

To add a specified graph to the bottom of the display order list for a defined custom dashboard tab in the GUI, use the **graph** command in custom dashboard graph order configuration mode. To remove a specified graph from the list, use the no form of the command. If auto-completion is used when selecting the graph name, then the list of options displayed includes only those graph names not already selected. See the **up** and **down** commands for information on moving graphs up and down the display order list.

When you amend the list of displayed graphs, the changes are displayed in the GUI tab following the next data summarization update for the chosen GUI reporting period. For example, if the 24-hour reporting period is selected in the GUI, the changes will be updated in the GUI tab after five minutes.

graph <graph name>
no graph <graph name>

Syntax Description

<i>graph name</i>	<p>Specifies the name of the graph to be added or removed.</p> <p>The list of available graphs is as follows:</p> <p>Microburst-detection "Average Rate" "Packet Rate" Peak-to-mean "Packet Size distribution (by bytes)" "Packet Size distribution (by packets)" "Top 10 Applications" "Top 10 Talkers" "Top 10 Listeners" "Top 10 Conversations" "Corvil Bandwidth - Delay" "Corvil Bandwidth - Queue Length" "5 minute Network Service Index" "End-to-end Delay" "End-to-end Jitter" "End-to-end Loss" "EQ Delay" "EQ Delay variation" "EQ Loss" "Interface ICMP Round-trip Delay"</p> <p>Graph names with spaces between words must be enclosed in quotes (“ ”) when being specified in a command.</p>
-------------------	--

Example

In this example, the Top 10 Conversations chart is added to the bottom of the list of displayed graphs in the GUI tab:

```
host(config-custom-dashboard-go)# graph "Top 10 Conversations"
```

In the following example, the GUI End-to-End Latency graph is removed from the list of displayed graphs in the GUI tab:

```
host(config-custom-dashboard-go)# no graph "End-to-end Delay"
```

graph-order

Mode

Custom dashboard configuration
host (config-custom-dashboard)

Usage Guidelines

When a custom dashboard is first defined, the list of displayed graphs is empty; there is no default set of displayed graphs. To set (or reset) the default list of displayed graphs in the GUI tab for a defined custom dashboard, or to enter graph order configuration mode to manually change the display order list for a defined custom dashboard, use the **graph-order** command in custom dashboard configuration mode. To remove the complete set of graphs from the GUI custom dashboard tab, use the no form of the command. See the **up** and **down** commands for information on moving graphs up and down the display order list.

When you amend the list of displayed graphs, the changes are displayed in the GUI tab following the next data summarization update for the chosen GUI reporting period. For example, if the 24-hour reporting period is selected in the GUI, the changes will be updated in the GUI tab after five minutes.

graph-order [full-list]
no graph-order

Syntax Description

full-list	<p>[Optional] Specifies that all available graphs are displayed in the custom dashboard GUI tab in their default order.</p> <p>The list of graphs in default order is as follows:</p> <p>Microburst-detection "Average Rate" "Packet Rate" Peak-to-mean "Packet Size distribution (by bytes)" "Packet Size distribution (by packets)" "Top 10 Applications" "Top 10 Talkers" "Top 10 Listeners" "Top 10 Conversations" "Corvil Bandwidth - Delay" "Corvil Bandwidth - Queue Length" "5 minute Network Service Index" "End-to-end Delay" "End-to-end Jitter" "End-to-end Loss" "EQ Delay" "EQ Delay variation" "EQ Loss" "Interface ICMP Round-trip Delay"</p>
-----------	---

Example

In this example, the default set of displayed graphs is specified for a custom dashboard:

```
host(config)# custom-dashboard Telepresence  
host(config-custom-dashboard)# graph-order full-list
```

In the following example, the **graph-order** command is used without the optional full-list parameter to enter graph order configuration mode so that the list of displayed graphs in a custom dashboard can be changed manually:

```
host(config)# custom-dashboard Telepresence  
host(config-custom-dashboard)# graph-order  
host(config-custom-dashboard-go)# up 4 "End-to-end Delay"  
host(config-custom-dashboard-go)# no graph "End-to-end Delay variation"
```

In the following example, the **no graph-order** command is used to remove the set of displayed graphs for the custom dashboard:

```
host(config)# custom-dashboard Telepresence  
host(config-custom-dashboard)# no graph-order
```


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

<i>command name</i>	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
  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
  custom-dashboard Configure a custom-dashboard
  decapsulate     Enables protocol decapsulation
  delete          Delete files and/or directories from a filesystem
  dir             List files on a specified filesystem
  domain          Configures DNS Name Servers.
  end             Return to base context
  exit            Exit configuration mode or EXEC
  gps            Enable or disable USB-based GPS clock
  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.
-- 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 Cisco ADE measurement interface names PortA, PortB, PortC, and PortD are fixed and cannot be deleted.

```
interface <interface name>
no interface <interface name>
```

Syntax Description

<i>interface name</i>	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

<i>install</i>	Installs a license file.
<i>remote filename</i>	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

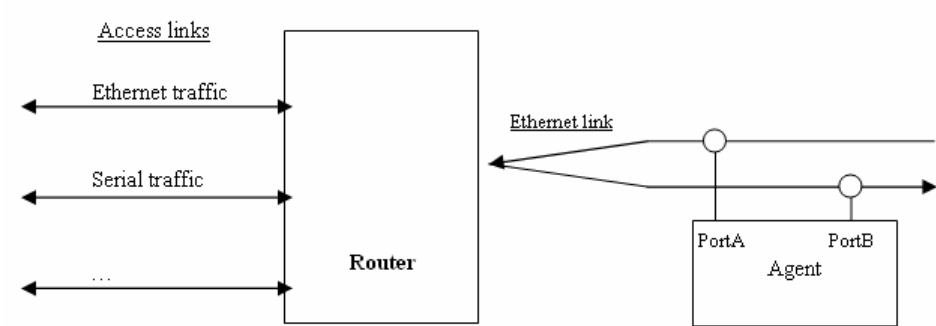
Mode

Site router interface configuration
host(config-site-router-if)#
Site router peer-interface configuration
host(config-site-router-pif)#

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.

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 Cisco ADE 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

<i>adjustment value</i>	Specifies a value to allow for link overhead adjustments when determining the correct number of bytes in a packet. The <i>adjustment-value</i> 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 <i>adjustment-value</i> 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 Cisco ADE, 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.

local-site <name>

Syntax Description

<i>name</i>	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.
<i>-<number of lines></i>	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]} | [**host** {[hostname | IP address]} [**transport udp** [port port]]]

Syntax Description

<i>hostname</i>	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.
<i>IP address</i>	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 | gre | 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,.-_]
```

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

<i>name</i>	Specify a configured custom application or a predefined application, for example, appletalk, ipx, eigrp, icmp.
<i>property-key</i>	<p>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.</p> <p>No default.</p>
<i>property-value</i>	<p>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/*'.</p> <p>No default.</p>

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

<i>class-map name</i>	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	match ethertype=0x8137
Reverse Address Resolution Protocol (RARP)	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

<i>ethertype value</i>	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 gre

Mode

Class-map configuration
host(config-cmap)#

Usage Guidelines

To configure the match criteria for a class-map to match GRE-decapsulated traffic, use the **match gre** command.

The **match gre** will not match any traffic unless the **decapsulate gre** command has already been used and GRE decapsulation by the system is enabled.

To remove the **match gre** rule, use the no form of the command.

match gre
no match gre

Syntax Description

This command has no arguments or keywords.

Example

In this example, the class-map match criterion is configured to be successful only for GRE-encapsulated packets:

```
match gre
```

In this example, the BQM sees packets before and after a GRE tunnel. We want to monitor the traffic inside the GRE tunnel:

```
decapsulate gre
```

```
class-map gre-tunnel  
  match gre
```

```
site branch1  
  subnet 10.1.0.0/24  
  ! note that the GRE-payload must have IP addresses in the  
  ! 10.1.0.0/24 subnet. The IP address of the outer IP header  
  ! will be ignored.  
  router default  
    interface default  
      filter-class gre-tunnel !ignore non GRE-encapsulated traffic
```

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>	<p>Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match.</p> <p>The current release supports only the numerical specification. Here are the keywords:</p> <p><0-63> Differentiated services codepoint value</p> <p>af11 Match packets with AF11 dscp (001010) == 10</p> <p>af12 Match packets with AF12 dscp (001100) == 12</p> <p>af13 Match packets with AF13 dscp (001110) == 14</p> <p>af21 Match packets with AF21 dscp (010010) == 18</p> <p>af22 Match packets with AF22 dscp (010100) == 20</p> <p>af23 Match packets with AF23 dscp (010110) == 22</p> <p>af31 Match packets with AF31 dscp (011010) == 26</p> <p>af32 Match packets with AF32 dscp (011100) == 28</p> <p>af33 Match packets with AF33 dscp (011110) == 30</p> <p>af41 Match packets with AF41 dscp (100010) == 34</p> <p>af42 Match packets with AF42 dscp (100100) == 36</p>

	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>	<p>Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match.</p> <p>The current release supports only the numerical specification. Here are the keywords:</p> <p><0-63> Differentiated services codepoint value</p> <p>af11 Match packets with AF11 dscp (001010) == 10</p> <p>af12 Match packets with AF12 dscp (001100) == 12</p> <p>af13 Match packets with AF13 dscp (001110) == 14</p> <p>af21 Match packets with AF21 dscp (010010) == 18</p> <p>af22 Match packets with AF22 dscp (010100) == 20</p> <p>af23 Match packets with AF23 dscp (010110) == 22</p> <p>af31 Match packets with AF31 dscp (011010) == 26</p> <p>af32 Match packets with AF32 dscp (011100) == 28</p> <p>af33 Match packets with AF33 dscp (011110) == 30</p> <p>af41 Match packets with AF41 dscp (100010) == 34</p>

	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>	<p>Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match.</p> <p>The current release supports only the numerical specification. Here are the keywords:</p> <p><0-63> Differentiated services codepoint value</p> <p>af11 Match packets with AF11 dscp (001010) == 10</p> <p>af12 Match packets with AF12 dscp (001100) == 12</p> <p>af13 Match packets with AF13 dscp (001110) == 14</p> <p>af21 Match packets with AF21 dscp (010010) == 18</p> <p>af22 Match packets with AF22 dscp (010100) == 20</p> <p>af23 Match packets with AF23 dscp (010110) == 22</p> <p>af31 Match packets with AF31 dscp (011010) == 26</p> <p>af32 Match packets with AF32 dscp (011100) == 28</p> <p>af33 Match packets with AF33 dscp (011110) == 30</p>

	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 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 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

<i>vlan id</i>	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>	<p>Matches a dscp value from 0 to 63. Cannot be used with tos or precedence commands in a single match.</p> <p>The current release supports only the numerical specification. Here are the keywords:</p> <p><0-63> Differentiated services codepoint value</p> <p>af11 Match packets with AF11 dscp (001010) == 10</p> <p>af12 Match packets with AF12 dscp (001100) == 12</p> <p>af13 Match packets with AF13 dscp (001110) == 14</p> <p>af21 Match packets with AF21 dscp (010010) == 18</p> <p>af22 Match packets with AF22 dscp (010100) == 20</p> <p>af23 Match packets with AF23 dscp (010110) == 22</p> <p>af31 Match packets with AF31 dscp (011010) == 26</p> <p>af32 Match packets with AF32 dscp (011100) == 28</p> <p>af33 Match packets with AF33 dscp (011110) == 30</p> <p>af41 Match packets with AF41 dscp (100010) == 34</p> <p>af42 Match packets with AF42 dscp (100100) == 36</p> <p>af43 Match packets with AF43 dscp (100110) == 38</p>

	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 peer-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

<i>percent</i>	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

Network service objective Configuration
host (config-nso-map) #

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 the one-way latency or queuing-targets and the packet protection targets in the associated network service objective. The **no** version of this command disables Corvil Bandwidth measurement.

measure-bandwidth [event-threshold {**bandwidth** *kbps* | **percent** *percent*}
no measure-bandwidth

Syntax Description

<i>kbps</i>	Specifies the event threshold bandwidth value in kilobits per second. Range: 1-20,000,000 kbps. No default.
<i>percent</i>	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 network service objective, event detection is triggered when the measured Corvil Bandwidth is 66% of the link rate:

```
nso-map high-priority
  one-way-latency milliseconds 500
  protect-packets percent 99 busy-period hours 1
  measure-pnqm event-thresholds latency loss
  measure-icmp event-thresholds delay loss
  measure-eq event-thresholds delay loss
  queuing-targets delay-milliseconds 50
  measure-bandwidth event-threshold percent 66
  measure-microburst milliseconds 5 event-threshold percent 100
```

measure-eq

Mode

Port configuration
host (config-nso-map) #

Usage Guidelines

To enable Network Service Index calculations and estimation of the achieved loss or latency for a class or interface, use the **measure-eq** command when defining a network service objective. 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 network service objective, then the latency and loss values are taken from the configured one-way latency and packet protection targets. Check the network service objective configuration so that you know if queuing-targets are explicitly configured 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 network service objective means that the Expected Queuing graphs in the GUI will not be available.

If you want to disable Expected Queuing calculation using the **no measure-eq** command when configuring multi-class policy maps you must disable EQ in all classes and also at the interface level. The interface level usually has the default network service object applied but this is not shown when you use the **show config** command and in addition no EQ results are displayed at interface level. When you attempt to disable EQ you should use the **show policy-map**, or **show detailed-config** commands to check and ensure that both network service objectives used by the class and interface have EQ disabled.

measure-eq [event-thresholds [delay] [loss]]
no measure-eq

Syntax Description

delay	Specifies that event detection is triggered if the latency 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 measure-eq command is used to enable Network Service Index calculations and expected queuing latency and loss. If the delay value configured in the queuing targets for the network service objective is exceeded, or if loss due to queue buffer overflow is detected, then BQM will trigger alerts in each case:

```
host (config-nso) # measure-eq event-thresholds delay loss
```

measure-icmp

Mode

Network service objective Configuration

host(config-nso-map)#

Usage Guidelines

To enable ICMP ping measurements for monitoring end-to-end connections between sites, use the **measure-icmp** 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 end-to-end ICMP measurements.

measure-icmp [interval-milliseconds *msecs*] [size *bytes*]
 [roundtrip-target-milliseconds *msecs*]
 [event-thresholds [delay] [loss]]

no measure-icmp

Syntax Description

interval-milliseconds <i>msecs</i>	Specifies the number of milliseconds in the interval between ping packets. Range: 500-1000000 msecs. Default: 10000 msecs.
size <i>bytes</i>	Specifies the IP layer size of the ICMP ping packet. Range: 36-1500 bytes. Default: 36 bytes.
roundtrip-target-milliseconds <i>msecs</i>	Specifies the target roundtrip duration. Range: 1-10000 msecs Default: Twice the one-way latency
delay	Specifies that event detection is triggered if any packet is delayed by more than the configured roundtrip target. No default.
loss	Specifies that an 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-icmp
```

To enable end-to-end ping measurement with an event threshold to trigger event detection when delay exceeds 500ms, use the following:

```
measure-icmp roundtrip-target-milliseconds 500 event-thresholds delay
```

To enable end-to-end ping measurement with an event threshold to trigger event detection in case of packet loss, use the following:

```
measure-icmp event-thresholds loss
```

measure-microburst

Mode

Network service objective Configuration

host(config-nso-map)#

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

<i>raw</i>	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.
<i>msecs</i>	Specifies the peak-rate measurement value in milliseconds. Range: 1 – 10000. Default: 50
<i>kbps</i>	Specifies the event threshold bandwidth value in kilobits per second. Range: 1-20,000,000 kbps. No default.
<i>percent</i>	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 network service objective, event detection is triggered when the measured 5 millisecond microburst reaches the link rate:

```
nso-map high-priority
  one-way-latency milliseconds 500
  protect-packets percent 99 busy-period hours 1
  measure-pnqm event-thresholds latency loss
  measure-icmp event-thresholds delay loss
  queuing-targets delay-milliseconds 50
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-microburst milliseconds 5 event-threshold percent 100
```


measure-pnqm

Mode

Port configuration

```
host(config-nso-map)#
```

Usage Guidelines

To enable Passive Network Quality Monitoring (PNQM) measurement of end-to-end latency, latency variation and loss between sites, use the **measure-pnqm** command when defining a network service objective. The optional keywords enable detection of events using the configured one-way latency and one-way latency variation targets as the thresholds on latency and latency variation. An event is triggered if any packets are lost. Check the network service objective configuration so that you know what one-way latency or one-way latency variation target values are configured.

Use the no form of the command to disable end-to-end PNQM measurement. Disabling the PNQM parameter in the network service objective means that PNQM results will not be available in the CLI or GUI.

measure-pnqm [**packets-per-second** [*packets* | **all**]] [**event-thresholds** [**latency**] [**latency-variation**] [**loss**]]
no measure-pnqm

Syntax Description

packets-per-second [<i>packets</i> all]	Specifies the sampling rate for end-to-end PNQM measurement between sites. Choose either a certain number of packets or 100% sampling. Range: 1 – 1000 pps Default: 100 pps
latency	Specifies that event detection is triggered if the latency exceeds the configured one-way latency value. Default: Enabled
latency-variation	Specifies that event detection is triggered if the latency variation exceeds the configured one-way latency variation value. Default: Enabled
loss	Specifies that event detection is triggered if any packets are lost. Default: Enabled

Example

In this example, the **measure-pnqm** command is used to enable PNQM measurements as part of defining a network service objective. The sampling rate for PNQM measurement is set to all packets. If the one-way latency value configured in the network service objective is exceeded, or if loss is detected, then BQM will trigger alerts in each case:

```
host(config-nso-map)# measure-pnqm packets-per-second all event-thresholds latency loss
host(config-nso-map)#
```

media

Mode

Port Configuration

```
host(config-port)#
```

Usage Guidelines

By default on the two-port Cisco ADE 2120 and 2130 models, this release is configured to use electrical measurement ports. If you are setting up the two-port optical model of the device, you need to specify that you will be using the two optical ports for traffic measurement. To do this you use the **media** command from the port context of the CLI.

media {rj45 | sfp}

Syntax Description

rj45	Specify that electrical ports be used for measurement.
sfp	Specify that optical ports be used for measurement.

Example

In this example, the **port** command is used to enter port configuration mode for the PortA and PortB measurement interfaces and in each case the **media** command is used to set the measurement ports for an optical deployment:

```
host(config)$ port portA
host(config-port)$ media sfp
host(config-port)$ end
host(config-)$ port portB
host(config-port)$ media sfp
host(config-port)$ end
```

nso

Mode

Policy-map configuration

```
host(config-pmap)#
```

Policy-map Class configuration

```
host(config-pmap-c)#
```

Usage Guidelines

To create a network service objective in a policy-map or class entry for a previously configured network service objective map, use the **nso** command. To remove a network service objective from a policy-map or class entry for a network service objective map, use the **no** form of this command.

You configure measurement of the parameters specified by a network service objective by applying the latter with a **nso** command inside a policy-map, for example:

```
policy-map pmap
  nso mql
  class cls
    nso mql
```

It is important to note the positioning of **nso** 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 network service objective named mql 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
  nso mql
```

This results in mql being applied to class cls only. To achieve the desired effect, you insert an explicit exit command between the bandwidth and nso commands. For greater clarity, the **nso mql** command should be placed in the policy-map before any class configuration, as shown below:

```
policy-map pmap
  nso mql
  class cls
    bandwidth percent 10
```

Although a network service objective enables Corvil Bandwidth and Expected Queuing, 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 network service objectives 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 network service objective that cannot be deleted. It is named network-service-objective-default by analogy with class-default. If no nso command is used within a class, the default is applied. If no nso command is used within policy-maps, the default 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
  nso network-service-objective-default
  class cls
  nso network-service-objective-default
```

The parameters of network-service-objective-default can be changed with the **nso-map** command. For example, the default peak-rate timescale can be changed to 100ms with the following CLI fragment:

```
nso-map network-service-objective-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 network service objectives, and never for network-service-objective-default.

nso *name*

no nso *name*

Syntax Description

<i>name</i>	Specify the name of the previously configured network service objective (case-sensitive) to be referenced in the policy-map or class.
-------------	---

Example

In this example, having created a network service objective called mqm and a policy-map called pmap_1, a policy-map entry for class_map1 is created:

```
nso-map mqm
  one-way-latency milliseconds 500
  protect-packets percent 98 busy-period minutes 30
  measure-pnqm event-thresholds latency loss
  measure-icmp event-thresholds delay loss
  queuing-targets delay milliseconds 150
  measure-eq event-thresholds delay loss
  measure-bandwidth
  measure microburst milliseconds 150

policy-map p_map1
  nso mqm
```

nso-map

Mode

Network service objective Configuration

host(config-nso-map)#

Usage Guidelines

To create a network service objective context with the specified unique name, use the **nso-map** command. Applying this map in a policy-map enables quality measurement features for an interface. When you are in network service objective 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 **protect-packets** commands

Expected Queuing Latency and Loss (service-level estimation) – see **measure-eq** command

Network Service Index measurement – see **measure-eq** and **protect-packets** commands

Queuing targets – see **queuing-targets** command

Use the **no** version of this command to remove the specified network service objective.

nso-map <name>

no nso-map <name>

Syntax Description

<i>name</i>	Specifies a unique name for the network service objective.
-------------	--

Examples

To create a new network service objective, in this case named “low-speed”, use the following:

```
nso-map low-speed
```

To enter the context of an existing network service objective, in this case named “high-speed” to edit the configured parameters, use the following:

```
nso-map high-speed
```

The following is an example of a complete network service objective configuration:

```
nso-map high-priority
  one-way-latency milliseconds 500
  protect-packets percent 98 busy-period minutes 30
  measure-pnqm event-thresholds latency loss
  measure-icmp event-thresholds delay loss
  queuing-targets delay milliseconds 150
  measure-eq event-thresholds delay loss
  measure-bandwidth
  measure-microburst milliseconds 150
```

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

<i>file-url</i>	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_2007-08-16-041235.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**, **custom-application**, **custom-dashboard**, **domain**, **match**, **nso-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 command sets 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

<i>IP address</i>	Specify the IP v4 dotted decimal address of the server providing the clock synchronization .
<i>hostname</i>	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)#
```

one-way-latency

Mode

Network service objective Configuration
host(config-nso-map)#

Usage Guidelines

To configure the one-way latency target for end-to-end monitoring in an nso-map, use the **one-way-latency** command. Defining a one-way latency value is mandatory when defining a network service objective. You also have the option of defining a one-way latency variation target.

You use the **protect-packets** command to set the percentage of packets that must meet the configured latency target.

The one-way latency target specified here is used as the queuing delay target by the system for calculating Expected Queuing results unless you specify a different value using the **queuing-targets** command. The one-way latency target value is also used as the basis for the ICMP round-trip event threshold value. This threshold is set by default to twice the one-way latency.

one-way-latency milliseconds msec [variation milliseconds msec]

Syntax Description

one-way-latency milliseconds <i>msec</i>	Specifies the one-way latency measurement value in milliseconds. Range: 1 – 10000. Default: 500
variation milliseconds <i>msec</i>	[Optional] Specifies the latency variation measurement value in milliseconds. Range: 1 – 10000. Default: None

Examples

To set a one-way latency target of 300 milliseconds, use the following:

```
one-way-latency milliseconds 300
```

To set a one-way latency target of 450 milliseconds and a latency variation target of 50 milliseconds, use the following:

```
one-way-latency milliseconds 300 variation milliseconds 50
```

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

<i>username</i>	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 Cisco ADE 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

<i>interface name</i>	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 data center
  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. The **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] {hostname | ip-address} [data hex-data-pattern | df-bit
    | [repeat repeat-count] | [size datagram-size]
    | [source source-address] [timeout seconds]]
```

Syntax Description

<i>hostname ip address</i>	Specifies the target DNS hostname or IP v4 address. Only IP Addresses are supported. This release does not support the use of names with commands.
<i>hex-data-pattern</i>	Specifies the data pattern. <0 – FFFF>, no default
<i>df-bit</i>	Enables the "do-not-fragment" bit in the IP header. Default off
<i>count</i>	Specifies the number of ping packets that will be sent to the destination address. <1-2147483647>, default 5
<i>datagram-size</i>	Specifies the size of the datagram. <36-1500>, default 56
<i>source-address</i>	Specifies the source ip address. Only IP Addresses are supported. This release does not support the use of names with commands.
<i>seconds</i>	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)#
```

In this example, the connection to the router with DNS name siteA-rtr1 is verified:

```
host(config)# ping siteA-rtr1
PING 20.20.20.20 (172.18.3.99) 56(84) bytes of data.
64 bytes from 20.20.20.20: icmp_seq=1 ttl=64 time=2.30 ms
64 bytes from 20.20.20.20: icmp_seq=2 ttl=64 time=0.209 ms
64 bytes from 20.20.20.20: icmp_seq=3 ttl=64 time=0.836 ms
64 bytes from 20.20.20.20: icmp_seq=4 ttl=64 time=0.465 ms

--- 20.20.20.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.209/0.954/2.308/0.813 ms
host(config)#
```


ping-address

Mode

Site router interface configuration
host(config-site-router-if)#

Usage Guidelines

BQM generates end-to-end traffic performance statistics per-interface based on ICMP round trip times to a specified host address. To specify an always-available ICMP responder host address, 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.

You can test the availability of the chosen host using the **ping-address-test** command.

ping-address *hostname / ip address*

Syntax Description

<i>hostname / ip address</i>	Specifies the target always-available hostname or IP v4 address on a site subnet.
------------------------------	---

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 stabl

  interface Serial0/1
    description "Link to data center"
    bandwidth 512
    service policy output low-speed
    connects-to Datacenter core1 Serial0/1
```

ping-address-test

Mode

Site router interface configuration

```
host(config-site-router-if)#
```

Usage Guidelines

BQM generates end-to-end traffic performance statistics based on ICMP round trip times to a specified host address on a site subnet. To test the availability of the configured ICMP responder host address, use the **ping-address-test** command.

The test may take a few seconds to complete before results are displayed.

ping-address-test

Syntax Description

This command has no keywords or parameters.

Example

In this example, the test is successful:

```
host(config-site-router-if)$ ping-address-test
Test will take several seconds. Please wait...
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.028 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=0.033 ms

--- 192.168.10.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.028/0.033/0.047/0.008 ms
```

In this example, the test does not run because no ICMP responder address has been configured for the interface:

```
host(config-site-router-if) # ping-address-test
No ICMP-ping address has been specified for this interface...
host(config-site-router-if) #
```

pnqm-server

Mode

Site configuration

```
host(config-site-router-if)#
```

Usage Guidelines

BQM generates end-to-end traffic performance statistics based on Passive Network Quality Monitoring measurements between two BQM appliances. To define a PNQM measurement channel between the interface and a remote site interface, use the **pnqm-server** command. The **pnqm-server** command can only be invoked on a remote-site interface, but it then also applies to a peer-interface, or a 'connects-to' local-site interface, if either exist for the remote-site interface in question

When PNQM is activated for an interface, it is activated for all classes in the interface whose network service objective has 'measure pnqm' enabled. PNQM results are reported per class. You can deactivate PNQM for individual classes.

The autoconf and report-class-mismatch parameters are mutually exclusive. You can only specify traffic misclassification detection when you are performing a manual configuration of the remote Cisco ADE for PNQM measurement.

The sampling-override parameter cannot be specified without first specifying autoconf or report-class-mismatch.

For a multiclass interface, the autoconf and report-class-mismatch parameters require the specification of a sampling-override. For a FIFO interface with autoconf or report-class-mismatch configured and without a sampling-override, it will not be possible to change the applied policy-map to a multiclass without first enabling a sampling-override.

The strict-loss parameter cannot be specified with autoconf. Again, it is only possible to disable re-routing detection when performing a manual configuration of the remote Cisco ADE for PNQM measurement.

The system disallows automatic configuration with the autoconf parameter when no subnets have been configured for the site. The system also issues a warning message when the site configuration uses filter classes or attached ports, as these will be ignored if an automatic configuration is attempted.

Use **no pnqm-server** to delete the PNQM measurement channel.

pnqm-server <remote-BQM-address> [**port** <remote-BQM-port>] [**app-port** <remote-BQM-app-port>]
[autoconf] [report-class-mismatch] [sampling-override <one-in N>] [strict-loss]
no pnqm-server

Syntax Description

<i>remote-BQM-address</i>	Specifies the IP address of the target Cisco ADE. Only IP addresses are supported. This release does not support the use of host names with commands.
<i>port remote-BQM-port</i>	Specifies the remote Cisco ADE port number. Default port number used is 5100.
<i>app-port remote-BQM-app-port</i>	Specifies the remote Cisco ADE applications port number used for retrieval of remote EQ data.
<i>autoconf</i>	Enables automatic configuration of the remote BQM to support the PNQM channel.

report-class-mismatch	Enables traffic misclassification and re-routing detection for debugging purposes.
sampling-override <i>N</i>	Overrides the configured per-class sampling rate with the specified integer value. You enter an integer value, <i>N</i> , and that represents a one-in- <i>N</i> sampling rate. For example, entering sample-override 4 means you are configuring a sampling rate of one-in-four packets.
strict-loss	Disables re-routing detection.

Example

In this example, automatic configuration of PNQM measurement is specified:

```
host(config-site-router-if) # pnqm-server 192.168.5.2 autoconf
```

In this example, as part of the initial configuration of a multi-class network, the sampling rate is initially set to all packets on the interface ('one-in-one'). This overrides the per class sampling rate configured in the network service objective applied to each class. Setting the sampling rate enables misclassification detection to help troubleshoot any potential issues with the configuration:

```
host(config-site-router-if) # pnqm-server 10.2.12.4 report-class-mismatch sampling-override 1
```

In this example, the network deployment precludes re-routing of packets along different paths between the PNQM channel endpoints, so re-routing detection is disabled:

```
host(config-site-router-if) # pnqm-server 10.2.12.4 strict-loss
```

pnqm-server-test

Mode

Site configuration

```
host(config-site-router-if)#
```

Usage Guidelines

BQM generates end-to-end traffic performance statistics based on Passive Network Quality Monitoring measurements between two BQM appliances. To test the availability of the BQM host address, use the **pnqm-server-test** command.

When specifying the remote BQM IP address for PNQM, you can test the configuration. Using the **pnqm-server-test** command tests the following:

- Local BQM configuration is complete (that is, interface configured and reverse direction configured)
- Remote BQM PNQM service available
- Remote BQM version compatible
- Remote BQM configuration is compatible
- Channels can be established and report signature generation at both ends per class for 45 seconds.
- The test may take a few seconds to complete before results are displayed.

pnqm-server-test

Syntax Description

This command has no keywords or parameters.

Example

In this example, the test is successful:

```
host(config-site-router-if)# pnqm-server-test
Test may take several seconds. Please wait...
Successfully opened socket to remote BQM.
Successfully received response from remote BQM.
Successfully checked version.
Starting tests for each class...
Tested 3 streams. 3 saw traffic (success), 0 with no traffic (notice), 0 could not be
established (error).
Test completed...
```

In this example, the test does not run because no PNQM responder address has been configured for the interface:

```
host(config-site-router-if) # pnqm-server-test
No PNQM server address has been specified for this interface...
host(config-site-router-if) #
```

In this example, the test fails because no communication is possible with the remote Cisco ADE on the default port:

```
host(config-site-router-if)# pnqm-server-test
Test may take several seconds. Please wait...
ERROR: Cannot connect to remote BQM on port 5100.
```

pnqm-settings

Mode

Global

host(config)#

Usage Guidelines

For Passive Network Quality Monitoring (PNQM) to operate correctly between two Cisco ADEs, BQM communication port settings on each Cisco ADE must be correct. The first port is for the PNQM protocol (default port: 5100) and the second is for the application layer to retrieve data from a remote BQM appliance (default port: 5101). To set the PNQM port parameters to different values, use the **pnqm-settings** command.

Since more real-world traffic also produces more PNQM traffic when ALL is selected as the sampling rate, a throttling mechanism is present that prevents the system from overloading its own or the network's capacities. An upper limit on PNQM-related traffic for each interface is enforced. You can configure this global parameter and it is then applied on a per-interface basis.

pnqm-settings port <port> [**app-port** <app-port>] [**max-overhead percent** <percent>]

Syntax Description

port <i>por</i> >	Sets the port number on which the PNQM server listens. Default: 5100
app-port <i>app-port</i>	Sets the port number on which the PNQM application server listens. Defaults to <port> plus one if unspecified.
max-overhead <i>percent</i>	Specifies the maximum percentage of available per-interface bandwidth that PNQM is allowed to consume. Default: 5%

Example

In this example, the PNQM port settings and the upper limit on PNQM signature traffic for each interface are changed:

```
host(config-site-router-if) # pnqm-settings port 5105 app-port 5108 max-overhead percent 10
```

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 network service objective. 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 than the link has available.

policy-map <policy-map name>

no policy-map <policy-map name>

Syntax Description

<i>policy-map name</i>	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

<i>port_name</i>	Specify the Cisco ADE 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 latency 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 latency and jitter.

The configured LFI value represents the maximum tolerable latency to be incurred by fragmented packets. The packet fragment size for fragmenting classes is based on the required latency. Cisco recommends fragmenting data packets to sizes that incur no more than a 10-millisecond latency. 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 latency 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 delay** 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 <i>delay max</i>	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 units 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

<i>bandwidth-kbps</i>	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 – 20,000,000 kbps
percent <i>percentage</i>	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%
<i>burst</i>	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 2,000,000 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=accllist6

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
```

protect-packets

Mode

Configuration
host(config-nso-map)

Usage Guidelines

To establish the percentage of packets that must meet the configured end-to-end and queuing targets, use the **protect-packets** command. You must define a packet protection target when defining a network service objective. You cannot remove a packet protection target from a network service objective but you can change it using the command with different values.

The *percent* parameter allows you to define the fraction of the packets during the defined *busy-period* that must meet the configured targets.

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 targets are met for the configured fraction of packets over any consecutive period of length *busy-period*. For example, say the protection target is set to 99% and the busy period is set to 30 minutes. Bandwidth-sizing calculation for a 24-hour period 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.

The packet protection target specified here is also used by default as the basis for the queuing loss target by the system for calculating Expected Queuing results. You can specify a different value using the **queuing-targets** command. For example, a configured packet protection target of 99% implies a loss target of 1%.

protect-packets percent *percent* busy-period {minutes *mins* | hours *hours* | day | week}

Syntax Description

<i>percent</i>	Specifies the percentage of packets allowed to exceed the configured queuing targets during the specified busy-period. Range: 0.0-99.99999%. Default: 99.9%.
<i>mins</i>	Specifies the number of minutes in the busy period. Range: 5–1440 minutes. Values allowed: 5, 60, 120, 240 minutes. Default: 240 minutes.
<i>hours</i>	Specifies the number of hours in the busy period. Values allowed: 1, 2, 4 hours. Default: 4 hours.

day	Specifies a busy period of one day.
week	Specifies a busy period of one week.

Example

In this example network service objective, 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):

```
nso-map high-priority
  one-way-latency milliseconds 500
  protect-packets percent 99 busy-period hours 1
  measure-pnqm event-thresholds latency loss
  measure-icmp event-thresholds delay loss
  queuing-targets delay-milliseconds 50
  measure-eq event-thresholds delay loss
  measure-bandwidth event-threshold percent 100
  measure-microburst milliseconds 50 event-threshold percent 100
```

queuing-targets

Mode

Network service objective Configuration

host(config-nso-map)#

Usage Guidelines

To configure the delay target for Corvil Bandwidth and Expected Queuing Loss and Latency calculation, use the **queuing-targets** command. If the **queuing-targets** command is absent from a network service objective, then Corvil Bandwidth and Expected Queuing Latency and Loss calculations will be based on the one-way latency and packet protection values configured in the network service objective.

The targets specified here serve as the QoS targets for calculating Corvil Bandwidth and also for Expected Queuing Latency 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.

You cannot remove a queuing-targets command from a network service objective. To reset the command to its default value, you use the following: **queuing-targets delay-milliseconds use-one-way protect-packets use-one-way**

queuing-targets delay-milliseconds [use-one-way|<msecs>] protect-packets [use-one-way | percent <percent>]

Syntax Description

delay-milliseconds [use-one-way msec]	Specifies the number of milliseconds delay. You can either specify that the configured one-way latency value is used, or you can specify a different millisecond value. Range: 5 -10000 kbps. Default: the configured one-way latency value
protect-packets [use-one-way percent percent]	Specifies the loss target as a percentage of packets. You can either specify that the configured packet protection target is used, or you can specify a different permitted packet loss percentage. For example, if you use the configured packet protection target, and that target is configured in the network service objective as 99%, then the loss target is 1%.

Examples

To configure a delay queuing-target of 150 milliseconds and a loss target of 1% (by protecting 995 of packets), use the following:

```
host(config-nso)$ queuing-targets delay-milliseconds 150 protect-packets percent 99
```

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-level** command must first be used.

The **Event 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

<i>number-of-packets</i>	Specify the maximum number of packets that the queue for this class can accumulate. Range: 16 – 100000 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 BQM as an admin user to use this command.

Usage Guidelines

To reboot the Cisco ADE 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, custom dashboard interface, local-site, nso-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** | **custom-dashboard** | **nso-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

<i>site-name</i>	Specifies site for router or interface renaming.
<i>router-name</i>	Specifies site and router name for interface renaming.
<i>old-name</i>	Specifies the old name for class-map, custom application, custom dashboard, interface, nso-map, policy-map, router or site. Note, not required for local-site as only a single local-site is allowed.
<i>new-name</i>	Specifies the name for the class, class-map, custom application, custom dashboard, interface, local-site, nso-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 if not specified. 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 { status | [data] | [data-with-captures]} {backup:filename |
[ftp://[hostname | IP address]/filename] [user] [password]] |
[scp://[hostname | ip address]/filename] [user] [password]]}
```

Syntax Description

<i>status</i>	Displays the status of the most recent restore operation.
<i>backup:path</i>	Selects restore from an accessible file system.
<i>ftp://hostname/path</i>	Selects restore from an FTP server.
<i>scp://hostname/path</i>	Selects restore from a remote machine via ssh or scp.
<i>user</i>	Specifies the login username (ftp and scp.)
<i>password</i>	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

<i>name</i>	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 Data center 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 Data center 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 system configuration. You can use the **show** command to check the current service status.

service *service-name*

no service *service-name*

Syntax Description

<i>service name</i>	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. 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

<i>policy-map name</i>	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 Cisco ADE, involving the setup of the 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 Cisco ADE. 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.
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	Optionally specify an IP address for DNS name resolution. If an IP address is not specified, it can be specified later using the domain command.
Hostname	Accept the default hostname (BQM) by pressing Enter or edit it to specify a hostname.

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, custom-dashboard, local-sites, interfaces, nso-maps, ntp, peer-interfaces, policy-maps, , and sites. The **show config** command displays captures, class-maps, custom-applications, custom-dashboard, interfaces, local-sites, nso-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, or advanced PNQM details.

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.

If you have a USB-connected GPS clock, you can check status using the **show gps** command.

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 | custom-dashboard | local-sites | nso-map |
policy-map | sites | snmp-server [<*name*>[*]]

show config [class-map | custom-application | custom-dashboard | local-sites | interfaces |
nso-map | peer-interfaces | policy-map |
sites | snmp-server [<*name*>[*]]

show detailed-config

show faults-info

show file-systems

show gps

```
show interface <site> <router> <name> [ {stats { [class <class>]
[top <n>] [applications | conversations | listeners | talkers]
[ascending | descending] } } | { pnqm {[class <class>]} } } ]
```

```
show interfaces [<name>[*]] [ {stats { [class <class>]
[top <n>] [applications | conversations | listeners | talkers]
[ascending | descending] } } | { pnqm {[class <class>]} } } ]
```

```
show peer-interface <site> <router> <name> [ {stats { [class <class>]
[top <n>] [applications | conversations | listeners | talkers]
[ascending | descending] } } | { pnqm {[class <class>]} } } ]
```

```
show peer-interfaces [<name>[*]] [ {stats { [class <class>]
[top <n>] [applications | conversations | listeners | talkers]
[ascending | descending] } } | { pnqm {[class <class>]} } } ]
```

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 BQM alerts.
audit	Displays a list of recent BQM changes.

capture [<i><name></i> [*]]	<p>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.</p> <p>The following information is displayed:</p> <ul style="list-style-type: none"> • Capture configuration details • current capture status • total size of capture file and size limit • time limit • number of captured/dropped frames <p>The following describes the displayed packet capture status values:</p> <p>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.</p>												
class-map [<i><name></i> [*]]	Displays the list of configured class-maps and their associated match rules.												
local-site [<i><name></i> [*]]	Displays the configured local-site details.												
custom-application [<i><name></i> [*]]	Displays the list of configured custom applications.												
custom-dashboard [<i><name></i> [*]]	Displays the classes and graphs defined in the named custom dashboard for use in the GUI.												
detailed-config	Displays the detailed current operating configuration.												
faults-info	Displays an overview of the enable/disable state of the various faults.												
file systems	<p>Displays the used/free space information on the available file system. The information displayed includes the following:</p> <ul style="list-style-type: none"> • name of file system • total size of file system in KB • free space of file system in KB 												
gps	Displays the status of a connected GPS system.												
interface <i><site></i> <i><router></i> <i><name></i> [[pnqm [class <i><class></i>]]] [[stats [class <i><class></i>] [top <i><n></i>] [applications conversations listeners talkers] [ascending descending]]] 	<p>Displays details for a specific named interface, its attached service-policies and classes, where the available parameters are as follows:</p> <table> <tr> <td><i>site</i></td> <td>specifies the name of the site containing the interface.</td> </tr> <tr> <td><i>router</i></td> <td>specifies the name of the router containing the interface.</td> </tr> <tr> <td><i>name</i></td> <td>specifies the name of a chosen interface.</td> </tr> <tr> <td><i>pnqm class</i></td> <td>specifies the name of a PNQM class.</td> </tr> <tr> <td><i>class</i></td> <td>specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.]</td> </tr> <tr> <td><i>n</i></td> <td>number of applications, conversations, listeners or talkers to display. Note that fewer items than those</td> </tr> </table>	<i>site</i>	specifies the name of the site containing the interface.	<i>router</i>	specifies the name of the router containing the interface.	<i>name</i>	specifies the name of a chosen interface.	<i>pnqm class</i>	specifies the name of a PNQM class.	<i>class</i>	specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.]	<i>n</i>	number of applications, conversations, listeners or talkers to display. Note that fewer items than those
<i>site</i>	specifies the name of the site containing the interface.												
<i>router</i>	specifies the name of the router containing the interface.												
<i>name</i>	specifies the name of a chosen interface.												
<i>pnqm class</i>	specifies the name of a PNQM class.												
<i>class</i>	specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.]												
<i>n</i>	number of applications, conversations, listeners or talkers to display. Note that fewer items than those												

	<p>requested may be displayed if there are insufficient numbers, [Default: 10]</p> <p>ascending sort display with largest quantity at the top. [Default: ascending].</p> <p>descending sort display with smallest quantity at the top. [Default: ascending].</p>
interfaces [<name>[*]] {[pnqm [class <class >]]} {[stats [class<class> top <n> [applications conversations listeners talkers] [ascending descending]]}]	<p>Displays the list of configured interfaces, their attached service-policies and classes, where the available parameters are as follows:</p> <p><i>name</i> specifies the name of a chosen interface.</p> <p><i>pnqm class</i> specifies the name of a PNQM class.</p> <p><i>class</i> specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.]</p> <p><i>n</i> 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]</p> <p>ascending sort display with largest quantity at the top. [Default: ascending].</p> <p>descending sort display with smallest quantity at the top. [Default: ascending].</p>
nso-map [<name>[*]]	Displays the list of nso-maps or specific nso-map(s) with wildcarding. The nso-map(s), if they exist, are displayed.
peer-interface <site> <router> <name> {[pnqm [class <class >]]} {[stats { [class <class>] [top <n>] [applications conversations listeners talkers] [ascending descending]]}]	<p>Displays details for a specific named peer-interface, its attached service-policies and classes, where the available parameters are as follows:</p> <p><i>site</i> specifies the name of the site containing the peer-interface.</p> <p><i>router</i> specifies the name of the router containing the peer-interface.</p> <p><i>name</i> specifies the name of a chosen interface.</p> <p><i>pnqm class</i> specifies the name of a PNQM class.</p> <p><i>class</i> specifies an optional class associated with the chosen interface [Default: All classes associated with the interface.]</p> <p><i>n</i> 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]</p> <p>ascending sort display with largest quantity at the top. [Default: ascending].</p> <p>descending sort display with smallest quantity at the top. [Default: ascending].</p>
peer-interfaces [<name>[*]] {[pnqm [class <class >]]}	Displays the list of configured peer-interfaces, their attached service-policies and classes, where the available parameters are as follows:

{[stats [class<class> top <n> [applications conversations listeners talkers] [ascending descending]]}	<p><i>name</i> specifies the name of a chosen peer-interface.</p> <p><i>pnqm class</i> specifies the name of a PNQM class.</p> <p><i>class</i> specifies an optional class associated with the chosen peer-interface [Default: All classes associated with the peer-interface.]</p> <p><i>n</i> 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]</p> <p>ascending sort display with largest quantity at the top. [Default: ascending].</p> <p>descending sort display with smallest quantity at the top. [Default: ascending].</p>
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 Cisco ADE.
routers	Displays the configured router details.
config [class-map local-site custom-application custom-dashboard interfaces nso-map peer-interfaces policy-map sites snmp-server] [<name>[*]]	Displays the current operating configuration or specific class-maps, custom applications, custom dashboards, interfaces, nso-maps, peer-interfaces, policy-maps, and sites (including associated routers and interfaces) with wildcards.
sites [<name>[*]]	Displays the list of sites configured in the BQM network model.
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 BQM as an admin user to use this command.
users	Listing of the current 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
    nso low_speed
    class class-default
policy-map mpls_policy
    class realtime
        nso low_speed
        bandwidth 25
    class critical
        nso low_speed
        bandwidth 20
    class video
        nso low_speed
        bandwidth 20
    class bulk
        nso low_speed
        bandwidth 10
    class besteffort
        nso 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 "remotel"
-- 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 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)#
```

In the following example, the **show gps** command is used to display the status of the GPS system connected to the BQM USB port:

```
host(config)$ show gps
```

```
GPS subsystem status: active
```

```
Receiver details:
```

```
    Hardware: Acutime Gold GPS Timing Receiver, rev: 3001
Product date: 8/4/2007, serial no: 84977307
    Firmware: AcuGold v1.10.0
```

```
Status, position & time:
```

```
Device mode: Overdetermined clock (default)
    Status: Overdetermined fixes (best accuracy)
    Latitude:  53.20'32'' N
    Longitude:  6.14'25'' W
    UTC Time: Fri Jul  6 08:46:51 2007
```

```
Satellite tracking data:
```

```
    Satellite: 27, signal level:  8.4
    Satellite: 20, signal level: -1.0
    Satellite: 25, signal level: 14.6
    Satellite:  4, signal level:  2.0
    Satellite: 23, signal level: 15.8
    Satellite: 13, signal level: 13.2
    Satellite: 10, signal level: -0.8
    Satellite:  2, signal level: -1.0
host(config)$
```


In the following example, the **show interfaces** command is used to display advanced details of PNQM operation for all interfaces including the string 've0' in their names:

```

host(config)# show interfaces ve0 pnqm
site DC
  router headgwhost
    interface ve0
      bandwidth 1000
      max-reserved-bandwidth 75
      subnet-filtering
      service-policy output testmap
      Traffic Stats - 362 Kbps mean, 1.2 Mbps 1s peak, 63.2 Mbps 5ms peak
                    - 7.7 Mbps 50ms peak (configured)
                    - 17,895,924 packets, 21,916,966,655 bytes
      PNQM Stats   - 3707792 packets sampled, 670 lost (0.02%), 667 in
                    missing flows      interface ve0

  class class-default
    Traffic Stats - 227 Kbps mean, 1.2 Mbps 1s peak, 52.8 Mbps 5ms peak
                  - 818 Kbps Corvil Bandwidth
                  - 5.9 Mbps 50ms peak (configured)
                  - 1.5 Mbps 500ms peak (delay-target)
                  - 11,925,321 packets, 14,604,890,509 bytes
    PNQM Stats   - 1982248 packets sampled, 358 lost (0.02%), 379 in
                  missing flows
                  - PNQM availability: 98%, GPS availability: 0%
                  - 18.939 ms min, 64.231 ms mean, 628.763 ms max
                    (67.765 ms max error)
                  - Channel status: OK
                  - 1990739 signature lookups (8052 failures),
                    current sample rate: 1-in-6
                  - src: 127.0.0.1:5100,
                    rt-class/DC/headgwhost/ve0/output/class-default
                    OK, received 1668275 signatures in
                    448813.507383 seconds (3.72 sigs/sec)
                  - 0.000% hash collisions, 240 signatures in
                    history
                  - dest: 172.18.2.75:5100,
                    rt-class/DC/headgwhost/ve0/output/class-default
                    OK, received 1667414 signatures in
                    448525.757181 seconds (3.72 sigs/sec)
                  - 0.000% hash collisions, 231 signatures in
                    history
                  - internal clock stats: o=20.551s o_err=0.000s
                    skew=-5.30161e-05 maxdrift=4.45487e-07
                  - Reverse Channel:
                    rt-class/branch2/b2-r/ve0/output/class-default

```

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 Cisco ADE 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 Cisco ADE 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

<i>name</i>	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 Data center 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 Data center 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 use 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

<i>size</i>	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
```

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 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

<i><hostname ip-address></i>	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.
<i>port<port></i>	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

server <i><hostname ip-address></i>	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
destination <i><hostname ip-address></i>	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 <i><port></i>	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

<i><hostname ip address></i>	Specifies the DNS hostname or IP address of the host to which SNMP notifications are sent. The <i>ip-address</i> 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 <i>port</i>	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 fault <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][frequency]

Syntax Description

<i>name</i>	Specifies the name of the fault.
	<div>Corvil Bandwidth Threshold Exceeded The Corvil Bandwidth measurement indicates the class bandwidth threshold has been exceeded.</div> <div>CPU Failure CPU Failure detected.</div> <div>CPU Utilization High High CPU Utilization detected.</div> <div>Database Fault Database fault detected.</div> <div>E2E Availability Issue Connectivity to the site is currently unavailable.</div> <div>E2E Delay Threshold Exceeded The ICMP round trip delay value has crossed the configured threshold.</div> <div>E2E Loss Detected The ICMP loss value has crossed the configured threshold.</div> <div>Expected Policing Threshold Exceeded The EQ policer value has crossed the configured threshold.</div> <div>Expected Queuing Delay Threshold Exceeded The EQ delay value has crossed the configured threshold.</div> <div>Expected Queuing Loss Threshold Exceeded The EQ loss value has crossed the</div>

	<p>configured threshold.</p> <p>Fan Failure Fan failure detected.</p> <p>GPS Failure GPS failure detected.</p> <p>Hard Disk Threshold Exceeded Hard disk threshold exceeded detected.</p> <p>Hard Drive Failure Hard drive failure detected.</p> <p>ICMP Failure Detected ICMP failure, possibly due to network, version, license or configuration problems - see logs for details.</p> <p>License Expired License is expired.</p> <p>License Invalid License invalid detected.</p> <p>License Near Expiration License will expire soon.</p> <p>Memory Usage High High Memory usage detected.</p> <p>Micro-Burst Detected Micro-Bursts exceeding the configured bandwidth threshold have been detected.</p> <p>Network Service Threshold Exceeded The Network Service Indicator crossed the configured threshold.</p> <p>PNQM Failure Detected PNQM failure, possibly due to network, version, license or configuration problems - see logs for details.</p> <p>PNQM Latency Threshold Cleared The PNQM latency value is back within the configured threshold.</p> <p>PNQM Latency Threshold Exceeded The PNQM latency threshold has been exceeded.</p> <p>PNQM Latency Variation Threshold Cleared The PNQM latency variation value is back within the configured threshold.</p> <p>PNQM Latency Variation Threshold Exceeded The PNQM latency variation threshold has been exceeded.</p> <p>PNQM Loss Threshold Cleared The PNQM loss threshold is back within the configured threshold.</p> <p>PNQM Loss Threshold Exceeded The PNQM loss threshold has been exceeded.</p> <p>Port Down Port down detected.</p> <p>Power Supply Failure Power supply failure detected.</p> <p>Soft Disk Threshold Exceeded Soft disk threshold exceeded detected.</p> <p>System Shutdown The system has shutdown.</p> <p>System Startup The system has started up.</p> <p>System Throughput High High network card buffer utilization detected.</p> <p>Temperature High High Temperature detected.</p> <p>Watchdog Restart System Watchdog has restarted.</p> <p>NOTE: Names containing spaces must be delimited by quotes, for example: "Watchdog Restart"</p>
traps-severity	<p>Specifies the trap severity value for the fault, one of the following values:</p> <p>Informational – events that need communicating but do not cause failures</p> <p>Warning – typically used for thresholds that warn of an impending failure</p> <p>Minor – not used for defaults</p> <p>Major – an event that has the potential to make the system no longer operational</p> <p>Severe – the system is no longer operational</p>
syslog-severity	<p>Specifies the syslog severity value for the fault, one of the following values:</p> <p>emergency</p> <p>alert</p> <p>critical</p> <p>error</p> <p>warning</p>

	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 <i>frequency</i>	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 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

<i>Name</i>	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

<i>Name</i>	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 BQM status, 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 BQM status, use the following:

```
host(config)# status
Cisco Bandwidth Quality Manager software: Version 4.0 (trunk.29025 Tue 21 Aug 2007)
CorvilMeter software: CDK_3_0_BUILD_47 (conf Aug 21 04:51:38 2007)
Application Recognition Module: ARM v4.1.2 (full)
Logging: <off>
Access control: unrestricted
  uptime is 5 days, 23 hours, 6 minutes, 3 seconds

License system id: 03e5edbb4514add29b
License features: Sites: 1000, Bandwidth: 1000 Mbps, Packet Capture: enabled
License expires at: Fri Sep  7 00:00:00 2007
License time remaining: 10 days, 11 hours, 34 minutes, 17 seconds

cpu #0: "Intel(R) Xeon(TM) CPU 3.40GHz", 1024 KB cache, 4%
cpu #1: "Intel(R) Xeon(TM) CPU 3.40GHz", 1024 KB cache, 2%
cpu #2: "Intel(R) Xeon(TM) CPU 3.40GHz", 1024 KB cache, 5%
cpu #3: "Intel(R) Xeon(TM) CPU 3.40GHz", 1024 KB cache, 5%
5-minute average load (all CPUs): 2%

logical disk #0: total=422352152 KB, used=32421476 KB (8%)
  "IBM          SERVERAID"
logical disk #1: total=0 KB, used=0 KB (0%)
  "Not present"
  Alert: Logical disk 1 is not present

14 fan component(s), 0 alert(s)
2 power supply component(s), 0 alert(s)
6 temperature sensor component(s), 0 alert(s)
BIOS date: 10/11/04

Last Backup/Restore operation 'no status available for the last backup/restore
operation'
```

Memory: total=3115908 KB, cached=563824 KB, used=2462100 KB (79%)
5-minute average usage: 79%

NIC buffer usage: 2%

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
- nso-maps: 1
- 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

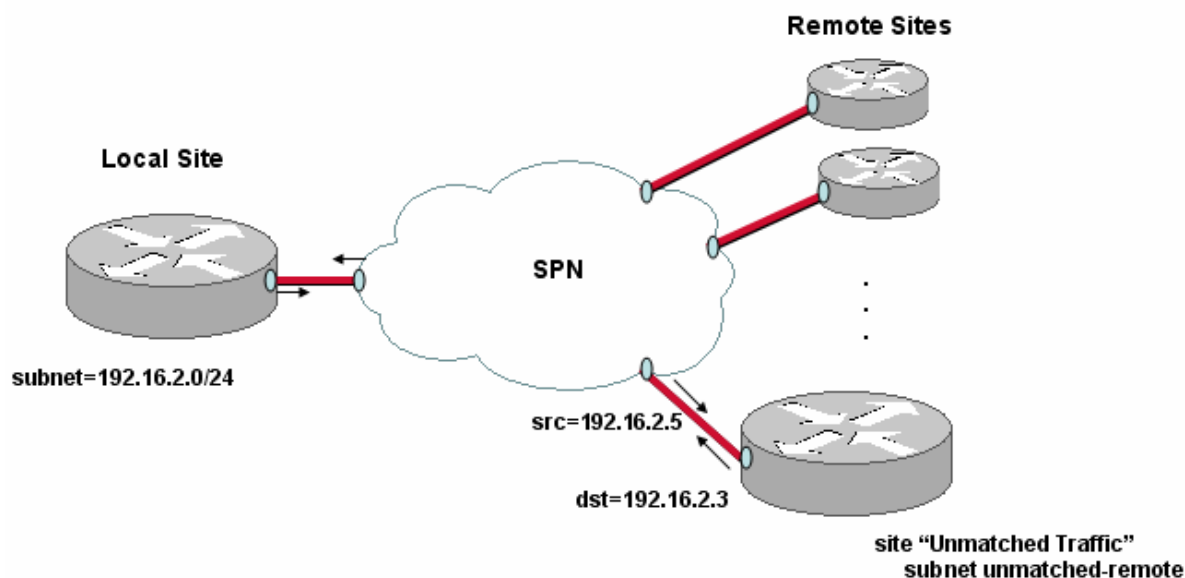
When you are developing the network model for a deployment, you define subnets for each site. To define a subnet for a site, you use the **subnet** command. To remove a site you use the no form of the command. In general, configured subnets are used to identify traffic that originates from or is destined 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

<i>ip address</i>	Specify an IP address for the configured site or local-site subnet. No default.
<i>prefix</i>	Specify the prefix value to identify the subnet. No default.
<i>netmask</i>	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 Data center 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 Data center 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 Cisco ADE ports (PortA, PortB, PortC, PortD, PortAC, PortBD)
- using the **filter-class** commands or if you define a particular set of match rules using a class-map

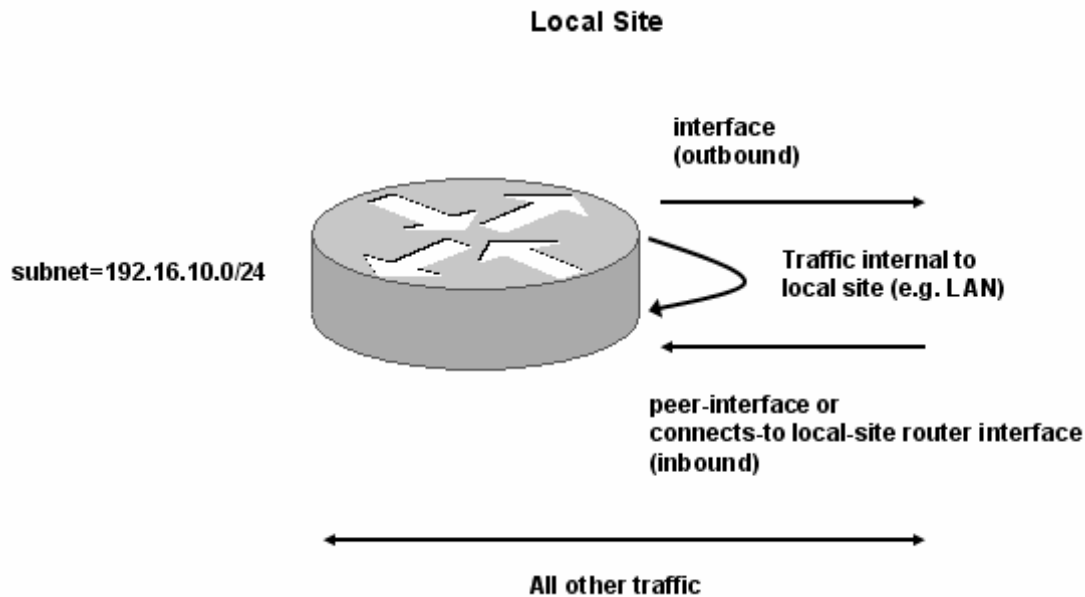
The use of the Cisco ADE physical ports (such as PortA, PortB and so on) in the default first day of service configuration requires subnet filtering to be explicitly disabled. So the default BQM configuration includes a **no subnet-filtering** command on each relevant interface. Note that the default BQM configuration has no subnets defined for any sites. For example, from the default configuration:

```

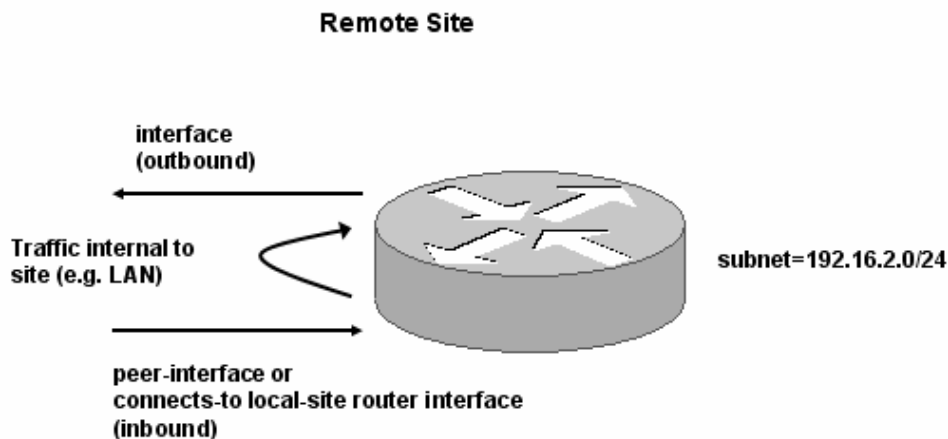
interface PortA
  attached-port PortA
  bandwidth 1000000
  max-reserved-bandwidth 75
  no subnet-filtering
  service-policy output default
  class class-default

```

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 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.

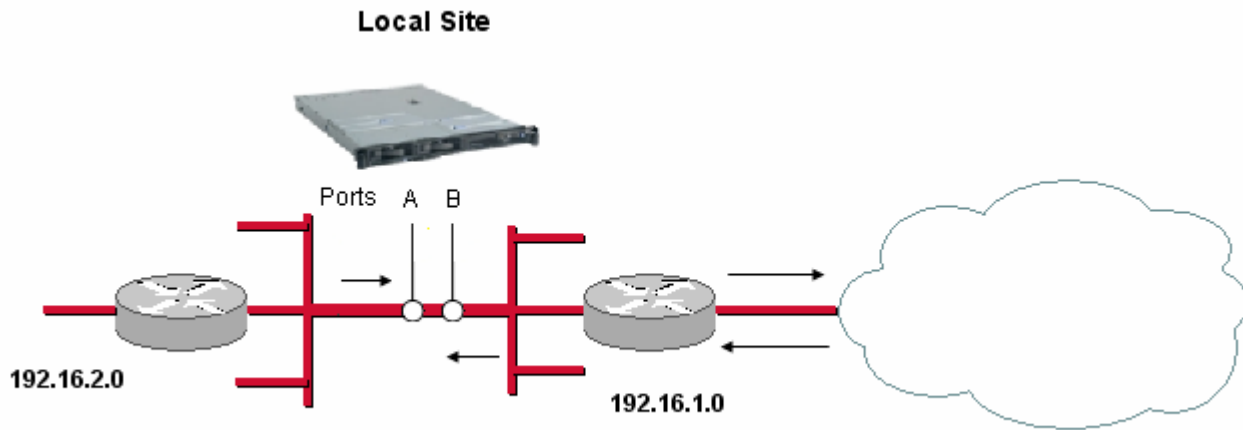
subnet-filtering {exclude-local | non-local-only}
no subnet-filtering

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, 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 Cisco ADE 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

<i>parameter</i>	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] {hostname | ip-address} [[numeric]] [port <number>]
                | [probe <number hops>] | [source <source-address>]
                | [ttl <min. ttl> <max. ttl>] | [timeout <seconds>]]
```

Syntax Description

<i>ip hostname</i> <i>ip address</i>	Specifies the target DNS hostname or IP v4 address.
<i>numeric</i>	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
<i>port number</i>	Specifies a UDP port number. <1-65535>, default 33434
<i>probe number hops</i>	Specifies the number of hops <1-65535>, default 3
<i>source source-address</i>	Specifies the source address.
<i>ttl min. ttl</i>	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>,
<i>ttl max. ttl</i>	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
<i>timeout seconds</i>	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)#
```

up

Mode

Policy-map configuration
(`config-pmap`)

Usage Guidelines

To move a class up in the list of defined classes in a policy-map, use the **up** command in policy-map configuration mode. By default the specified class is moved up one place. This can be changed by specifying the number of places, for example to move a class up three places. See the **down** command for information on moving classes down in a policy-map list.

Order of classes is important in 'match-first' policy-maps whereby only the first matching class matches traffic and subsequent classes further down the list are not matched.

up [*<number places>*] *<class name>*

Syntax Description

<i>number places</i>	Specifies the number of places up the list by which the specified graph is moved. By default the specified graph is moved up one place.
<i>class name</i>	Specifies the name of the class to be moved.

Example

In this example, the video class moved up the list of classes by one place:

```
host(config-pmap)# up video
```

In this example, the voice class moved up the list of classes by two places:

```
host(config-pmap)# up 2 voice
```

Mode

Custom dashboard graph order configuration
`host(config-custom-dashboard-go)`

Usage Guidelines

To move a specified graph up in the display order list for a defined custom dashboard tab in the GUI, use the **up** command in custom dashboard configuration mode. See the **down** command for information on moving graphs down the display order list.

When you re-order the list of displayed graphs, the changes are displayed in the GUI tab following the next data summarization update for the chosen GUI reporting period. For example, if the 24-hour reporting period is selected in the GUI, the changes will be updated in the GUI tab after five minutes.

up [*<number places>*] *<graph name>*

Syntax Description

<i>number places</i>	Specifies the number of places up the list by which the specified graph is moved. By default the specified graph is moved down one place.
<i>graph name</i>	<p>Specifies the name of the graph to be moved.</p> <p>The list of available graphs is as follows (in the default order):</p> <ul style="list-style-type: none"> Microburst-detection "Average Rate" "Packet Rate" Peak-to-mean "Packet Size distribution (by bytes)" "Packet Size distribution (by packets)" "Top 10 Applications" "Top 10 Talkers" "Top 10 Listeners" "Top 10 Conversations" "Corvil Bandwidth - Delay" "Corvil Bandwidth - Queue Length" "5 minute Network Service Index" "End-to-end Delay" "End-to-end Delay variation" "End-to-end Loss" "EQ Delay" "EQ Delay variation" "EQ Loss" "Interface ICMP Round-trip Delay" <p>Graph names with spaces between words must be enclosed in quotes (" ") when being specified in a command.</p>

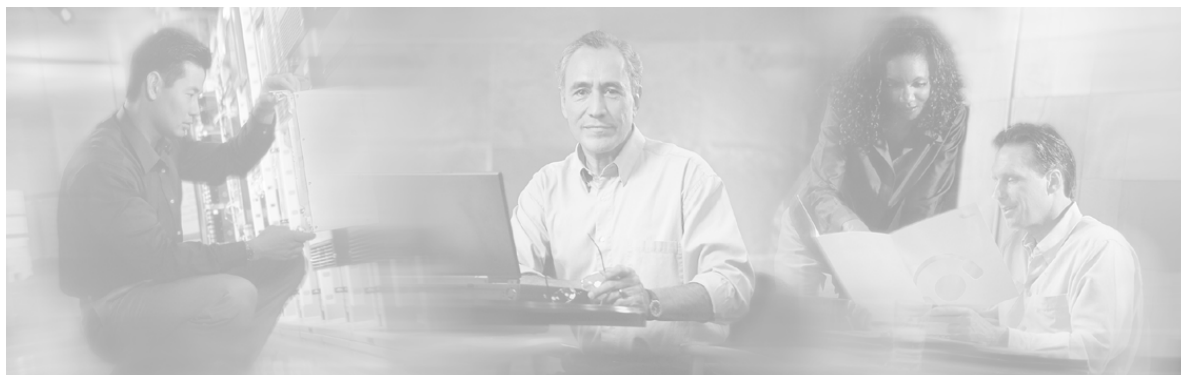
Example

In this example, the Top 10 Conversations chart is moved up the list of displayed graphs by one place:

```
host(config-custom-dashboard-go)# up "Top 10 Conversations"
```

In the following example, the GUI End-to-End Latency graph is moved up the list of displayed graphs by three places:

```
host(config-custom-dashboard-go)# up 3 "End-to-end Delay"
```

11 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. 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
```




12 Appendix B: Common Application Static Port Assignments

The Cisco ADE 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
SNNTTP	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



13 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 Half-Life Ping traffic, you use the following command:

```
host(config-cmap)$ match application "half-life ping"
```

OR

```
host(config-cmap)$ match application "Half-Life Ping"
```

AARP	Abacast	Abacast transfer
Agresso	Amanda	Amanda transfer
AppleTalk	Ares	Ares transfer
ARP	Audiogalaxy	Audiogalaxy transfer
Battle.net	Battlefield 1942.	Battlefield 2142.
BGP-4	BitTorrent encrypted transfer	BitTorrent KRPC
BitTorrent tracker	BitTorrent transfer	BOOTP
BSD Rlogin	BSD Syslog	BuddyBuddy
Chat at chat.zone.com	Citrix CGP	Citrix ICA
ClubBox	ClubFolder	Congaltan
CoolDisk	Corvil SSP	Counter-Strike: Source
CrazyFile download	CrazyFile search	CTS bookook
CTS bridge	CTS daewoo	CTS daishin
CTS dongyang	CTS generic	CTS hanyang
CTS hyundai	CTS kyobo	CTS Kyobo AnchorSpot2
CTS leading	CTS merit	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	Day of Defeat: Source
DCE RPC	Diablo 2	Direct Connect
Direct Connect ping	Direct Connect search result	Direct Connect transfer
DiskPop	DiskPot	DiskPump

DiyHard	DiyHard search	DiyHard transfer
DNS	DSLReports speed test	EBS lecture
eDonkey	eDonkey encrypted	EGP
EIGRP	ENdisk	EVE Online
eXeem search	eXeem tracker	F-Secure virus definition
FileBee	FileGuri	FilePia
First Class	FLICKA	Foldero
FolderPlus	FreePop	FreePop transfer
FTP	FTP transfer	GameSpy
GameSpy chat	GameSpy server query	GIT
Gnutella	Gnutella transfer	GRE
GroupWise	Gunbound	H.245
H.323	Half-Life	Half-Life 2
Half-Life 2: Lost Coast	Half-Life ping	Half-Life: Source
Hanafos QBic	Hangame GoStop	Hardmoa
Hello	Hot Standby Router Protocol	HotDisk
HotDisk transfer	HotLine	HotLine transfer
HP JetDirect	HTTP	HTTP media stream
HTTP proxy	HTTP RealPlayer stream	ICMP
iDisk	IMAP4	iPop
IPSec	IPv6	IPX
IRC	IRC DCC chat	IRC DCC transfer
Iron Mountain Connected	iSCSI	ISO Transport Over TCP
JJangFile	JJangFile transfer	JJangHard download
JJangHard upload	Joost registration	Joost-UDP
Kademlia	Kazaa	Kazaa server
Kazaa transfer	Kerberos v5	Kontiki
Kontiki transfer	Kor-p2p-generic search	Lotus Notes
Lotus Sametime	ManoLito	ManoLito transfer
MAPI over DCE RPC	McAfee SecureCast	MelOn
MGCP	MGCP transfer	MMS
MS SMServer	MSN messenger	MSN messenger chat
MSN messenger over HTTP	MSN messenger transfer	MySQL
Napster	Napster WinMX	Napster WinMX transfer
NateOn	NateOn filerom	NateOn login
NateOn transfer	NeoFolder	NetBios Name Service
NetWare	NNTP	NTP
OnFile	OpenFT transfer	OpenVPN
OSCAR	OSCAR over HTTP	OSCAR P2P
Others	p2pia	PDBox
PDBox ping	PDBox W	Peepop
Peepop search	PeerEnabler	PeerEnabler transfer
POP3	PPLive	PPStream
Pruna Plus	Q.931	QQ
QQ login	QQ Login	QQ transfer
Radius	RAdmin	Radmin Communication
Rakion	Red Swoosh	Red Swoosh transfer
RPC v2	RSH	Rsync
RTMP	RTMPT	RTP
RTSP	RTSP media stream	Runescape
SCCP	Second Life	Service Location Protocol
Share	SILC	SIP

SIP pickup	SIP RTCP	SIP RTP
Skype discovery	Skype login	Skype-Hub2Hub
Skype-P2P	Skype-SSL	Skype-TCP
Skype-UDP	Slingbox media stream	SMB
SMTP	SNMP v1	SNMP v2c
SNMP v3	SOAP over HTTP	Socks v4
Socks v5	SoftEther	Softnyx login
Soribada	Soribada search	Soulseek
Soulseek transfer	Source engine server	SpotLife
SSH	SSL v2	SSL v3
Steam	Steam transfer	Steam UDP
Sunfile	SunFolder	SVN m
TDS	TeamSpeak	Telnet
Teredo	Terminal Services	TFTP
TFTP transfer	Thunder	Thunder UDP
Tinc VPN	TNS	Tor
Toto disk transfer	TPTEST	TPTEST transfer
UMA	undefined	Undetermined
Unknown	Unreal Tournament	Unreal Tournament transfer
UPnP	V-share	Vanguard
VDisk	Vendetta Online	Vendetta Online updater
Ventrilo VoIP	VMware	VNC
WebDAV	WeDisk	WinNy v1
WinNy v2	World of Warcraft	WeDisk
WinNy v1	WinNy v2	World of Warcraft
World of Warcraft login	X11	Xfire
XMMS Phone Home	XMPP	Xtoc
Yahoo! messenger	Yahoo! voice	Yahoo! webcam chat



14 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 Elektronik 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 (Configuration Test Protocol)
9001	Bridge Communications XNS Systems Management
9002	Bridge Communications TCP/IP Systems Management
9003	Bridge Communications
FF00	BBN VITAL LANBridge cache wakeup



15 Index

?

? command 10-11

A

Active flows graph
 event analysis 5-38

alarms
 quality, overview 1-7
 quality, tab 1-7

Alarms
 configuring severity, frequency 9-34
 filtering results 4-14
 monitoring quality 4-12
 quality, reporting results 4-15
 quality, sorting results 4-14
 quality, types 4-13
 recent, dashboard 4-6

alerts
 system, tab 1-8
 system, overview 1-8

allow command 10-13

Analyzing an event
 event analysis 5-26

Application recognition
 upgrading 9-19

ATM PVC, FR PVC, Metro Ethernet, Leased Line
 deployment
 basic (GUI) 3-2
 basic, CLI 8-41
 basic, defining remote sites (GUI) 3-5
 basic, editing local site (GUI) 3-3
 dual-homed (GUI) 3-8
 dual-homed, CLI 8-46
 dual-homed, defining policy-maps (GUI) 3-9
 dual-homed, defining remote sites (GUI) 3-11
 dual-homed, editing the local site (GUI) 3-9

attach command 10-14

attached-ports command 10-15

Attaching a traffic policy to an interface (CLI) 8-31

Average bit rate graph
 event analysis 5-36
 traffic insight 6-11

Average packet rate graph
 event analysis 5-37
 traffic insight 6-12

B

Backing up configuration files 9-17

Backing up packet capture files 9-17

backup command 10-16

bandwidth command 10-18

Bandwidth Quality Manager mode
 switching to System Administration 1-7

bandwidth sizing
 overview 1-5
 tab 1-5

Bandwidth sizing
 Corvil Bandwidth graph results 7-9
 defining custom report periods 7-5
 filtering results 7-5
 monitoring multi-class requirements 7-12
 monitoring single-class requirements 7-11
 overview 7-1
 recommendations 7-7
 reporting results 7-6
 selecting a report period 7-4
 sorting results 7-5
 viewing results 7-7

Byte-counts graph
 event analysis 5-36

C

capture command 10-20

Changing passwords 9-2

class command 10-22

class-adjust command 10-24

Class-map
 defined 2-14
 overview 2-14

class-map command 10-26

Class-maps

- configuring (GUI)..... 2-15
- defining a match rule (GUI) 2-15

clear command 10-27

clock set command 10-28

clock timezone command 10-28

Command completion (CLI) 8-3

configuration

- overview 1-7
- tab 1-7

Configuration

- default network service objective 2-3
- network service objective 2-3
- order of tasks 2-1
- overview 2-1

Configuration file

- defining a network service objective (CLI) 8-5
- defining a traffic class (CLI) 8-7

Configuration files

- attaching a traffic policy to an interface (CLI) 8-31
- combining match-all and match-any statements..... 8-10
- defining a remote site (CLI) 8-17
- defining a router (CLI) 8-17
- defining a traffic policy (CLI) 8-14
- defining an interface (CLI) 8-17
- using nested class-maps (CLI)..... 8-10
- working with (CLI) 8-31

Configuring a custom dashboard..... 2-57, 8-77

Configuring a PNQM Channel..... 2-53

Configuring class-maps (GUI) 2-15

Configuring custom applications..... 2-33

Configuring LFI for an interface 2-55

Configuring network service objectives (GUI) ... 2-6

- attributes 2-6

Configuring network settings 9-6

Configuring NTP time server 9-9

Configuring policy-maps 2-21

Configuring QoS monitoring features (GUI)

- network service objectives..... 2-6

Configuring sites

- editing the local site..... 2-41

Congestion analysis

- Sizing Index defined..... 5-3

Congestion

- monitoring 5-2

connects-to command..... 10-31

copy command 10-32

custom applications

- configuration (GUI)..... 2-33

Custom applications

- overview 2-32

custom dashboard

- configuration (GUI)..... 2-57, 8-77

Custom dashboard

- overview 2-57, 8-77

custom-application command..... 10-35

custom-dashboard command 10-37

D

dashboard

- overview 1-3
- tab 1-3

Dashboard

- introduction 4-2
- navigation tree..... 4-7
- recent alarms 4-6
- top application results 4-11
- viewing summary interface and class results 4-7
- WAN application leaders 4-5

decapsulate command..... 10-38

Defining policy-maps (CLI) 8-14

Defining a network service objective (CLI) 8-5

- QoS commands 8-5

Defining a remote site (CLI)..... 8-17

Defining a router (CLI)..... 8-17

Defining a traffic class

- combining match-all and match-any statements 8-10
- match commands (CLI) 8-9
- nested class-maps (CLI)..... 8-10

Defining a traffic class (CLI)..... 8-7

Defining a traffic filter

- event analysis..... 5-29

Defining a traffic policy

- commands (CLI) 8-15

Defining a traffic policy (CLI) 8-14

Defining an interface CLI) 8-17

Defining class-maps (CLI) 8-7

Defining remote sites, routers and interfaces

- commands (CLI) 8-17

delete command..... 10-40

Deleting

- remote site..... 2-57

Deleting a configuration object or entry 8-4

description command..... 10-41

Diagnostics 9-20

- audit trail, viewing 9-23
- storing system log messages 9-25
- technical support information 9-24
- watchdog operation 9-25

dir command 10-42

Disabling event detection packet capture 5-40

Disabling features

- overview 2-6

domain command 10-43, 10-44

down command 10-45, 10-170

duration command 10-47

E

Editing

- remote site..... 2-56

Editing the local site 2-41

estimate-service-level command 10-92, 10-97
 ethernet command 10-48
 event analysis
 overview 1-4
 tab 1-4
 Event analysis
 active flows graph 5-38
 analyzing an event 5-26
 average bit rate graph 5-36
 average packet rate graph 5-37
 byte-counts graph 5-36
 defining a traffic filter 5-29
 defining custom report periods 5-5
 delay Corvil Bandwidth results 5-19
 disabling event detection packet capture 5-40
 expected delay results 5-12, 5-15
 expected loss results 5-14, 5-17
 expected priority drops results 5-24
 filtering results 5-6
 investigating events 5-25
 microburst detection 5-9
 microburst results 5-18, 5-35
 Network Service Index results 5-21
 overview 5-2
 packet-counts graph 5-37
 priority class Corvil Bandwidth results 5-23
 queue length Corvil Bandwidth results 5-20
 reporting results 5-6
 selecting a report period 5-5
 sorting results 5-5
 viewing packet size distributions 5-38
 viewing round-trip delay and loss 5-7
 viewing top applications 5-31
 viewing top conversations 5-34
 viewing top listeners 5-33
 viewing top talkers 5-32
 zoom feature 5-28
 event-capture command 10-21
 exit command 10-49

F

Fault notification
 checking configuration status 9-35
 Filter classes
 using (CLI) 8-37
 filter-class command 10-50
 Filtering results
 alarms 4-14
 bandwidth sizing 7-5
 event analysis 5-6
 system alerts 9-22
 traffic insight 6-5
 Filtering traffic
 event analysis 5-29

G

gps command 10-52

graph command 10-53
 graph-order command 10-55
 GUI
 overview 1-1

H

Help (CLI)
 using 8-2
 help command 10-57
 Hybrid deployment
 configuring, CLI 8-68
 Hybrid deployment (GUI) 3-30

I

Identifying traffic leaders
 traffic insight 6-14
 Interface
 defined 2-37
 interface command 10-59
 IP address access
 restricting 9-7

L

License
 installation 9-4
 installation using ssh 9-5
 status 9-4
 license command 10-60
 link-adjust command 10-61
 Live View 4-24
 Local site
 defined 2-37
 editing 2-41
 local-site command 10-63
 log command 10-64
 logging command 10-65
 Logging Out (CLI) 8-5

M

manual packet capture
 performing 5-41
 match any command 10-68
 match application command 10-69
 match class-map command 10-71
 match command 10-66
 match ethertype command 10-72
 match ether-type command 10-72
 match gre command 10-74
 match ip command 10-75
 match mpls command 10-78
 match tcp command 10-80
 match udp command 10-83

match vlan command	10-86
max-reserved-bandwidth command	10-89
measure-bandwidth command	10-90
measure-microburst command	10-95, 10-107
measure-ping command	10-93
media command	10-98
Microburst detection	
event analysis	5-35
Modes	
switching	1-7
Monitoring	
congested interfaces	5-2
event analysis overview	5-2
traffic insight, overview	6-1
more command	10-102
More prompt	8-4
MPLS VPN, Internet VPN, Private VPN	
basic (GUI)	3-14
basic, CLI	8-50
basic, defining a remote site (GUI)	3-18
basic, defining class-maps (GUI)	3-15
basic, defining network service objectives (GUI)	3-15
basic, defining policy-maps (GUI)	3-16
dual-homed (GUI)	3-23
dual-homed, CLI	8-60
dual-homed, defining class-maps (GUI)	3-24
dual-homed, defining network service objectives (GUI)	3-24
dual-homed, defining policy-maps (GUI)	3-25
dual-homed, defining remote sites (GUI)	3-28
dual-homed, editing the local site (GUI)	3-26

N

Network deployments	
configuring (CLI)	8-41
Network model	
ATM PVC, FR PVC, Metro Ethernet, Leased line	2-38
MPLS VPN, Internet VPN, Private VPN	2-39
overview	2-37
Network service objective	
defined	2-3
overview	2-3
network service objective command	10-101
network service quality	
overview	1-3
tab 1-3	
Network settings	
configuration (CLI)	9-6
no command	10-104
nso command	10-99
ntp command	10-106
NTP time server	
configuration	9-9

P

Packet capture	
backing up files	9-17

manual, copying	5-45
manual, event analysis	5-47
manual, performing	5-41
manual, status	5-44
restoring files	9-18
setting password	5-47
Packet size distribution	
traffic insight	6-13
Packet size distributions	
viewing, event analysis	5-38
Packet-counts graph	
event analysis	5-37
Password	
set packet capture	5-47
password command	10-108
Passwords	
recovery	9-3
users, changing	9-2
Pdf reports	
creating	1-9
Peak-to-mean graph	
traffic insight	6-12
Peer-interface	
defined	2-37
peer-interface command	10-109
ping-address command	10-113
PNQM Channel	
Configuring	2-53
policy-map command	10-119
Policy-maps	
configuring	2-21
low latency queuing configuration (GUI)	2-29
multi-class configuration (GUI)	2-23
single-class configuration (GUI)	2-23
strict priority queuing configuration (GUI)	2-23
weighted-fair queuing configuration (GUI)	2-26
port command	10-120
ppp command	10-121
Pre-queuing traffic	
supported features	4-20
priority command	10-122
priority-level command	10-123

Q

quality alarms	
overview	1-7
tab 1-7	
Quality events timeline	5-3
queue-limit command	10-128
queuing-targets command	10-127

R

Recovering passwords	9-3
reload command	10-129
Remote site	

defined.....	2-37
editing.....	2-56
Remote sites	
deleting.....	2-57
Reporting results	
alarms.....	4-15
bandwidth sizing.....	7-4, 7-6
event analysis.....	5-6
traffic insight.....	6-4, 6-5
Reports	
generating.....	1-9
overview.....	1-9
restore command.....	10-131
Restoring configuration files.....	9-18
Restoring packet capture files.....	9-18
Restoring system software.....	9-15
Restricting IP access.....	9-7
Restricting SNMP access.....	9-6
Reviewing the system log.....	9-24
Router	
defined.....	2-37
router command.....	10-132

S

Saving configuration changes (CLI).....	8-5
service command.....	10-133
service-policy command.....	10-134
Setting system time.....	9-8
Setting the time zone.....	9-9
setup command.....	10-135
show command.....	10-136
shutdown command.....	10-146
signature streaming protocol.....	8-19
Site	
defined.....	2-37
site command.....	10-147
Site subnet	
defined.....	2-37
size command.....	10-148
size-for command.....	10-125
Sizing Index	
defined.....	5-3
Sizing policy	
busy period overview.....	2-8
Sizing recommendations.....	7-7
snaplength command.....	10-149
SNMP access	
restricting.....	9-6
SNMP Traps	
configuring fault notification.....	9-26
snmp-server command.....	10-150
Sorting results	
bandwidth sizing.....	7-5
event analysis.....	5-5
quality alarms.....	4-14
system alerts.....	9-22

traffic insight.....	6-5
Sparklines.....	4-4
SSP.....	8-19
start capture command.....	10-156
start command.....	10-155
status command.....	10-157
Storing system log messages.....	9-24
subnet command.....	10-161
Subnet filtering (CLI).....	8-34
Supported features	
interface direction.....	4-20
pre-queuing, post-queuing traffic.....	4-20
Switching modes.....	1-7
System Administration mode	
switching to Bandwidth Quality Manager.....	1-7
system alerts	
overview.....	1-8
tab 1-8	
System alerts	
commenting.....	9-22
configuring severity, frequency.....	9-34
filtering results.....	9-22
sorting.....	9-22
types.....	9-21
viewing.....	9-20
System status and resources.....	9-10

T

terminal command.....	10-167
Time settings	
configuration.....	9-8
Time zone	
configuration.....	9-9
Top applications	
viewing, event analysis.....	5-31
viewing, traffic insight.....	6-14
Top conversations	
viewing, event analysis.....	5-34
viewing, traffic insight.....	6-17
Top listeners	
viewing, event analysis.....	5-33
viewing, traffic insight.....	6-16
Top talkers	
viewing, event analysis.....	5-32
viewing, traffic insight.....	6-15
traffic insight	
overview.....	1-4
tab 1-4	
Traffic insight	
average bit rate graph.....	6-11
average packet rate graph.....	6-12
class results overview.....	6-7
filtering results.....	6-5
identifying interface and class traffic patterns.....	6-11
identifying traffic leaders.....	6-14
microburst results.....	6-9
packet size distribution chart.....	6-13

peak-to-mean graph 6-12
reporting results 6-5
sorting results 6-5
viewing interface and class results 6-7
viewing top applications 6-14
viewing top conversations 6-17
viewing top listeners 6-16
viewing top talkers 6-15
Traffic Insight
 defining custom report periods 6-4
 selecting a reporting period 6-4
Traffic Insight results
 overview 6-1

U

up command 10-170
Upgrading the application recognition module . 9-19
User sessions

viewing 9-3

V

Viewing live results 4-24
Viewing round-trip delay and loss 5-7

W

WAN application leaders
 dashboard 4-5

Z

Zoom feature
 event analysis 5-28