

a mind for networks



NetXplorer

Centralized, Proactive Management of all Network Traffic

Operation Guide

(P/N D357102 R9)



NetXplorer

Centralized, Proactive Management of all Network Traffic

Operation Guide

P/N D357102 R9



Important Notice

Allot Communications Ltd. ("Allot") is not a party to the purchase agreement under which NetEnforcer or Service Gateway was purchased, and will not be liable for any damages of any kind whatsoever caused to the end users using this manual, regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ALLOT OR ANY OF ITS SUBSIDIARIES. ALLOT ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Please read the End User License Agreement and Warranty Certificate provided with this product before using the product. Please note that using the products indicates that you accept the terms of the End User License Agreement and Warranty Certificate.

WITHOUT DEROGATING IN ANY WAY FROM THE AFORESAID, ALLOT WILL NOT BE LIABLE FOR ANY SPECIAL, EXEMPLARY, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR ANTICIPATED PROFITS, OR LOST BUSINESS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright

Copyright © 1997-2012 Allot Communications. All rights reserved. No part of this document may be reproduced, photocopied, stored on a retrieval system, transmitted, or translated into any other language without a written permission and specific authorization from Allot Communications Ltd.

Trademarks

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Allot and the Allot Communications logo are registered trademarks of Allot Communications Ltd.

Version History

Doc Revision	Internal Build	Product Version	Published	Summary of Changes
9	V9b17	NX12.3	29.05.12	
9	V9b16	NX12.3	09.05.12	GA Version
9	V9b15	NX12.3	02.05.12	Added tethering condition, IPv6 support, NIC tab, encrypted communication with captive portal, new scheduling options for reports
9	V9b14	NX12.2.1	01.05.12	
9	V9b13	NX12.2	09.02.12	Edits to mobile analytics
9	V9b12	NX12.2	19.01.12	Release
9	V9b11	NX12.2	12.01.12	
9	v9b10	NX12.2	15.12.11	Minor edits to mobile analytics
9	v9b9	NX12.2	15.11.11	Accounting information moved to NX Installation and Admin Guide
9	v9b8	NX12.2	24.10.11	Reports section restructured; Mobile Analytics and selective bypass added
9	v9b7	NX12.1	6.9.11	
9	v9b6	NX12.1	4.9.11	
9	v9b5	NX12.1	24.8.11	

CONTENTS

Important Notice	i
Copyright	i
Trademarks	i
CHAPTER 1: INTRODUCING NETXPLOLER.....	1-1
What is NetXplorer?	1-1
Terms and Concepts.....	1-1
Catalog	1-1
Line	1-1
Pipe	1-2
Virtual Channel.....	1-2
NetEnforcer.....	1-2
Service Gateway	1-2
Subscriber Management Platform.....	1-3
AOS	1-3
Service Plan	1-3
CHAPTER 2: GETTING STARTED	2-1
Accessing NetXplorer	2-1
NetXplorer User Interface	2-2
Menu Bar	2-2
Main Toolbar	2-11
Quick Access Toolbar.....	2-13
Navigation Pane.....	2-13
Application Pane.....	2-14
Logs Pane.....	2-14
General NetXplorer Conventions	2-15
NetXplorer Language	2-16
CHAPTER 3: CONFIGURING NETXPLOLER.....	3-1
Enabling NetXplorer Server.....	3-1
Viewing the Network.....	3-2
Adding a NetEnforcer or Service Gateway	3-4
Configuring a NetEnforcer or Service Gateway.....	3-7
NetEnforcer or Service Gateway Configuration Parameters	3-7
Configuring the Network.....	3-28
Network Configuration Parameters	3-28
Asymmetrical Traffic	3-43
Guidelines	3-44
Asymmetric Configuration	3-45
CHAPTER 4: DEFINING CATALOG ENTRIES.....	4-1

Working with Catalogs	4-1
Catalog Icons	4-3
Accessing Catalogs	4-3
Deleting Entries from a Catalog	4-4
Host Catalog.....	4-5
Defining Host Lists	4-5
Grouping Hosts	4-10
Creating a Host Text File.....	4-13
Creating a Host Group Text File.....	4-14
Subscriber Host Groups	4-14
Country Classification	4-15
Searching for Hosts.....	4-16
Service Catalog	4-17
Defining a Service	4-19
Defining a Service Group	4-21
Adding Content.....	4-24
Adding User Defined Signatures	4-26
Protocol Updates.....	4-32
Time Catalog.....	4-42
ToS (Type of Service) Catalog.....	4-45
User Defined ToS Entry	4-46
Encapsulation Catalog	4-47
Defining VLANs.....	4-47
Defining GREs.....	4-48
Defining Encapsulation Groups.....	4-49
Quality of Service Catalog	4-51
Ignoring Quality of Service	4-52
Defining QoS for Lines.....	4-52
Defining QoS for Pipes.....	4-56
Defining QoS for Virtual Channels	4-60
Service Activation Catalog.....	4-65
Port Redirection	4-66
Captive Portal	4-67
VLAN Redirection.....	4-70
Integrated Services.....	4-72
DoS Catalog.....	4-78
Quota Catalog.....	4-80
Daily Quota Time Synchronization	4-83
Quota Enforcement Thresholds	4-83
Service Plan Catalog	4-83
Interface Catalog	4-91
Charging Application Catalog.....	4-93
Charging Plan Catalog.....	4-95
Mobile Device Catalog	4-98
CHAPTER 5: DEFINING POLICIES.....	5-1

NetXplorer Enforcement Policy	5-1
Overview.....	5-1
Enforcement Policy Elements.....	5-2
Using Lines, Pipes, Virtual Channels and Conditions	5-6
NetXplorer Enforcement Policy Editor	5-7
NetXplorer Charging Policy	5-28
Overview.....	5-28
NetXplorer Charging Policy Editors.....	5-29
CHAPTER 6: NETXPLOER ALARMS.....	6-1
Overview.....	6-1
Alarm Object Indicators.....	6-1
Navigation Pane.....	6-2
Configuring Alarms, Traps and Actions on Events	6-2
Viewing Events	6-5
Sorting Events.....	6-7
Searching for Events.....	6-7
Configuring User-defined Alarms.....	6-8
Configuring Alarm Definitions.....	6-8
Configuring Alarm Actions	6-13
Assigning Alarms	6-15
Viewing the Alarms Log	6-17
Sorting Alarms.....	6-18
Filtering Alarms.....	6-19
Viewing Alarm Properties	6-21
Searching for Alarms	6-21
Managing Alarms	6-22
Acknowledging Alarms	6-22
Removing Alarms	6-23
Monitoring & Reports.....	6-23
CHAPTER 7: MONITORING REPORTS	7-1
Monitoring Reports Options	7-1
Real-Time Monitoring	7-1
Long-Term Reporting.....	7-2
Mobile Analytics.....	7-2
Monitoring Interface.....	7-3
Quick Access Toolbar.....	7-3
Menu Options	7-5
Navigation Pane.....	7-7
Graph Views	7-8
Monitoring Reports Graphs	7-10
Core Graphs	7-10
Additional Graphs.....	7-10
Subscriber Graphs.....	7-11
Report Descriptions.....	7-12

Core Graphs	7-12
Additional Graphs.....	7-31
Subscriber Graphs.....	7-50
Scheduling a Report	7-88
Defining a Scheduled Report	7-89
Compound Reports	7-95
Working with Graphs	7-97
Data Display Options.....	7-97
Drilling Down into Graph Results	7-98
Favorite View	7-100
Monitoring Groups	7-100

FIGURES

Figure 2-1 – NetXplorer Log On Dialog Box	2-1
Figure 2-2 – NetXplorer Window Components	2-2
Figure 2-3: Quick Access Toolbar – Enforcement Policy Editor.....	2-13
Figure 2-4: Navigation Pane – Network.....	2-13
Figure 2-5: Application Pane.....	2-14
Figure 2-6: Logs Pane displaying Alarms Log.....	2-14
Figure 2-7: Display Language Configuration Dialog.....	2-17
Figure 3-1: NetXplorer Application Server Registration Dialog	3-1
Figure 3-2: Navigation Pane – Network.....	3-3
Figure 3-3: NetEnforcer Properties – New Dialog	3-5
Figure 3-4: NetEnforcer Properties – Import Dialog.....	3-6
Figure 3-5: Configuration – General Parameters	3-8
Figure 3-6: Configuration - Identification & Key Parameters.....	3-9
Figure 3-7: Configuration - SNMP Parameters.....	3-12
Figure 3-8: Configuration - Security Parameters	3-13
Figure 3-9: Configuration - NIC Parameters.....	3-15
Figure 3-10: Configuration - Networking Parameters.....	3-17
Figure 3-11: Configuration – IP Properties	3-19
Figure 3-12: Configuration – Date/Time Parameters	3-22
Figure 3-13: Configuration – Service Activation Parameters	3-23
Figure 3-14: Configuration – Slots and Boards – AC-10000.....	3-26
Figure 3-15: Configuration – Slots and Boards – SG-Sigma	3-27
Figure 3-16: Network Configuration – Servers.....	3-29
Figure 3-17: Network Configuration – SNMP.....	3-30
Figure 3-18: Network Configuration - SMP tab.....	3-32
Figure 3-19: Network Configuration - SMP Domains tab	3-33
Figure 3-20: Network Configuration - Accounting tab.....	3-34

Figure 3-21: Network Configuration – Protocol Updates tab	3-35
Figure 3-22: Network Configuration – Service Protector tab	3-36
Figure 3-23: Network Configuration – Integrated Service tab.....	3-37
Figure 3-24: WebSafe Blacklist/Whitelist Format	3-40
Figure 3-25: Network Configuration – Net Awareness tab.....	3-42
Figure 3-26: Network Configuration – Mobile Data tab.....	3-43
Figure 3-27: Asymmetry Network Diagram	3-44
Figure 3-28: Asymmetry Configuration dialog	3-45
Figure 3-29: Asymmetry Group - New dialog	3-46
Figure 3-30: VLans Settings dialog.....	3-46
Figure 4-1: Sample Catalog.....	4-3
Figure 4-2: Quick Access Toolbar – Catalog Editor	4-4
Figure 4-3: Host Catalog	4-5
Figure 4-4: Host List Entry Properties – New Host List	4-7
Figure 4-5: Add Host Item	4-8
Figure 4-6: Entry Scope Properties	4-8
Figure 4-7: External Text File Host List Entry Properties	4-9
Figure 4-8: Host Group Entry Properties	4-11
Figure 4-9: External Text File Host Group Entry Properties	4-12
Figure 4-10: Dynamic External Text File Host Group Entry Properties.....	4-13
Figure 4-11: Subscriber Host Group Entry Properties	4-15
Figure 4-12: Country Classification Entry Properties	4-15
Figure 4-13: Host Search Dialog	4-17
Figure 4-14: Service Catalog.....	4-18
Figure 4-15: Service Entry Properties	4-20
Figure 4-16: Ports Entry Properties – New Service	4-20
Figure 4-17: Service Protocol Library.....	4-21
Figure 4-18: Add Group Items	4-22
Figure 4-19: Move Service Wizard – Select Source	4-24

Figure 4-20: Service Entry Properties – New Content	4-25
Figure 4-21: Application Type Content Editor.....	4-26
Figure 4-22: HTTP UDS Entry Properties	4-28
Figure 4-23: HTTP UDS Entry Properties -Add	4-29
Figure 4-24: Edit Content Values dialog.....	4-31
Figure 4-25: Service Catalog Web Updates Configuration tab	4-33
Figure 4-26: Protocol Update – Pending Changes	4-35
Figure 4-27: Protocol Update – Installation to NetXplorer Server Summary	4-36
Figure 4-28: Protocol Update Wizard – Installation to Devices.....	4-37
Figure 4-29: Version to Install to Device	4-39
Figure 4-30: Protocol Update – Pending Changes	4-40
Figure 4-31: Protocol Update – Installation to NetXplorer Server Summary	4-40
Figure 4-32: Protocol Update Wizard – Rollback Devices – Rollback to Previous Version	4-42
Figure 4-33: Time Entry Properties.....	4-43
Figure 4-34: Add Time Item.....	4-43
Figure 4-35: Sample ToS Catalog	4-45
Figure 4-36: ToS Catalog – Predefined Entry Properties.....	4-46
Figure 4-37: ToS Entry Properties	4-46
Figure 4-38: VLAN Entry Properties dialog	4-48
Figure 4-39: GRE Entry Properties dialog	4-49
Figure 4-40: GRE Entry Properties dialog	4-50
Figure 4-41: Default QoS Catalog.....	4-51
Figure 4-42: New Line QoS Entry Properties	4-53
Figure 4-43: Line Enhanced QoS Entry Properties.....	4-54
Figure 4-44: Defining QoS for Pipes.....	4-56
Figure 4-45: Pipe Enhanced QoS Entry Properties	4-58
Figure 4-46: Virtual Channel QoS Entry Properties	4-60
Figure 4-47: Virtual Channel Enhanced QoS Entry Properties.....	4-63
Figure 4-48: Virtual Channel Enhanced QoS Entry Properties – Expedited Forwarding	4-65

Figure 4-49: Service Activation Catalog.....	4-66
Figure 4-50: Captive Portal Entry Properties - HTTP.....	4-67
Figure 4-51: Captive Portal Entry Properties - HTTPS.....	4-69
Figure 4-52: VLAN Redirection Entry Properties	4-70
Figure 4-53: Add VLAN Server.....	4-71
Figure 4-54: Local Service Entry Properties	4-72
Figure 4-55: Edit Server	4-74
Figure 4-56: Integrated Service Entry Properties	4-76
Figure 4-57: Integrated Service Entry Properties	4-77
Figure 4-58: Integrated Service Entry Properties	4-78
Figure 4-59: DoS Catalog.....	4-78
Figure 4-60: DoS Entry Properties	4-79
Figure 4-61: Volume Based Quota Entry Properties.....	4-81
Figure 4-62: Time Based Quota Entry Properties	4-82
Figure 4-63: Pipe Service Plan Entry Properties - General	4-84
Figure 4-64: Pipe Service Plan Entry Properties – Conditions/Actions	4-85
Figure 4-65: Pipe Service Plan Entry Properties – Applications.....	4-87
Figure 4-66: Service Plan Application Properties	4-88
Figure 4-67: VC Service Plan Entry Properties - General.....	4-89
Figure 4-68: VC Service Plan Entry Properties – Conditions/Actions.....	4-89
Figure 4-69: Interface Catalog.....	4-91
Figure 4-70: Physical Port Entry Properties	4-92
Figure 4-71: Interface Group Entry Properties.....	4-93
Figure 4-72: Charging Application Catalog	4-94
Figure 4-73: Charging Application Entry Properties	4-94
Figure 4-74: Add Application Service Items.....	4-95
Figure 4-75: Charging Plan Catalog.....	4-96
Figure 4-76: Charging Plan Entry Properties	4-96
Figure 4-77: Add Charging Application Item dialog	4-97

Figure 4-78: Mobile Device Catalog	4-98
Figure 5-1: Line/Pipe/Virtual Channel/Condition Relationship.....	5-1
Figure 5-2: Enforcement Policy Editor	5-7
Figure 5-3: Enforcement Policy Columns Visibility dialog	5-9
Figure 5-4: Defining Enforcement Policy Workflow.....	5-10
Figure 5-5: Insert Line Dialog – Enforcement Policy Tab.....	5-11
Figure 5-6: Insert Pipe Dialog – Enforcement Policy Tab	5-13
Figure 5-7: Insert Pipe Template Dialog – Enforcement Policy Tab	5-15
Figure 5-8: Pipe Service Plan Properties – Insert Dialog	5-18
Figure 5-9: Virtual Channel Properties Dialog.....	5-19
Figure 5-10: Virtual Channel Template Properties Dialog	5-21
Figure 5-11: Virtual Channel Service Plan Properties – Insert Dialog	5-22
Figure 5-12: Condition Properties Dialog	5-23
Figure 5-13: Enforcement Policy Distribution Dialog	5-26
Figure 5-14: Restore Enforcement Policy and Catalogs Dialog.....	5-27
Figure 5-15: Online Charging Policy Editor	5-29
Figure 5-16: Offline Charging Policy Editor.....	5-30
Figure 5-17: New Charging Policy Rule Dialog	5-31
Figure 6-1: Events/Alarms Pane.....	6-2
Figure 6-2: Event Types Configuration.....	6-3
Figure 6-3: Action Alarm Definition Entry Properties.....	6-4
Figure 6-4: Events Date Coverage	6-5
Figure 6-5: Sample Events Log	6-6
Figure 6-6: Find Dialog.....	6-8
Figure 6-7: Alarm Definition.....	6-9
Figure 6-8: Alarm Definition Entry Properties Dialog.....	6-9
Figure 6-9: New Alarm Definition Entry Properties	6-11
Figure 6-10: Select Alarm Type	6-11
Figure 6-11: Select Direction	6-12

Figure 6-12: Select Units.....	6-12
Figure 6-13: Select Severity	6-12
Figure 6-14: Select Values	6-13
Figure 6-15: Alarm Action Definition Entry Properties – Send Email to	6-14
Figure 6-16: Alarm Action Definition Entry Properties – Script Action	6-14
Figure 6-17: New Alarm Definition Assignment Editor	6-16
Figure 6-18: Alarms Log.....	6-17
Figure 6-19: Alarm Log Filter Definitions: Severity Tab	6-19
Figure 6-20: Alarm Log Filter Definitions: Acknowledge Tab.....	6-19
Figure 6-21: Alarm Log Filter Definitions: Type Tab	6-20
Figure 6-22: Alarm Log Filter Definitions: Date & Time Tab.....	6-20
Figure 6-23: Alarm Log Filter Definitions: Names & Description Tab	6-20
Figure 6-24: Alarm Properties Dialog.....	6-21
Figure 6-25: Find Dialog.....	6-22
Figure 7-1: Quick Access Toolbar – Monitoring Reports	7-3
Figure 7-2: Reports Navigation Pane	7-7
Figure 7-3: Graph Views	7-8
Figure 7-4: Bar Chart	7-9
Figure 7-5: Pie Chart	7-9
Figure 7-6: Line Chart.....	7-9
Figure 7-7: Stack Area Chart.....	7-9
Figure 7-8: Real-Time Monitoring: Statistics dialog, Time tab	7-13
Figure 7-9: Real-Time Monitoring: Statistics dialog, Display tab	7-14
Figure 7-10: NetEnforcer Statistics	7-15
Figure 7-11: Most Active Protocols on Network – Bar Chart.....	7-15
Figure 7-12: Distribution of Specific Protocols on Network – Data Displayed Over Time	7-16
Figure 7-13: Distribution of Specific Protocols on Network – Data Displayed for Period as a Whole	7-16
Figure 7-14: Long-Term Reporting: Protocols dialog box, Time tab	7-17

Figure 7-15: Real-Time Reporting: Protocols dialog, Objects tab	7-18
Figure 7-16: Long-Term Reporting: Protocols dialog, Limits tab	7-19
Figure 7-17: Long-Term Reporting: Pipes dialog, Display tab	7-20
Figure 7-18: Long-Term Reporting: Pipes dialog box, Time tab	7-22
Figure 7-19: Long-Term Reporting: Pipes dialog, Objects tab	7-23
Figure 7-20: Long-Term Reporting: Pipes dialog, Limits tab	7-24
Figure 7-21: Long-Term Reporting: Pipes dialog, Display tab	7-25
Figure 7-22: Real-Time Reporting: Hosts dialog box, Time tab	7-27
Figure 7-23: Real-Time Reporting: Hosts dialog, Objects tab	7-28
Figure 7-24: Real-Time Reporting: Hosts dialog, Limits tab	7-29
Figure 7-25: Real-Time Reporting: Hosts dialog, Display tab	7-30
Figure 7-26: Real-Time Monitoring: Utilization dialog box	7-32
Figure 7-27: Long Term Reporting Typical Time dialog box – Time tab	7-34
Figure 7-28: Time Scope Selections dialog box	7-35
Figure 7-29: Most Popular Pipes on Network – Bar Chart	7-35
Figure 7-30: Long-Term Reporting: Pipe Popularity dialog box, Time tab	7-37
Figure 7-31: Long-Term Reporting: Pipe Popularity dialog, Objects tab	7-38
Figure 7-32: Long-Term Reporting: Pipe Popularity dialog, Limits tab	7-39
Figure 7-33: Long-Term Reporting: Pipe Popularity dialog, Display tab	7-40
Figure 7-34: Asymmetry Traffic Graph	7-41
Figure 7-35: Real-Time Reporting: Asymmetry Traffic dialog box, Time tab	7-42
Figure 7-36: Real-Time Reporting: Asymmetry Traffic dialog, Display tab	7-43
Figure 7-37: WebSafe Traffic	7-44
Figure 7-38: HTTP	7-44
Figure 7-39: Integrated Services	7-45
Figure 7-40: Bandwidth Usage Percentiles	7-45
Figure 7-41: Percentile Protocols	7-46
Figure 7-42: Real-Time Monitoring: VoIP Minutes of Use dialog box, Time tab	7-47
Figure 7-43: Real-Time Monitoring: VoIP Minutes of Use dialog, Limits tab	7-48

Figure 7-44: Real-Time Monitoring: VoIP Minutes of Use dialog, Display tab.....	7-49
Figure 7-45: VoIP Minutes of Use Report	7-50
Figure 7-46: Subscribers Usage Report.....	7-51
Figure 7-47: Service Plan Usage Report	7-52
Figure 7-48: Service Plan Popularity Distribution	7-52
Figure 7-49: Service Plan Quota Usage Analysis	7-53
Figure 7-50: Service Plan Quota Volume Analysis.....	7-53
Figure 7-51: Service Plan Quota Popularity Analysis.....	7-54
Figure 7-52: Cell Distribution Report	7-54
Figure 7-53: Most Active Cells Report	7-55
Figure 7-54: Report Identity Window	7-56
Figure 7-55: Report Topic	7-56
Figure 7-56: Report Subject – Mobile Analytics.....	7-57
Figure 7-57: Report Schedule.....	7-57
Figure 7-58: Session Signaling Report – Bar Graph.....	7-59
Figure 7-59: Session Signaling Report – Table.....	7-59
Figure 7-60: Mobile Analytics: Session Signaling, Time dialog	7-60
Figure 7-61: Mobile Analytics: Time Scope Selection dialog box	7-60
Figure 7-62: Mobile Analytics: Session Signaling, Display dialog	7-61
Figure 7-63: Roaming Out Volume Report – Pie Graph.....	7-62
Figure 7-64: Roaming Out Volume Report – Table.....	7-62
Figure 7-65: Mobile Analytics: Roaming Out Volume, Time dialog	7-63
Figure 7-66: Mobile Analytics: Time Scope Selection dialog box	7-64
Figure 7-67: Mobile Analytics: Roaming Out Volume, Display dialog	7-64
Figure 7-68: Service Plans Metrics Report – Stacked Area Graph	7-65
Figure 7-69: Service Plans Metrics Report – Table	7-65
Figure 7-70: Mobile Analytics: Service Plan Metrics, Time dialog.....	7-66
Figure 7-71: Mobile Analytics: Time Scope Selection dialog box	7-66
Figure 7-72: Mobile Analytics: Service Plans Metrics, Objects dialog	7-67

Figure 7-73: Mobile Analytics: Service Plans Metrics, Display dialog	7-67
Figure 7-74: Service Plans Transits Report – Bar Graph	7-68
Figure 7-75: Service Plans Transits Report – Pie Chart	7-69
Figure 7-76: Mobile Analytics: Service Plan Transits, Time dialog	7-69
Figure 7-77: Mobile Analytics: Time Scope Selection dialog box	7-70
Figure 7-78: Mobile Analytics: Service Plans Transits, Limits dialog	7-70
Figure 7-79: Mobile Analytics: Service Plans Selections dialog	7-71
Figure 7-80: Mobile Analytics: Service Plans Transits, Display dialog	7-71
Figure 7-81: Top Protocols Report Stacked by Device – Bar Graph	7-72
Figure 7-82: Top Protocols Report by Device – Table	7-72
Figure 7-83: Mobile Analytics: Top Protocols, Time dialog	7-73
Figure 7-84: Mobile Analytics: Time Scope Selection dialog box	7-74
Figure 7-85: Mobile Analytics: Top Protocols, Objects dialog.....	7-74
Figure 7-86: Mobile Analytics: Top Protocols, Limits dialog	7-75
Figure 7-87: Mobile Analytics: Device Models Selections dialog.....	7-75
Figure 7-88: Mobile Analytics: Top Protocols, Display dialog	7-76
Figure 7-89: Subscriber Volume Percentiles Report Stacked by Device – Bar Graph	7-77
Figure 7-90: Mobile Analytics: Subscriber Volume Percentiles, Time dialog	7-77
Figure 7-91: Mobile Analytics: Time Scope Selection dialog box	7-78
Figure 7-92: Mobile Analytics: Subscriber Volume Percentiles, Objects dialog.....	7-78
Figure 7-93: Mobile Analytics: Subscriber Volume Percentile, Display dialog	7-79
Figure 7-94: Session Bitrate Report Stacked by Device – Bar Graph.....	7-80
Figure 7-95: Mobile Analytics: Session Bitrate, Time dialog.....	7-80
Figure 7-96: Mobile Analytics: Time Scope Selection dialog box	7-81
Figure 7-97: Mobile Analytics: Session Bitrate, Objects dialog	7-81
Figure 7-98: Mobile Analytics: Session Bitrate, Limits dialog.....	7-82
Figure 7-99: Mobile Analytics: Device Models Selections dialog.....	7-83
Figure 7-100: Mobile Analytics: Session Bitrate, Display tab	7-83
Figure 7-101: Session Bitrate Report Stacked by Device – Bar Graph.....	7-84

Figure 7-102: Mobile Analytics: Session Duration, Time dialog.....	7-85
Figure 7-103: Mobile Analytics: Time Scope Selection dialog box	7-85
Figure 7-104: Mobile Analytics: Session Duration, Objects dialog.....	7-86
Figure 7-105: Mobile Analytics: Session Duration, Limits dialog.....	7-86
Figure 7-106: Mobile Analytics: Device Models Selections dialog.....	7-87
Figure 7-107: Mobile Analytics: Session Duration, Display dialog.....	7-87
Figure 7-108: Report tab	7-89
Figure 7-109: Report Identity Window	7-89
Figure 7-110: Report Topic	7-90
Figure 7-111: Report Subject	7-90
Figure 7-112: Report Objects	7-91
Figure 7-113: Report Time	7-92
Figure 7-114: Report Scope.....	7-93
Figure 7-115: Report Display	7-93
Figure 7-116: Report Schedule.....	7-94
Figure 7-117: Report Definition Summary	7-95
Figure 7-118: Compound Report Properties	7-96
Figure 7-119: Displaying Bandwidth	7-97
Figure 7-120: Most Active Virtual Channels	7-99
Figure 7-121: Protocols Distribution on Virtual Channel VoIP.....	7-99
Figure 7-122: Group Properties – Line Group	7-101
Figure 7-123: Group Properties – Pipe Group	7-102
Figure 7-124: Items Selection – Virtual Channel Group.....	7-103

Chapter 1: Introducing NetXplorer

What is NetXplorer?

NetXplorer is a highly scalable Network Business Intelligence system that centrally manages the NetEnforcer or Service Gateway product line. It enables strategic decision making based on comprehensive network application and subscriber traffic analysis.

With the exponential growth in the use of the Internet, the business of today is how to manage the network environment intelligently. NetXplorer enables real time monitoring of network troubleshooting and problem analysis; it provides long term reporting for capacity planning, tracking usage and trend analysis; it allows for the proactive management of traffic and system-wide alarms; it allows for the collection and export of auditing data for billing and quota purposes. NetXplorer configures the NetEnforcer or Service Gateway device and a central catalog enables global Enforcement Policy provisioning.

Business Network Intelligence assures the true alignment of network and business. NetXplorer gives power to the network service provider or corporation to manage its network and conduct business with intelligence.

Terms and Concepts

This section introduces some of the basic terms and concepts used in NetXplorer.

Catalog

Catalog entries, which are defined in the catalog editor, serve as conditions or actions in the rules which make up a Enforcement Policy. In this way, they can be seen as the building blocks of your Enforcement Policy. Once a catalog has been defined in the catalog editor, it can be reused in different rules.

Line

A line is a logical entity within a Enforcement Policy and represents the highest level of hierarchy. The total bandwidth running through the NetEnforcer or Service Gateway can be divided into lines and each line can then be managed as if it were an independent link. A line consists of a rule based on one or more sets of conditions and a set of actions that apply when all of the conditions are met. The default fallback line exists in every Enforcement Policy. Additional lines can then be added above the fallback line in the Enforcement Policy table. The fallback line cannot be modified or deleted. Traffic which is not classified in any of the lines above it in the hierarchy will be classified in the fallback line. Every line, including the fallback line, contains one or more pipes.

Pipe

A pipe is a logical entity within a Enforcement Policy. The total bandwidth running through each line can be divided into pipes, and each pipe can then be managed independently. Each pipe consists of a rule based on one or more sets of conditions and a set of actions that apply when all of the conditions are met. By default, every line contains at least one pipe – the fallback pipe. Additional pipes can then be added above the fallback pipe in the Enforcement Policy table. The fallback pipe cannot be modified or deleted, and traffic that is not classified into any other pipes within a given line will be classified in the fallback pipe. Every pipe, including the fallback pipe, contains one or more virtual channels.

Virtual Channel

A Virtual Channel (VC) is a logical entity within a Enforcement Policy and represents the most granular level of Enforcement Policy hierarchy. The total bandwidth running through each pipe can be divided into VCs, and each VC can then be managed independently. Each VC consists of a rule based on one or more sets of conditions and a set of actions that apply when all of the conditions are met. By default, every pipe contains at least one VC – the fallback VC. Additional VCs can then be added above the fallback VC in the Enforcement Policy table. The fallback VC cannot be modified or deleted, and traffic that is not classified into any other VCs within a given pipe will be classified in the fallback VC.

NetEnforcer

The NetEnforcer is a broadband optimization device which collects traffic statistics from the network and can implement quality of service per application and per subscriber. Traffic statistics are collected in order to provide both real-time and long-term data about the network. As well as collecting detailed information about the traffic passing through, it, the NetEnforcer can also shape that traffic, applying quality of service parameters which have been pre-defined by the user.

Service Gateway

The Service Gateway is a platform for enhancing service optimization and service deployment. The Service Gateway provides an open, carrier-grade solution for broadband service providers to manage multiple 10 or 1 Gigabit lines and deploy value added services in one integrated platform. Application and subscriber information within the Service Gateway is identified for each traffic flow and subsequently the flow is dispatched to an array of additional services and actions using a single DPI process.

Subscriber Management Platform

Allot's Subscriber Management Platform or SMP is an additional element of the Allot solution which enables Service Providers to manage subscribers or, when integrated with a PCRF in a mobile environment, to manage sessions.

AOS

The Allot Operating System or AOS is Allot's state-of-the-art infrastructure for application identification and service optimization technologies. AOS provides a unified software platform to be used on Allot's newer devices, such as the NetEnforcer series AC-500, AC-1400, AC-3000 and the Service Gateway series SG-Sigma and SG-Sigma E.

Service Plan

Service Plans are used with Allot's Subscriber Management Platform and contain QoS Catalog entries that quickly and easily define key parameters for subscriber accounts, for example, minimum and maximum bandwidth.

Service Plans may be created for Pipes or for VCs, depending upon the structure of the Enforcement Policy table. It is possible to define a Pipe Service Plan, where each VC is defined in the Pipe Service Plan and handles a separate application, or to create individual VC Service Plans for each VC.

Chapter 2: Getting Started

Accessing NetXplorer

Once you have completed the initial setup as described in the NetXplorer Installation and Administration Guide, you can access the NetXplorer via your Web browser. The first time that you connect to the NetXplorer, you may be prompted to install Java 1.6.

To connect to NetXplorer:

1. In Internet Explorer, browse to **http://<<NX IP>>** and select **Launch NetXplorer** in the NetXplorer Control Panel.

OR

Double click the shortcut icon on the desktop or in the system's *Start* menu.

2. The Java Application Starting window is displayed.
3. The NetXplorer Log On dialog is displayed.

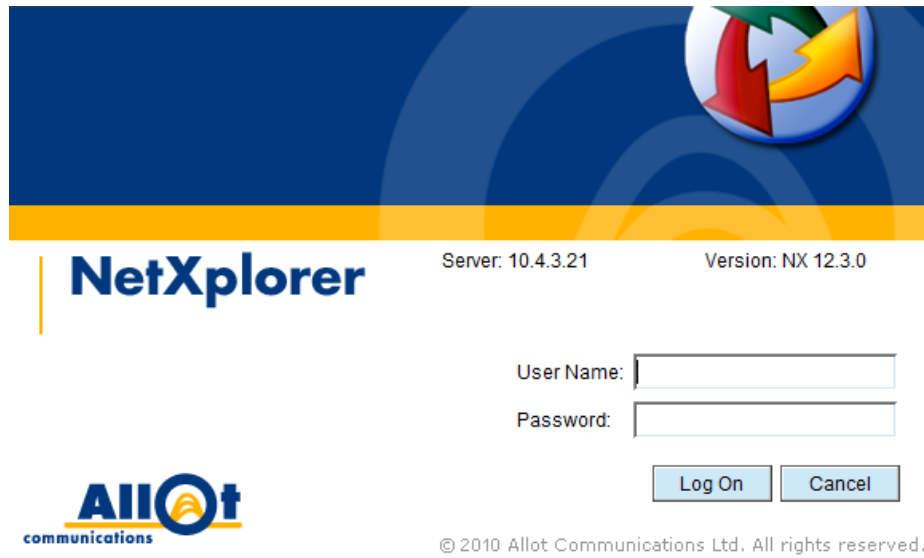


Figure 2-1 – NetXplorer Log On Dialog Box

4. In the **User Name** field, enter **admin** and in the **Password** field, enter **allot** or the password that was established at set up. These are the default user name and password. They may be different if you changed them during the initial configuration.
5. Click **Log On**. The NetXplorer GUI is displayed.

NOTE It may take a few moments to display the NetXplorer GUI.

NetXplorer User Interface

The NetXplorer window is displayed when you open the program.

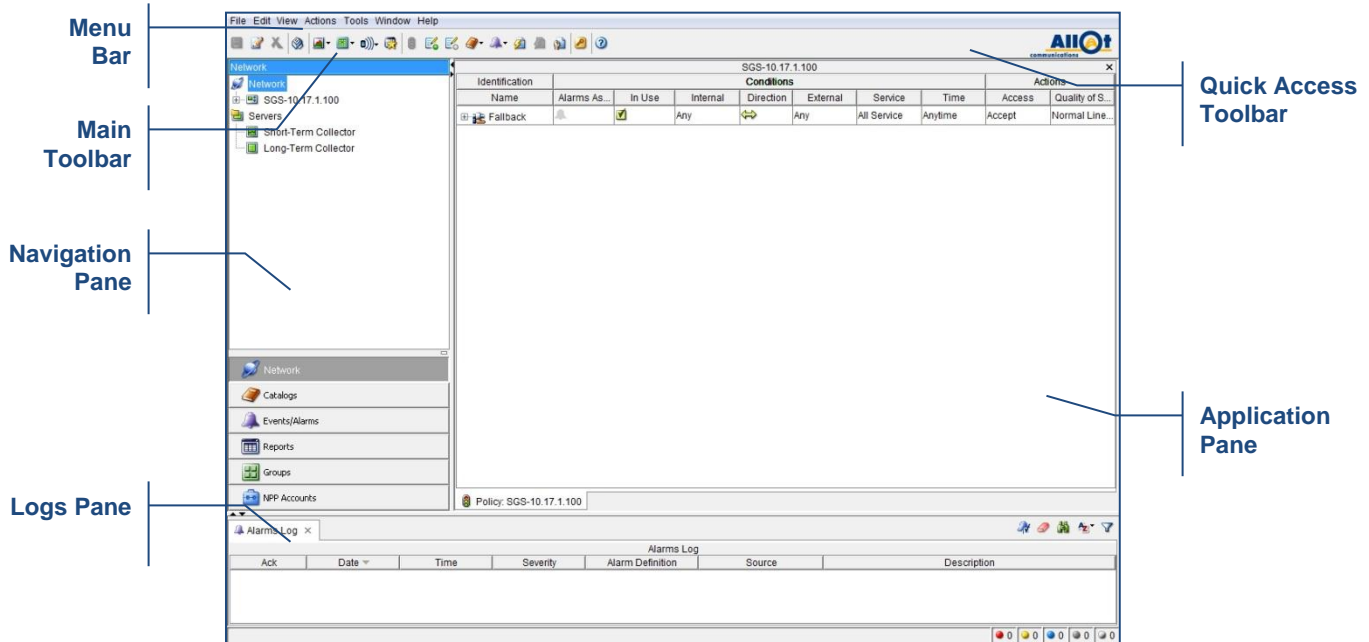


Figure 2-2 – NetXplorer Window Components

This section describes the following NetXplorer window components:

- **Menu Bar**, page 2-2
- **Main Toolbar**, page 2-11
- **Quick Access Toolbar**, page 2-13
- **Navigation Pane**, page 2-13
- **Application Pane**, page 2-14
- **Logs Pane**, page 2-14

Menu Bar

The NetXplorer menu bar provides easy access to the key functionality of the NetXplorer applications. This section describes the available menus and options.

NOTE The options enabled in each of the NetXplorer menus vary according to the currently active application.

File Menu

The *File* menu includes the following options:

OPTION	DESCRIPTION
Reload	Refreshes the display.
Save	Saves and applies changes made in the various NetXplorer applications
Print	Prints the current report, graph or chart.
Exit	Closes the NetXplorer window and exits NetXplorer.

Edit Menu

The *Edit* menu includes the following options:

OPTION	DESCRIPTION
Cut	Enables you to cut an item or catalog entry in the active window.
Copy	Enables you to copy an item or catalog entry in the active window.
Paste	Enables you to paste an item or catalog entry into the active window.
Delete	Enables you to delete an item or catalog entry from the active window.
Select All	Enables you to select all of the items in a table or list.
Find	Enables you to perform a search for a specific item or catalog.

View Menu

The *View* menu includes the following options:

OPTION	DESCRIPTION
Real-Time Monitoring	Enables you to view real-time monitoring data. You can manipulate the data and produce reports, as required. Selecting Real-Time Monitoring displays a submenu containing the available types of reports. Real-Time Monitoring must be enabled by entering an appropriate key. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
Long-Term Reporting	Enables you to collect and view Long-Term Reporting data. You can manipulate the data and produce reports, as required. Selecting Long-Term Reporting displays a submenu containing the available report types. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
Mobile Analytics	Enables you to generate Mobile Analytics graphs. Selecting Mobile Analytics displays a submenu containing the available types of reports. Mobile Analytics requires an SMP and must be enabled by entering an appropriate key. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
Favorite View	Displays a saved arrangement of Monitoring windows as your favorite view. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
Enforcement Policy Editor	Provides access to the Enforcement Policy Editor where you define QoS Enforcement Policy using rules for Lines, Pipes and Virtual Channels. (Refer to <i>Chapter 5, Defining Policies</i> for further information.)
Online Charging Policy	Provides access to the Online Charging Policy Editor where you define Charging policies for use with the Subscriber Management Platform. (Refer to <i>SMP User Guide</i> for further information.)
Offline Charging Policy	Provides access to the Offline Charging Policy Editor where you define Charging policies for use with the Subscriber Management Platform. (Refer to <i>SMP User Guide</i> for further information.)

OPTION	DESCRIPTION
Catalogs	Provides access to the NetXplorer catalogs where you define the possible values to be used in defining policies. Selecting Catalogs displays a submenu containing the available catalogs (Host, Service, Time, TOS, Encapsulation, Quality of Service, Service Activation, DoS, Quota, Service Plan, Interface, Charging Application and Charging Plan). (Refer to <i>Chapter 4, Defining Catalog Entries</i> for further information.)
Alarms	Provides access to NetXplorer's Alarms catalogs where you configure the actions to be taken in response to different types of alarms. Selecting Alarm Definitions displays a submenu containing the available Alarms catalogs (Alarm Definition, Alarm Action Definition, and Event Types Configuration). (Refer to <i>Chapter 6, NetXplorer Alarms</i> for further information.)
Events	Displays the events log for a selected NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel. (Refer to <i>Chapter 6, NetXplorer Alarms</i> for further information.)
Quota Events	Displays the Quota events log for a selected NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel. (This feature is only available with the appropriate key.)
Alarm Definition Assignment List	Displays the Alarm Definition Assignment list for the device selected in the Navigation pane. (Refer to <i>Chapter 6, NetXplorer Alarms</i> for further information.)
Collection Configuration	Displays the Monitoring Collection Parameters for the selected device.
SMP Groups Subscribers Capacity	Enables you to configure the number of Subscribers allowed in each SMP Group. (This feature is only available with the appropriate key.)
Enforcement Policy Distribution	Distributes the Enforcement Policy table of the selected machine NetEnforcer or Service Gateway to other selected NetEnforcer or Service Gateways on the network. Refer to <i>Chapter 5, Defining Policies</i> for more information)

OPTION	DESCRIPTION
Configuration	Enables you to specify server or NetEnforcer or Service Gateway configuration and setup parameters in the Configuration application. (Refer to <i>Chapter 3, Configuring NetXplorer</i> for further information.)
Asymmetry Configuration	Allows you to create Asymmetry Groups and assign devices to each group.

Actions Menu

The *Actions* menu includes the following options:

NOTE These Actions menu items appear when Network is highlighted in the Navigation Pane. The menu items will change depending upon what selection is made in the Navigation Pane.

OPTION	DESCRIPTION
New NetEnforcer	Enables you to add a NetEnforcer or Service Gateway to the Network configuration.
New Collector	Enables you to add a Monitoring Data Collector to the Network configuration.
New Collector Group	Enables you to add a Group of Monitoring Data Collector to the Network configuration.
New SMP	Enables you to add a Subscriber Management Platform to the Network configuration. (This feature is only available with the appropriate key.)
New SMP Group	Enables you to add a Group of Subscriber Management Platforms to the Network configuration. (This feature is only available with the appropriate key.)
New SMP Router	Enables you to add a Subscriber Management Platform Router to the Network configuration when deploying a distributed SMP topology. This configuration is only applicable in specific situations, and for more information contact Allot Customer Support at support@allot.com (This feature is only available with the appropriate key.)
New Catalog Entry	Enables you to add a new entry to a selected category. Refer to <i>Chapter 4, Defining Catalog Entries</i> for further information.
New Alarm/Action Entry	Enables you to define a new Alarm or Action Definition. (Refer to <i>Chapter 6, NetXplorer Alarms</i> for further information.)
New Report Entry	Enables you to define a new report folder, new report or new compound report. (Refer to <i>Chapter 7, Monitoring & Reports</i> for further information.)

OPTION	DESCRIPTION
New Group	Enables you to define a customized group of entities for monitoring purposes (New Line Group, New Pipe Group or New Virtual Channel Group).
New Account	Enables you to add a new user Account to the NetXplorer. (This feature is only available with the appropriate key.)
Properties	Displays the Properties window for the selected device or catalog entry.

Tools Menu

The *Tools* menu includes the following options:

OPTION	DESCRIPTION
NetXplorer Application Server Registration	Enables you to enter the key to activate NetXplorer Server functionality (such as managing multiple NetEnforcers or Service Gateways).
Import NetEnforcer	Enables you to add a NetEnforcer or Service Gateway already installed on the Network to the NetXplorer.
Users Configuration	Enables you to define users for NetXplorer and determine the scope of actions that they are authorized to perform in the system. (This option is enabled for Admin users only.)
Restore Policies and Catalogs	Restores the Enforcement Policy Table and Catalogs of selected NetEnforcer or Service Gateways.
Protocol Updates	Enables you to configure the web-based updates of the Service Catalog.
Display Language Configuration	Enables you to change the language of the NetXplorer GUI.
Add and Activate Subscribers	Enables you to add a new Subscriber to the network and activate their account. (This feature is only available with an SMP Server installed and the appropriate key enabling Subscriber Management. This feature is not available if an SMP Session Management key is used.)
Stop and Remove Subscribers	Enables you to remove an existing Subscriber from the network and deactivate their account. (This feature is only available with an SMP Server installed and the appropriate key enabling Subscriber Management. This feature is not available if an SMP Session Management key is used.)
Subscriber Status	Displays the status and current service plan of a subscriber. (This feature is only available with an SMP Server installed and the appropriate key enabling Subscriber Management.)
Net Unit Information	Displays data concerning Cell usage for mobile traffic. This is relevant for CellWise functionality, described in Appendix F of the SMP User Guide.
Open ServiceProtector	Opens the ServiceProtector GUI if a ServiceProtector is defined in the Network tab (see page 3-36)

OPTION	DESCRIPTION
WebSafe	Allows you to Distribute Files, such as updated white or black lists, to all devices using WebSafe.

Window Menu

The *Window* menu includes the following options:

OPTION	DESCRIPTION
Close <current tab>	Closes the currently selected NetXplorer tab. (The name of the tab is displayed in the option name.)
Close All	Closes all currently active NetXplorer tabs.
<tab name>	Makes a specific NetXplorer tab active. (A separate menu option is displayed for each open tab. The active tab is indicated by a bullet.)










Help Menu








The *Help* menu includes the following options:

OPTION	DESCRIPTION
Index	Provides access to online help.
About NetXplorer	Provides NetXplorer version information.

Main Toolbar

The following buttons provide access to key NetXplorer functionality from the Main Toolbar.

BUTTON	DESCRIPTION
 Save	Saves changes made in the currently selected active application.
 Properties	Displays the properties of the selected item or catalog entry.
 Delete	Enables you to delete an item or catalog entry from the active window.
 Print	Prints the current report, graph or chart.
 Real-Time Monitoring	Enables you to view real-time monitoring data. You can manipulate the data and produce reports, as required. Selecting Real-Time Monitoring displays a submenu containing the available types of reports. Real-Time Monitoring must be enabled by entering an appropriate key. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
 Long-Term Reporting	Enables you to collect and view long-term reporting data. You can manipulate the data and produce reports, as required. Selecting Long-Term Reporting displays a submenu containing the available report types. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
 Mobile Analytics	Enables you to generate Mobile Analytics graphs. Selecting Mobile Analytics displays a submenu containing the available types of reports. Mobile Analytics requires an SMP and must be enabled by entering an appropriate key. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
 Favorite View	Displays a saved arrangement of Monitoring windows as your favorite view. (Refer to <i>Chapter 7, Monitoring Reports</i> for further information.)
 Enforcement Policy Editor	Provides access to the Enforcement Policy Editor where you define QoS Enforcement Policy using Lines, Pipes, Virtual Channels and rules. (Refer to <i>Chapter 5, Defining Policies</i> for further information.)

BUTTON	DESCRIPTION
 Catalogs	Provides access to the NetXplorer catalogs where you define the possible values to be used in defining policies. Selecting Catalogs displays a submenu containing the available catalogs. (Refer to <i>Chapter 4, Defining Catalog Entries</i> for further information.)
 Alarms	Provides access to the Alarms Editor and the Alarms Log. (Refer to <i>Chapter 6, NetXplorer Alarms</i> for further information.)
 Events	Displays the events log for a selected NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel. (Refer to <i>Chapter 6, NetXplorer Alarms</i> for further information.)
 Quota Events	Displays the quota events log for a selected NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel. (Only enabled if SMP/Quota Management is enabled on the Server).
 Configuration	Enables you to specify system configuration and setup parameters in the Configuration application. (Refer to <i>Chapter 3, Configuring NetXplorer</i> for further information.)
 Exit	Closes the NetXplorer window.
 Help Index	Provides access to online help.

NOTE The above buttons are enabled or disabled according to the current selection or operation

Quick Access Toolbar

The Quick Access Toolbar displays those buttons which are most relevant for the operation currently active in the Applications Pane. For example, when the Enforcement Policy Editor is active and a Pipe is selected, those buttons which can be used to manage Pipes and VCs appear in the Quick Access Toolbar.

The Quick Access Toolbar appears on the upper right hand side of the GUI, below the Menu Bar.

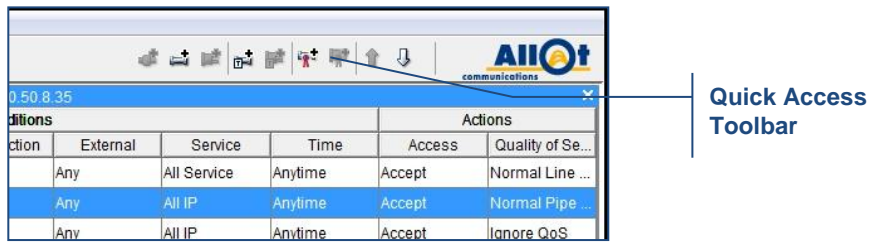


Figure 2-3: Quick Access Toolbar – Enforcement Policy Editor

Navigation Pane

The Navigation pane is divided into two sections. The lower portion of the Navigation pane enables you to select and open various NetXplorer applications. The upper portion of the pane displays a tree-like list of subcomponents or entries according to the application selected in the portion.

For example, when Catalogs is selected in the Navigation pane, the various catalogs are listed in the Navigation tree. To view the details of a specific catalog, select the catalog in the Navigation tree; the Application Details pane is updated accordingly.

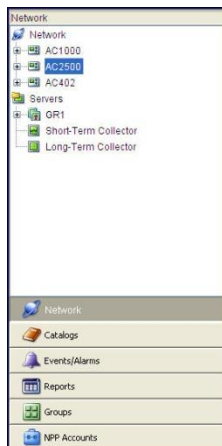


Figure 2-4: Navigation Pane – Network

Application Pane

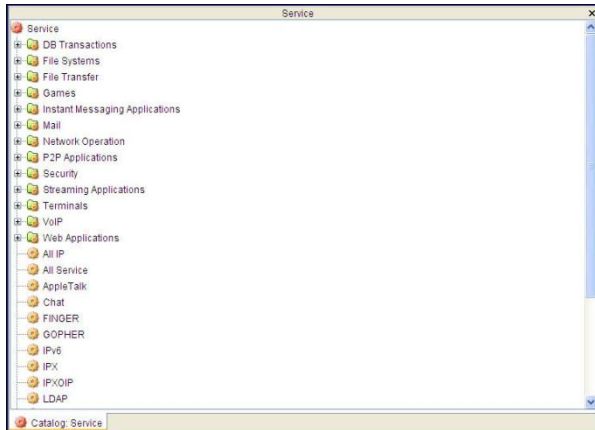


Figure 2-5: Application Pane

The Application Pane displays data regarding the currently active applications and operations.

A tab is displayed at the bottom of the pane for each open application. You can navigate easily between the open applications by clicking the tabs.

Logs Pane

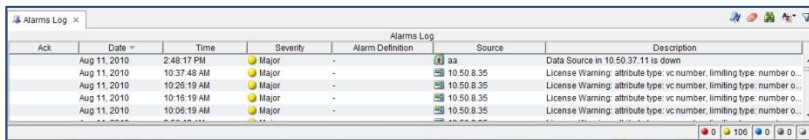


Figure 2-6: Logs Pane displaying Alarms Log

The Logs Pane displays the Alarms Log, a list of the alarms triggered by the alarm definitions. The Alarms Log is automatically refreshed every 30 seconds. The severity of an alarm is indicated by the color of the icon (Info: light gray, Warning: dark gray; Minor: blue; Major: yellow; Critical: red). A checkmark in the leftmost column indicates that the alarm has been acknowledged. The status bar at the bottom of the Alarms Log indicates the total number of active alarms, and provides their breakdown according to severity. For further details on configuring and managing alarms, refer to *Chapter 6, NetXplorer Alarms*.

General NetXplorer Conventions

NetXplorer Application Icons











The following icons are used throughout NetXplorer to represent the NetXplorer applications:




NOTE **NPP Accounts is only available to those users with NPP installed.**


-  Network
-  Catalogs
-  Events/Alarms
-  Reports
-  Groups
-  NPP Accounts


Network Component Icons


The following icons are used throughout NetXplorer to represent the elements of the network:

-  Network
-  NetEnforcer
-  Short Term Monitoring Collector
-  Long Term Monitoring Collector
-  Extended Monitoring Collector
-  SMP
-  SMP Group
-  Line
-  Pipe
-  Virtual Channel

In the Navigation tree, the  icon is added to Line, Pipe or Virtual Channel  indicate that it is the fallback element of its type, as applicable. For example,  represents the default pipe.

The severity of the most serious alarm for a system component) is indicated by the addition of a color-coded alarm icon on the lower right portion of the device icon (Warning: gray; Minor: blue; Major: yellow; Critical: red). For example, , indicates that a major alarm has occurred on the NetEnforcer or Service Gateway.

Accessibility problems are indicated by the addition of an icon in the upper right portion of the device icon. For example, , indicates that the NetEnforcer or Service Gateway is not accessible.

The populated severity of alarms for a system component or one of its sub elements is indicated by the addition of a color-coded alarm icon on the upper left portion of the device icon (Warning: gray; Minor: blue; Major: yellow; Critical: red). For example, , indicates a critical alarm is open for one at least one of the subelements in the network.

Catalog Icons

The following icons are used throughout NetXplorer to represent the different types of catalogs:

	Host		Encapsulation
	Service		Quality of Service
	Time		DoS
	ToS		Quota
	Service Activation		Service Plan
	Interface		Charging Apps
	Charging Plans		Mobile Device

NetXplorer Language

The NetXplorer GUI may be displayed in one of three languages, English, Korean or Chinese. This language may be selected by the user and changed at any time.

To set the language of the NetXplorer GUI:

1. Select **Tools > Display Language Configuration** from the NetXplorer Menu bar.

The Display Language Configuration dialog box appears.



Figure 2-7: Display Language Configuration Dialog

2. Select the appropriate language.
3. Click **Save** to enter the change and close the dialog box.

Chapter 3: Configuring NetXplorer

Enabling NetXplorer Server

In order to manage more than one NetEnforcer or Service Gateway using NetXplorer, NetXplorer Server must be enabled by entering the appropriate key. This key may be entered at installation or at any time following.

To enable NetXplorer Server:

1. Select **Tools > NetXplorer Application Server Registration** from the NetXplorer Menu bar.

The NetXplorer Application Server Registration dialog box appears.

The screenshot shows the 'NetXplorer Application Server Registration' dialog box. It is divided into two main sections: 'General' and 'Attributes'.
General Section:
- Activation Key: NMS-abc-3574X1R12R11112dJ1VT104R1J1VT105R1J1VT106R1J1R8J9000000VT108R1J1R8J
- Serial Number: abc
- Key Version: 1
- Marketing Version: 12
- Expiration Date: Wed Jan 01 00:00:00 IST 2020
Attributes Section:
- Number of Supported Devices: No of Active Elements: 100
- NPP: Enabled, No of Active Elements: 100
- Country Classification Subscription: Enabled
- Net Accounting: Enabled
- APU: Enabled
- Tiered Services: Enabled, Active Subscribers: 9000000
- Tiered Services Gx: Disabled
- Quota Management: Enabled, Active Subscribers: 9000000
- Volume Reporting: Disabled
At the bottom right, there are three buttons: 'Save', 'Delete', and 'Cancel'.

Figure 3-1: NetXplorer Application Server Registration Dialog

2. Enter the Activation Key and Serial Number provided by Allot to enable the NetXplorer Server functionality.

3. A Key Version, Marketing Version and Expiration Date will be generated automatically after clicking **Save**.
4. The number of devices supported by the key is indicated.
5. If Enforcement Policy Provisioning is enabled by the key that has been entered, it will be indicated (along with the maximum number of accounts) after **NPP**. For more information, see the NPP User Guide.
6. If Classification of Hosts by Country is enabled by the key that has been entered, it will be indicated after **Country Classification Subscription**.
7. If Accounting information is enabled by the key that has been entered, it will be indicated after **Net Accounting**.
8. If Service Catalog updates via the web are enabled by the key that has been entered, it will be indicated after **APU**.
9. If Subscriber Management is enabled by the key that has been entered, it will be indicated by one of the following attributes being enabled: **Tiered Services or Quota Management**. In addition, the number of supported active subscribers will be indicated if relevant. For more information, see the SMP User Guide.
10. If Session Management is enabled by the key that has been entered, it will be indicated by at least one of the following attributes being enabled: **Tiered Services Gx, Volume Reporting or Cell Awareness**. In addition, the number of active IP sessions will be indicated if relevant. For more information, see the SMP User Guide.
11. Click **Save** to enter the key and close the dialog box.

Viewing the Network

NetXplorer enables the central monitoring, configuration and management of multiple NetEnforcers or Service Gateways in your network. It enables easy access to devices via the network Navigation tree.

To view network components:

Click **Network** in the lower portion of the Navigation pane to display the network structure in the Navigation tree.

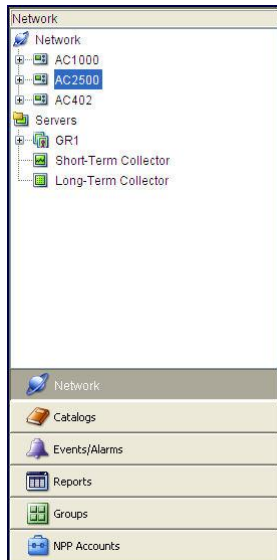











Figure 3-2: Navigation Pane – Network


The following icons are used throughout NetXplorer to represent the elements of the network:


-  Network
-  NetEnforcer or Service Gateway
-  Short Term Monitoring Collector
-  Long Term Monitoring Collector
-  SMP
-  SMP Group
-  Line
-  Pipe
-  Virtual Channel

In the Navigation tree, the  icon is added to a Line, Pipe or Virtual Channel to indicate that it is the fallback element of its type, as applicable. For example,  represents the fallback pipe.


The severity of the most serious alarms directly concerning a system component (or one of its sub elements) is indicated by the addition of a color-coded alarm icon (Information: light grey, Warning: gray; Minor: blue; Major: yellow; Critical: red). For example, , indicates that a major alarm has occurred on the NetEnforcer or Service Gateway.


Accessibility problems are indicated by the addition of an icon in the upper right portion of the device icon. For example, , indicates that the NetEnforcer or Service Gateway is not accessible.

The populated severity of alarms for a system component or one of its sub elements is indicated by the addition of a color-coded alarm icon on the upper left portion of the device icon (Warning: gray; Minor: blue; Major: yellow; Critical: red). For example, , indicates a critical alarm is open for one at least one of the sub elements in the network.

To expand the tree to view the subcomponents of a component, click .

To collapse the tree to hide the subcomponents of a component, click .

To view or edit the name and IP address of a NetEnforcer, select the component in the Navigation tree and click , or select **Properties** from the Action menu, or right-click and select **Properties** from the popup menu.

To view or edit the configuration of a NetEnforcer or Service Gateway, select the NetEnforcer or Service Gateway in the Navigation tree and click , or select **Configuration** from the View menu, or right-click and select **Configuration** from the popup menu.

NOTE **Lines, Pipes and Virtual Channels cannot be added/deleted/changed in the Network Tree. This must be done through the Enforcement Policy editor.**

Adding a NetEnforcer or Service Gateway

In order for NetXplorer to manage a NetEnforcer or Service Gateway, it must be added to the NetXplorer's network and properly configured. The IP address of the NetEnforcer or Service Gateway is required for this procedure.

NOTE **Initial configuration of the NetEnforcer or Service Gateway should be performed on the device (via the CLI interface) before it is added to the NetXplorer configuration. Refer to the hardware manual for the specific model for details.**

To add a NetEnforcer or Service Gateway:

1. In the Navigation pane, right-click Network in the Network of the Navigation tree and select **New NetEnforcer** from the popup menu.

OR

Select Network in the Network pane of the Navigation tree and then select **New NetEnforcer** from the Actions menu.

The NetEnforcer Properties - New dialog is displayed.



Figure 3-3: NetEnforcer Properties – New Dialog

2. Enter the Name, Admin Password and the IP address of the NetEnforcer or Service Gateway in the designated fields.

NOTE: The default admin password is 'allot' in all NetEnforcer and Service Gateways

3. Assign a Monitoring Collector or Collector Group to the NetEnforcer or Service Gateway from the drop down menus. This means that the new NetEnforcer or Service Gateway will transmit its monitoring data to that Collector or Group only. If it does not matter which Collector is used, select **<system defined>**. If you do not have any Monitoring Collectors on the Network, select **No Collector**.
4. Click **OK**. The NetEnforcer or Service Gateway is added to the Navigation tree. The Add NetEnforcer operation can take up to a couple of minutes to complete.

To Import a NetEnforcer or Service Gateway:

1. A NetEnforcer or Service Gateway can be imported into NetXplorer if it already exists on the network but has not previously been part of this NetXplorer network or had NetXplorer enabled. When a NetEnforcer or Service Gateway is imported, its Enforcement Policy tables and catalogs remain intact and are imported into the NetXplorer database.
2. Select **Import NetEnforcer** from the Tools menu.

The NetEnforcer Properties - Import dialog is displayed.



Figure 3-4: NetEnforcer Properties – Import Dialog

3. Enter the Name, Admin Password and IP address of the NetEnforcer or Service Gateway in the designated fields.
4. Enter the name of the NetEnforcer or Service Gateway and its IP address in the designated fields.
5. In the Password field, enter the admin password of the NetEnforcer or Service Gateway

NOTE: **The default admin password is 'allot' in all NetEnforcer and Service Gateways**

6. Assign a Monitoring Collector or Collector Group to the NetEnforcer or Service Gateway from the drop down menus. This means that the new NetEnforcer or Service Gateway will transmit its monitoring data to that Collector or Group only. If it does not matter which Collector is used, select **<system defined>**. If you do not have any Monitoring Collectors on the Network, select **No Collector**.
7. Click **OK**. The NetEnforcer or Service Gateway is added to the Navigation tree. The Import NetEnforcer operation can take up to a couple of minutes to complete.

Configuring a NetEnforcer or Service Gateway

Once you have added a NetEnforcer or Service Gateway to the NetXplorer configuration, you can modify the NetEnforcer or Service Gateway's configuration parameters remotely via NetXplorer.

For information concerning adding NetEnforcers or Service Gateways and other Servers to the network, see the NetXplorer Administration Guide.


To configure a NetEnforcer or Service Gateway:

1. In the Navigation pane, select and right-click the NetEnforcer or Service Gateway in the Navigation tree and select **Configuration** from the popup menu.


OR

Select the NetEnforcer or Service Gateway in the Navigation tree and then select **Configuration** from the View menu.

OR

Select the NetEnforcer or Service Gateway in the Navigation tree and then click the **Configuration** icon  on the toolbar.

The Configuration window for the selected NetEnforcer or Service Gateway is displayed.

2. Configure the NetEnforcer or Service Gateway parameters, as required. For a detailed description of the parameter in each of the NetEnforcer or Service Gateway Configuration tabs, refer to *NetEnforcer or Service Gateway Configuration Parameters*, page 3-7.
3. Click  or select **Save** from the File menu to save the changes to the NetEnforcer or Service Gateway configuration.

NetEnforcer or Service Gateway Configuration Parameters

The parameters available in the NetEnforcer or Service Gateway Configuration window are grouped on the following tabs:

- **General**, page 3-8
- **Identification & Key**, page 3-9
- **SNMP**, page 3-12
- **Security**, page 3-13

- **NIC**, page 3-15
- **Networking**, page 3-17
- **IP Parameters**, page 3-19
- **Date/Time**, page 3-22
- **Service Activation**, page 3-23
- **Slots & Boards**, page 3-24

Each tab includes parameters that can be configured as required. After modifying configuration parameters, you must select **Save** in order for the changes to take effect. The save process prompts a reset of the NetEnforcer or Service Gateway. Resetting is sometimes required to ensure that some saved parameter values are committed and activated on the NetEnforcer or Service Gateway.

NOTE **The Slots and Boards tab will only appear when configuring a NetEnforcer that utilizes blades or a Service Gateway.**

General

The General tab includes parameters that provide system status information.

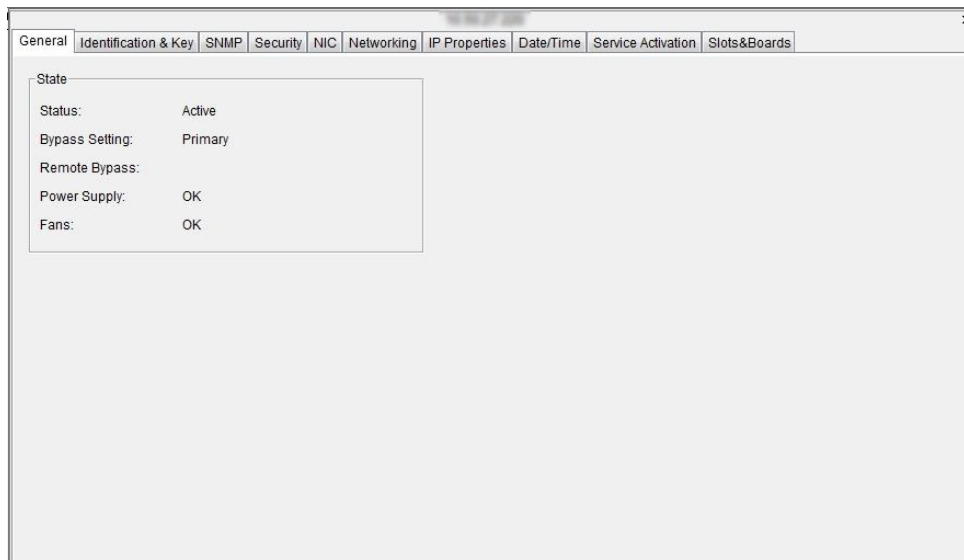


Figure 3-5: Configuration – General Parameters

The General tab includes the following parameters:

PARAMETER	DEFINITION
Status	Indicates whether or not the NetEnforcer or Service Gateway is operating in Bypass mode (Active or Non-bypass).
Bypass Setting	Indicates the current Bypass Setting.
Remote Bypass	If configured for redundancy, the role of the NetEnforcer or Service Gateway in the redundancy configuration. (Not applicable, Primary, or Secondary).
Power Supply	The status of the power supply on the device (OK, Unknown, or Problem).
Fans	The status of the fans on the device (OK, Unknown, or Problem).

Identification & Key

The **Identification & Key** tab includes parameters that provide system information and activate optional NetEnforcer or Service Gateway modules.

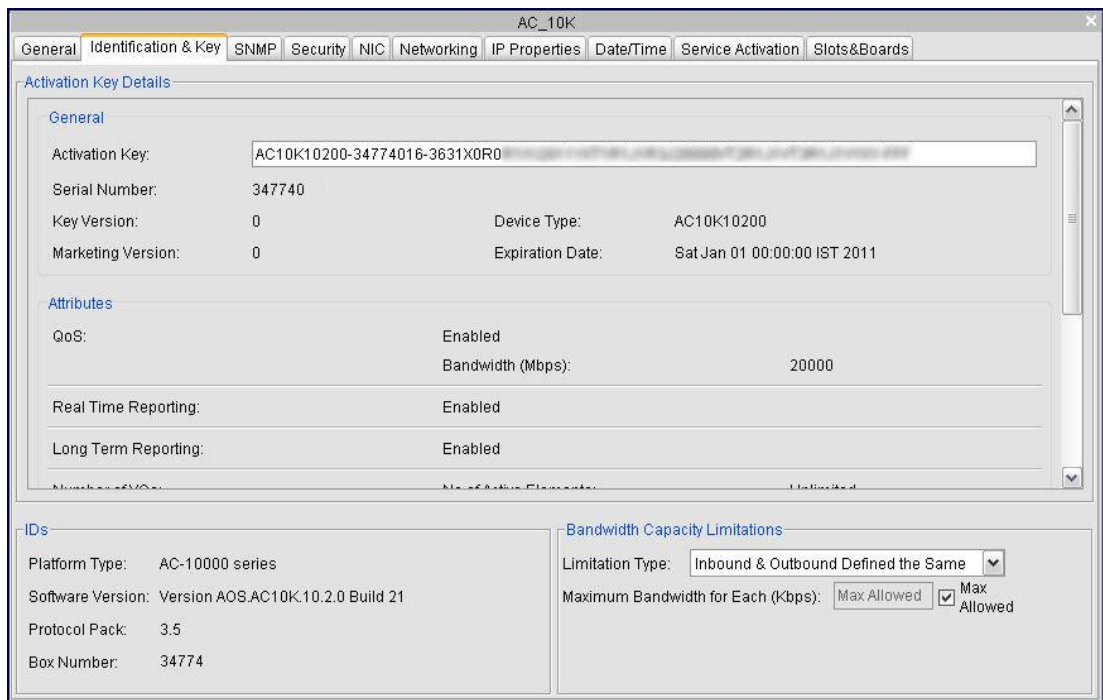


Figure 3-6: Configuration - Identification & Key Parameters

The **Identification & Key** tab includes the following parameters:

PARAMETER	DEFINITION
Activation Key	The activation key enables the NetEnforcer or Service Gateway. Enter the activation key supplied to you at purchase. The functionality enabled by the key is summarized in the fields below the key.
Serial Number	The Serial Number of the NetEnforcer or Service Gateway.
Key Version	For Internal Use Only
Marketing Version	For Internal Use Only
Device Type	The Type of NetEnforcer or Service Gateway.
Expiration Date	The expiration date of the entered Activation Key.
QoS	Quality of Service is enabled/disabled on the NetEnforcer or Service Gateway.
Real Time Reporting	Real Time Reporting is enabled/disabled on the NetEnforcer or Service Gateway. Real Time Reporting requires an appropriate key to be enabled.
Long Term Reporting	Long Term Reporting is enabled/disabled on the NetEnforcer or Service Gateway. Long Term Reporting is enabled by default.
Number of Lines	The maximum number of Lines that may be defined on the NetEnforcer or Service Gateway.
Number of Pipes	The maximum number of Pipes that may be defined on the NetEnforcer or Service Gateway.
Number of VCs	The maximum number of Virtual Channels that may be defined on the NetEnforcer or Service Gateway.
APU	Allot Protocol Update is enabled/disabled on the NetEnforcer or Service Gateway.

PARAMETER	DEFINITION
WebSafe Enforcement	WebSafe is enabled/disabled on the NetEnforcer or Service Gateway, listing the number of Core Controllers covered by the license.
WebSafe Subscription	WebSafe is subscribed to the Internet Watch Foundation blacklist service. This subscription is optional
Traffic Steering	Port or URL Redirection is enabled/disabled on the NetEnforcer or Service Gateway. For further information see Service Activation Catalog on page 4-65. If Enabled, the maximum Bandwidth (Mbps) and No of Subscribers appears.
SP Mitigation	ServiceProtector is enabled/disabled on the NetEnforcer or Service Gateway, listing the number of Core Controllers covered by the license.
MediaSwift – Cache Out	The Cache Out bandwidth of the MediaSwift Service, in Mbps.
Platform Type	The platform series of the NetEnforcer or Service Gateway
Software Version	The software version running on the NetEnforcer or Service Gateway.
Protocol Pack	The Protocol Pack version loaded into the Service Catalog of the NetEnforcer or Service Gateway.
Box Number	The ID number of the NetEnforcer or Service Gateway.
Bandwidth Capacity Limitations – Limitation Type	The way bandwidth limitations are imposed on the NetEnforcer or Service Gateway; Inbound & Outbound Defined Separately, Inbound & Outbound Defined the Same or Half Duplex .
Inbound Bandwidth Limited to:	The incoming bandwidth limitation of the NetEnforcer, in Kbps. Select the Max Allowed checkbox to allow the maximum value to be passed. This feature is available on NetEnforcer AC-400 or AC-800 Series models ONLY.
Outbound Bandwidth Limited to:	The outgoing bandwidth limitation of the NetEnforcer, in Kbps. Select the Max Allowed checkbox to allow the maximum value to be passed. This feature is available on NetEnforcer AC-400 or AC-800 Series models ONLY.

SNMP

The **SNMP** tab includes parameters that enable you to configure SNMP-compatible management functions.

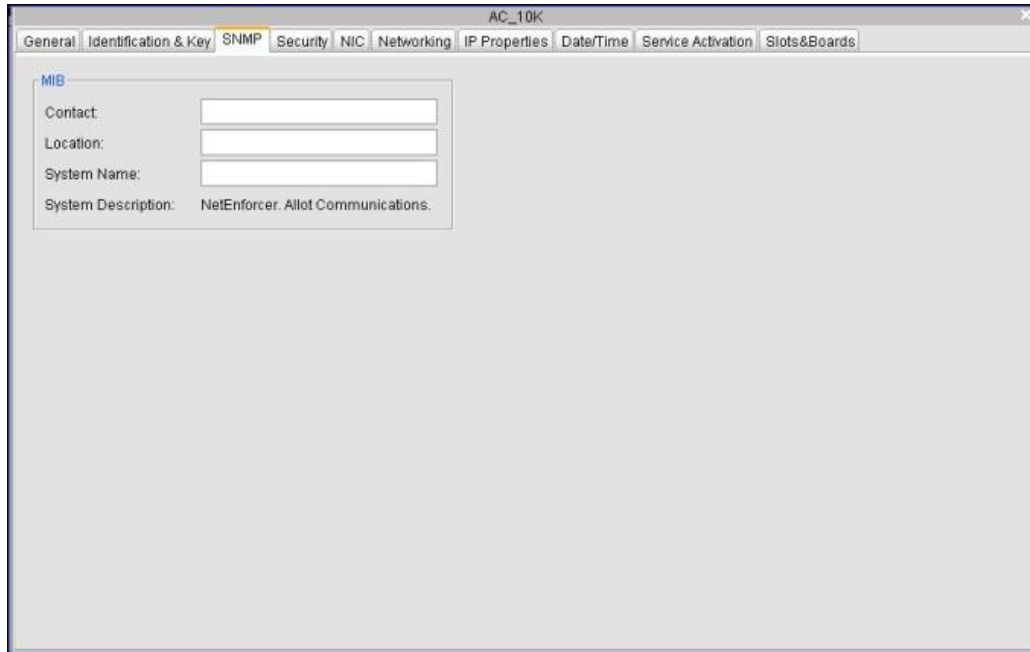


Figure 3-7: Configuration - SNMP Parameters

The Simple Network Management Protocol (SNMP) is a commonly used network management protocol that allows SNMP-compatible management functions such as device discovery, monitoring and event generation. NetEnforcer or Service Gateway support for SNMP includes MIB II with standard MIB II traps.

The **SNMP** tab includes the following parameters:

PARAMETER	DEFINITION
Contact	The contact person, for SNMP purposes.
Location	The location of system, for SNMP purposes.
System Name	The name of the system, for SNMP purposes.
System Description	A description of the system, for SNMP purposes.

Security

The **Security** tab includes parameters that enable you to specify security parameters as well as control access to NetEnforcer or Service Gateway management functions by specifying the names of hosts to whom you want to grant access permission.

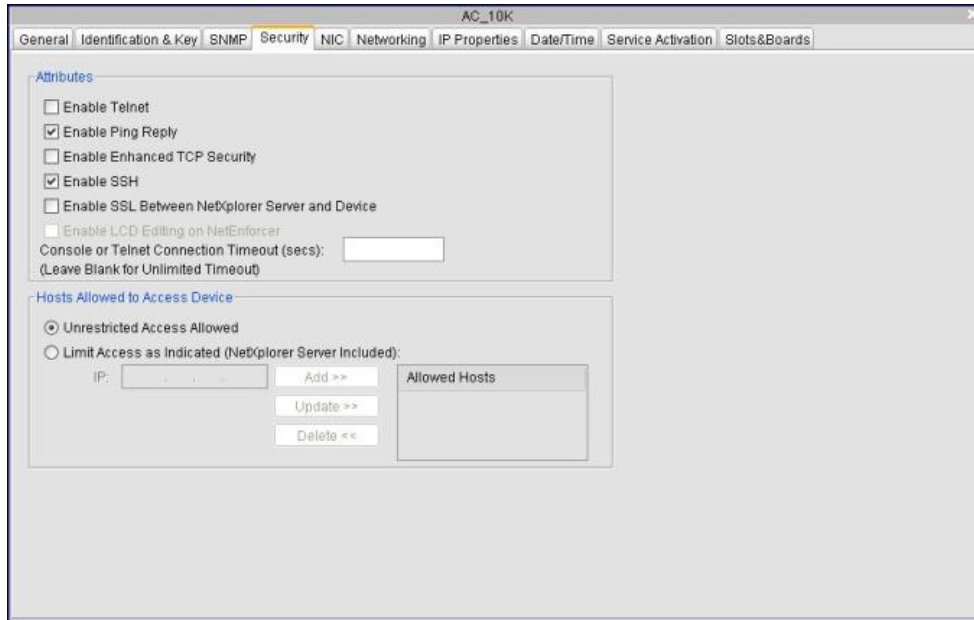


Figure 3-8: Configuration - Security Parameters

The upper section of the **Security** tab includes the following parameters:

PARAMETER	DEFINITION
Enable Telnet	Select this checkbox to enable remote Telnet communications with the NetEnforcer or Service Gateway.
Enable Ping Reply	Select this checkbox to enable remote Ping communications with the NetEnforcer or Service Gateway.
Enable Enhanced TCP Security	Select this checkbox to enable enhanced TCP Security. Enhanced TCP security is used to help prevent attacks in the transport layer.
Enable SSH	Select this checkbox to enable SSH communications. SSH communications are used to help prevent DoS attacks on the NetEnforcer or Service Gateway.

PARAMETER	DEFINITION
Enable SSL Between NetXplorer Server and Device	Select this checkbox to enable SSL communications. SSL communications are used to further secure connections between the NetXplorer Server and each NetEnforcer or Service Gateway. (NOTE: SSL v3.0 and TLS v1.0 are supported)
Enable LCD Editing on NetEnforcer	Enables the configuration of the NetEnforcer from the LCD on the front of the unit. This feature is not available on the AC-1400, AC-3000, AC-5000, AC-10000 and Service Gateway lines.
Console or Telnet Connection Timeout	In seconds, the time lapse after which an idle connection times out. A timeout of 0 (zero) means the connection will remain open indefinitely.

The lower section of the **Security** tab includes a list of hosts who have access permission to NetEnforcer or Service Gateway management functions. When the **Hosts Allowed to Access NetEnforcer** list is empty, there is unrestricted access to the NetEnforcer or Service Gateway management functions. When there are hosts in the **Hosts Allowed to Access NetEnforcer** list, only those hosts are allowed access to the NetEnforcer or Service Gateway management function.

WARNING If no hosts are defined, anyone can access NetEnforcer or Service Gateway management functions.

To add a host to the list, specify the IP address of the host in the designated field and click **Add**. The specified host is added to the **Hosts Allowed to Access NetEnforcer** list.

You can add as many hosts as required.

WARNING If you want to restrict access to a NetEnforcer or Service Gateway, do not forget to enter your own IP address as the first entry. This will ensure that you do not accidentally lock yourself out.

NOTE Regardless of the specific hosts defined, the NetXplorer can always access the NetEnforcer or Service Gateway.

To modify a host, select the host in the **Hosts Allowed to Access NetEnforcer** list to display its details in the IP field. Modify the details as required and click **Update**.

To remove a host, select the host in the **Hosts Allowed to Access NetEnforcer** list to display its details in the IP field and click **Delete**.

NOTE If the host that you selected is the only one in the **Hosts Allowed to Access NetEnforcer** list, a system message is displayed advising you that if you delete this host all hosts will be able to access the NetEnforcer or Service Gateway.

NIC

The **NIC** tab includes parameters that enable you to configure the system interfaces to either automatically sense the direction and speed of traffic, or use a predetermined duplex type and speed.

If you are configuring an Allot Service Gateway a representation of the currently installed blades appears at the top of the tab. Select a blade in the image to see the NICs for that blade.

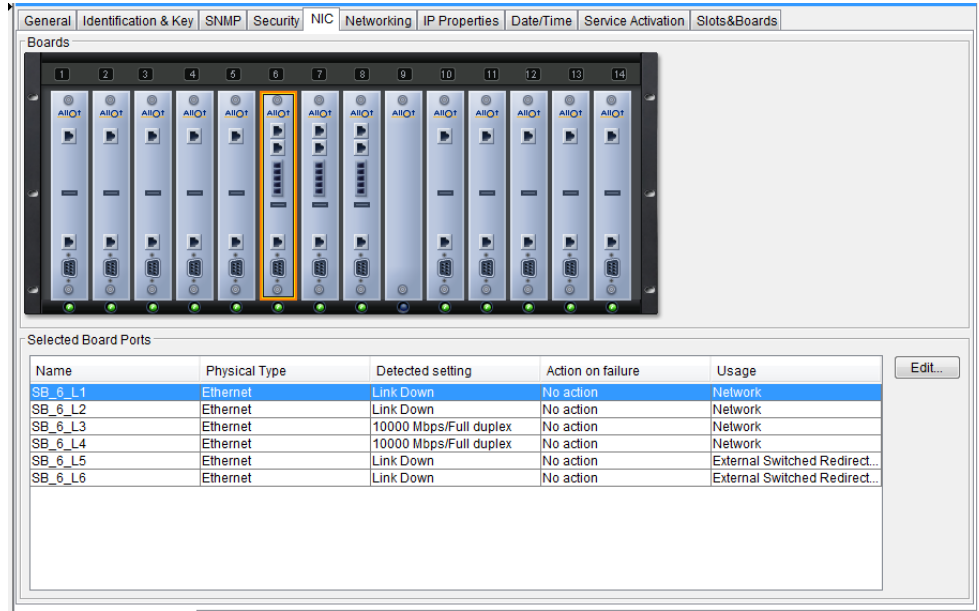


Figure 3-9: Configuration - NIC Parameters

NOTE In units supporting more than one Link, the interfaces are referred to as **INTERNAL <LINK NUMBER>** and **EXTERNAL <LINK NUMBER>**. For example, **INTERNAL2** and **EXTERNAL2**.

The **NIC** tab includes the following parameters for each port. To make changes to any of these parameters, click the field or highlight the device row and click the Edit button:

PARAMETER	DEFINITION
Name	The name of the interface.
Physical Type	The type of port (e.g: Ethernet).

PARAMETER	DEFINITION
Detected Setting	The actual speed detected (Link Down, Auto, 10 Mbps, 100 Mbps, or 1000 Mbps).
Action on Failure	<p>The action to be taken automatically should the NIC fail.</p> <p>Options are:</p> <ul style="list-style-type: none">• No action – No action is taken if the NIC fails.• Fail paired port – If the NIC fails, the system will shut down its counterpart. For instance, if the NIC is an internal NIC, the system will shut down its external counterpart.• Fail all – If the NIC fails, all NICs except for the management port will be shut down.• Bypass device – If a NIC fails, the device is bypassed by traffic.
Usage	The type of traffic handled by the port (Network, Media Swift Storage, External Switched Redirection, Cloned (HA) or Asymmetry).

Networking

The **Networking** tab includes parameters that enable you to configure the network topology.

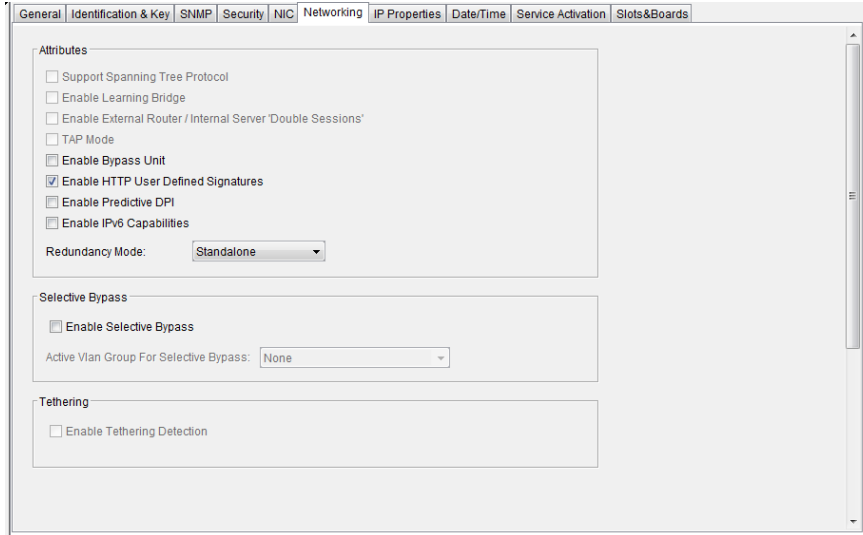


Figure 3-10: Configuration - Networking Parameters

The **Attributes** area of the **Networking** tab includes the following parameters. Not all parameters are available for all devices, and if unavailable will be grayed out:

PARAMETER	DEFINITION
Support Spanning Tree Protocol	Enables the use of a second NetEnforcer or Service Gateway as a backup system in a spanning tree configuration.
Enable Learning Bridge	Enables the use of a learning bridge, which maintains a database of physical addresses.
Enable External Router / Internal Server 'Double Sessions'	Enables Double Sessions, which are when a single connection goes through the NetEnforcer or Service Gateway as both Inbound and Outbound traffic. This usually occurs due to a connection being redirected by an external router.
TAP Mode	Enables TAP mode for Monitoring Only service.
Enable Bypass Unit	Enables the NetEnforcer or Service Gateway to go into bypass mode.

PARAMETER	DEFINITION
Enable HTTP User Defined Signatures	Allows the user to define signatures (UDS) for HTTP content.
Enabled Predictive DPI	For more information concerning Predictive DPI contact Allot Customer Support.
Enable IPv6 Capabilities	Allows IPv6 to be used by the selected device.
Redundancy Mode	<p>Indicates the Redundancy Mode to be used should one NetEnforcer or Service Gateway fail (Standalone, Parallel, Serial or Active).</p> <p>NOTE Different redundancy schemes are supported per Hardware series. For more information about the available redundancy modes, see the appropriate Hardware Guide</p>

The **Selective Bypass** area of the **Networking** tab includes the following parameters. Not all parameters are available for all devices, and if unavailable will be grayed out:

PARAMETER	DEFINITION
Enable Selective Bypass	Enables the use of Selective Bypass. Selective Bypass allows the user to select VLAN Groups that will not be subject to QoS. This requires that you have at least one VLAN Group configured.
Active VLAN Group for Selective Bypass	Defines VLAN Groups that will not be subject to QoS.

The **Tethering** area of the **Networking** tab includes the following parameters. Not all parameters are available for all devices, and if unavailable will be grayed out:

PARAMETER	DEFINITION
Enable Tethering Detection	Enables the identification of those mobile devices that are using tethering capabilities.

IP Properties

The **IP Properties** tab enables you to modify the IP and host name configuration of your network interfaces, as well as the DNS and connection control parameters.

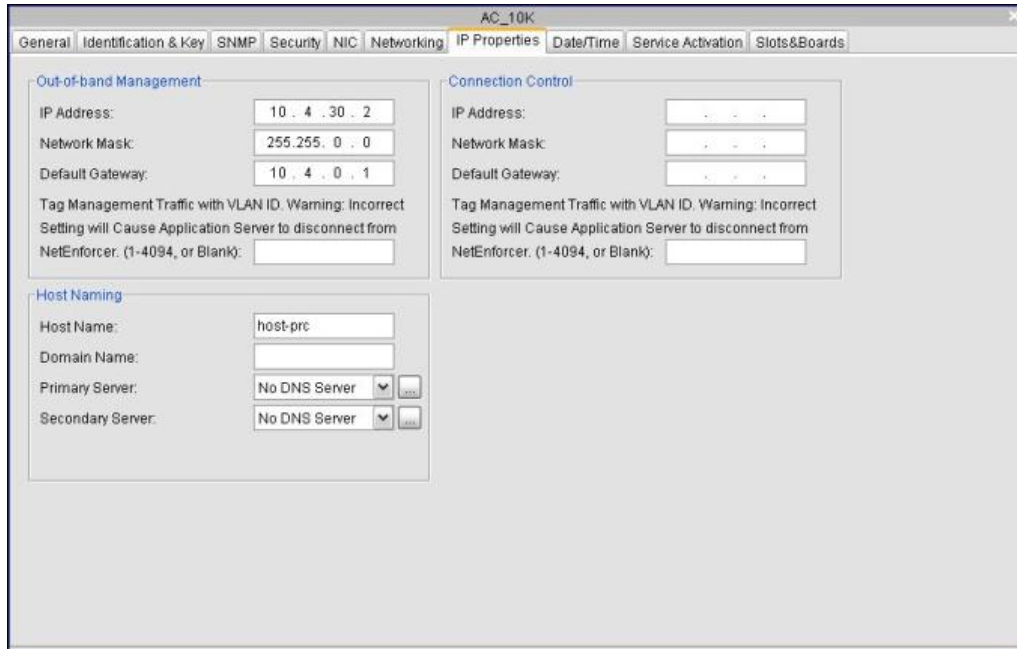


Figure 3-11: Configuration – IP Properties

The **Out-of-Band Management** area of the tab includes the following parameters:

PARAMETER	DEFINITION
IP Address	The IP address of NetEnforcer or Service Gateway.
Network Mask	The network subnet mask.
Default Gateway	The IP address of the default gateway. The default gateway enables clients to access the NetEnforcer or Service Gateway remotely and to provide a path if NetEnforcer or Service Gateway is on a different subnet than that of the client.
Tag Management Traffic with VLAN ID	Configures the NetEnforcer or Service Gateway to be managed based on specified VLAN-tagged traffic. NOTE Once this option is set and the VLAN ID is specified, the NetEnforcer or Service Gateway will be waiting for management traffic tagged with this specified VLAN.

The **Connection Control** area of the tab includes the following parameters:

PARAMETER	DEFINITION
IP Address	The IP address of the NetEnforcer or Service Gateway.
Network Mask	The network subnet mask.
Default Gateway	The IP address of the default gateway. The default gateway enables clients to access the NetEnforcer or Service Gateway remotely and to provide a path if the NetEnforcer or Service Gateway is on a different subnet than that of the client.

PARAMETER	DEFINITION
Tag Management Traffic with VLAN ID	<p>Configures the NetEnforcer or Service Gateway to be managed based on specified VLAN-tagged traffic.</p> <p>NOTE Once this option is set and the VLAN ID is specified, the NetEnforcer or Service Gateway will be waiting for management traffic tagged with this specified VLAN.</p>

The **Host Naming** area of the tab includes the following parameters:

PARAMETER	DEFINITION
Host Name	The host name of the NetEnforcer or Service Gateway.
Domain Name	The domain name.
Primary Server	The IP address of the primary domain name server.
Secondary Server	The IP address of the secondary domain name server.

Date/Time

The **Date/Time** tab includes the date, time and NTP server settings for the NetEnforcer or Service Gateway.

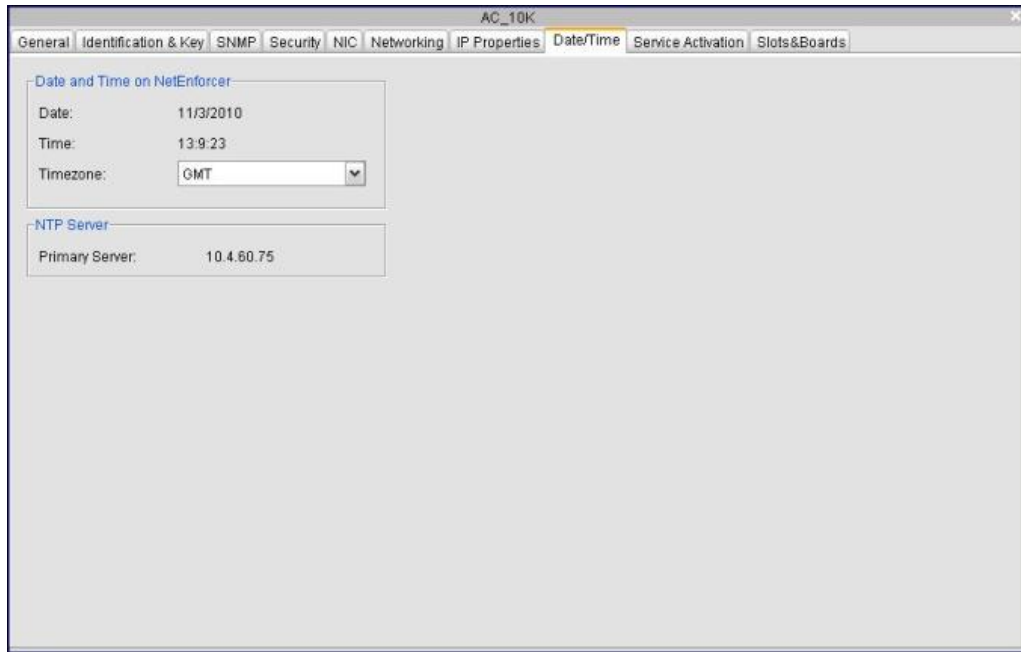


Figure 3-12: Configuration – Date/Time Parameters

The **Date and Time** area of the **Date/Time** tab includes the following parameters:

PARAMETER	DEFINITION
Date	The date set on the NetEnforcer or Service Gateway.
Time	The time set on the NetEnforcer or Service Gateway.
Timezone	The time zone set on the NetEnforcer or Service Gateway.

The **NTP Server** area of the **Date/Time** tab includes the following parameters:

PARAMETER	DEFINITION
Primary Server	The name of the primary NTP (Network Time Protocol) server that the NetEnforcer or Service Gateway receives the date and time from.

Service Activation

The **Service Activation** tab includes IP and Port Redirection Parameters to be defined

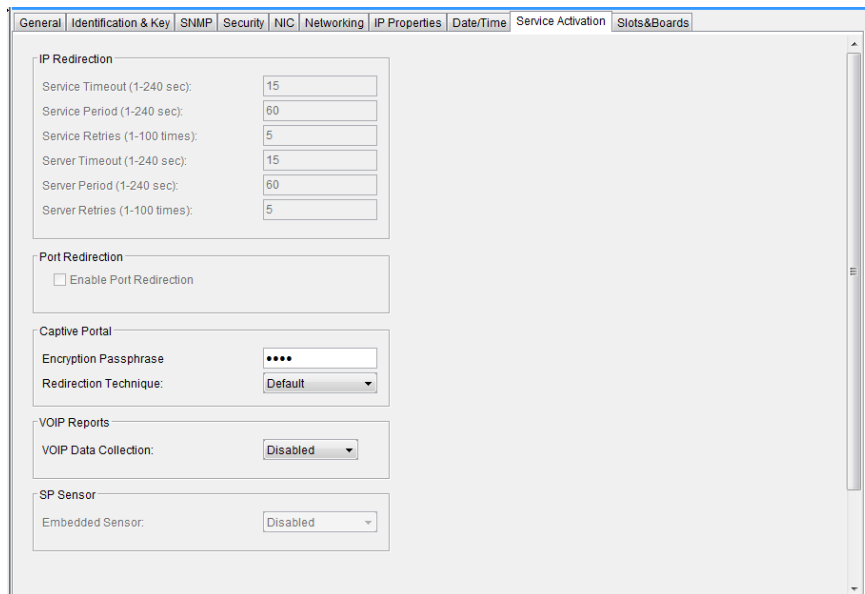


Figure 3-13: Configuration – Service Activation Parameters

The **IP Redirection** area of the **Service Activation** tab includes the following parameters:

PARAMETER	DEFINITION
Service Timeout	The length of time, in seconds, that NetXplorer waits before concluding that the service (for example, HTTP) is down.
Service Period	The length of time, in seconds, that NetXplorer waits between attempts to contact the service.
Service Retries	The number of times NetXplorer tries to connect to the service.

PARAMETER	DEFINITION
Server Timeout	The length of time, in seconds, that NetXplorer waits before concluding that the server is down.
Server Period	The length of time, in seconds, that NetXplorer waits between attempts to contact the server.
Server Retries	The number of times NetXplorer tries to connect to the server.

The **Port Redirection** area of the **Service Activation** tab includes the following parameters:

PARAMETER	DEFINITION
Enable Port Redirection	Enables the Port Redirection feature, which is configured from the Service Activation catalog.

The **Captive Portal** area of the **Service Activation** tab includes the following parameters:

PARAMETER	DEFINITION
Encryption Passphrase	Allows you to enter a passphrase for encrypting communication with the Captive Portal.

PARAMETER	DEFINITION
Redirection Technique	<ul style="list-style-type: none"> • On request – Means that the user is redirected to the predefined portal when the NE/SG sees the HTTP request. • On reply – Means that the NE/SG attempts to learn the potentially asymmetric network environment and thereafter perfectly replicate the packet's encapsulation method. E.g: For asymmetric encapsulation environments such as MPLS, Allot recommends to use “On reply” since the NE/SG will then know which MPLS tag to attach to the packet. • Default – The recommended option in most installations. The NE/SG chooses by itself whether to use “On request” or “On reply” – It identifies per session whether to make an effort to learn each sessions' two sided encapsulations.

The **VoIP Reports** area of the **Service Activation** tab includes the following parameters:

PARAMETER	DEFINITION
VoIP Data Collection	Enables the VoIP Minutes of Use report, see page 7-46.

The **SP Sensor** area of the **Service Activation** tab includes the following parameters:

PARAMETER	DEFINITION
-----------	------------

PARAMETER	DEFINITION
Embedded Sensor	Enables a Core Controller blade to act as a ServiceProtector sensor with the appropriate license key installed. For more information, contact Allot Customer Support..

Slots & Boards

The **Slots and Boards** tab is only available when configuring an Allot Service Gateway or a NetEnforcer running AOS (Allot Operating System).

The tab displays the following information:

PARAMETER	DEFINITION
Boards	Indicates graphically the Boards that are currently loaded into the device.
Common Sensors	Displays any open alarms that pertain to the entire device.
Selected Board Sensors	Displays all sensor readings that pertain to the selected board.

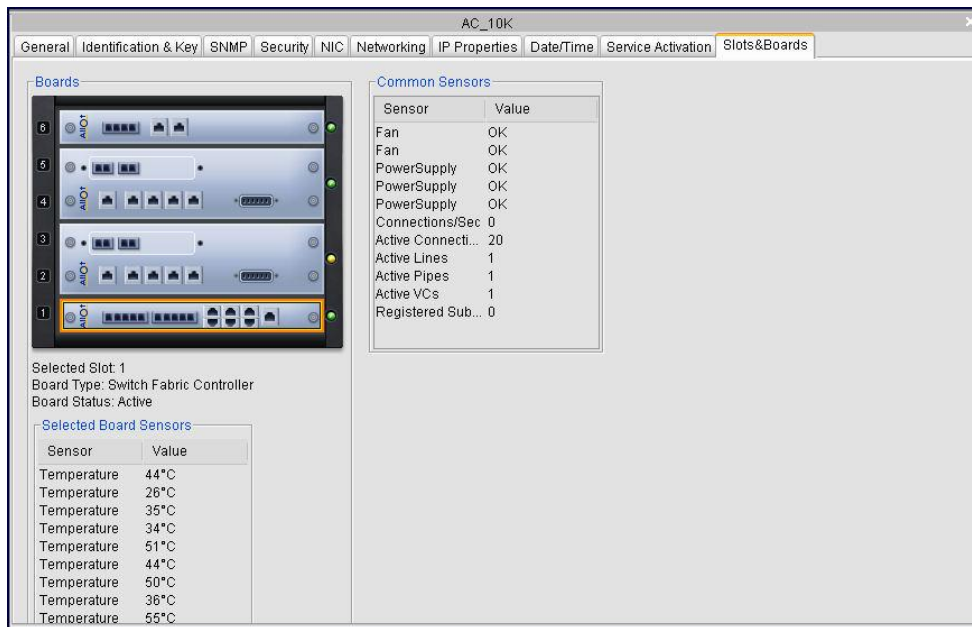


Figure 3-14: Configuration – Slots and Boards – AC-10000

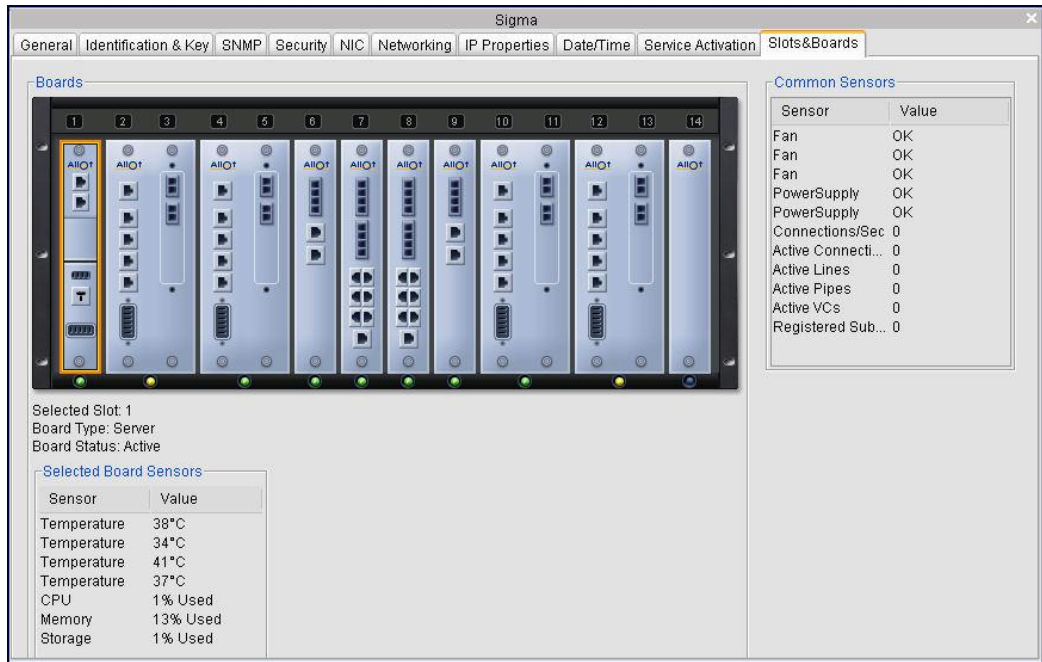


Figure 3-15: Configuration – Slots and Boards – SG-Sigma

Configuring the Network

You can configure the parameters of the SMTP server used to send reports and handle alarm actions. In addition, secure SNMP communications can be configured to include authentication and/or encryption.



To configure the Network:

1. In the Navigation pane, right-click the Network in the Navigation tree and select **Configuration** from the popup menu.

OR

Select the Network in the Navigation tree and then select **Configuration** from the View menu.

OR

Select the Network in the Navigation tree and then click the **Configuration** icon  on the toolbar.
2. Configure the Network parameters in the Network Configuration window, as required.
3. Click  or select **Save** from the File menu to save the changes to the NetEnforcer or Service Gateway configuration.

Network Configuration Parameters

The parameters available in the Network Configuration window are grouped in the following tabs:

- **Servers**, 3-29
- **SNMP**, page 3-30
- **SMP**, page 3-32
- **SMP Domains**, page 3-31
- **Accounting**, page 3-34
- **Protocol Updates**, page 3-35
- **Service Protector**, page 3-36
- **Integrated Service**, page 3-37
- **Net Awareness**, page 3-39

Servers

The Servers tab includes the parameters that enable the SMTP server to send reports and handle alarm actions.

Figure 3-16: Network Configuration – Servers

The Servers tab includes the following parameters:

PARAMETER	DEFINITION
SMTP Server IP Address and Port Address	The IP address and Port of the SMTP server that is used for emailing alarms and reports.
Enable SMTP Server Authentication	Select this box to require the SMTP Server listed in the field above to be authorized. Authorization details are entered in the following fields.
SMTP User Name	The user name defined for the SMTP server.
SMTP Password	The password to be used for the defined SMTP username.
Confirm Password	The password to be used for the defined SMTP username. (When assigning a password, the password is entered again here for confirmation.)

PARAMETER	DEFINITION
'From' Email Address for Dispatched Alarms & Reports	The Email address that will be shown as the source of any notifications of Alarms or Events.
Allowed Hosts	Defines those hosts that will be allowed CLI access to the NX server. (Used for example, to define hosts for server CLI. For more details see NetXplorer Installation and Administration Guide Chapter 6)

SNMP

The **SNMP** tab includes parameters that enable secure communications between NetXplorer and the NetEnforcers or Service Gateways. Secure communications can be configured to include authentication and/or encryption.

Upon saving any changes made in this SNMP panel, all NetEnforcer or Service Gateway SNMP agents **MUST** have the same user name, passphrase for authentication (if relevant), and passphrase for encryption (if relevant) as indicated in the panel. If not, SNMP communications failure will result.

NOTE **SNMP must be enabled on the individual NetEnforcer or Service Gateways as well as on the network.**

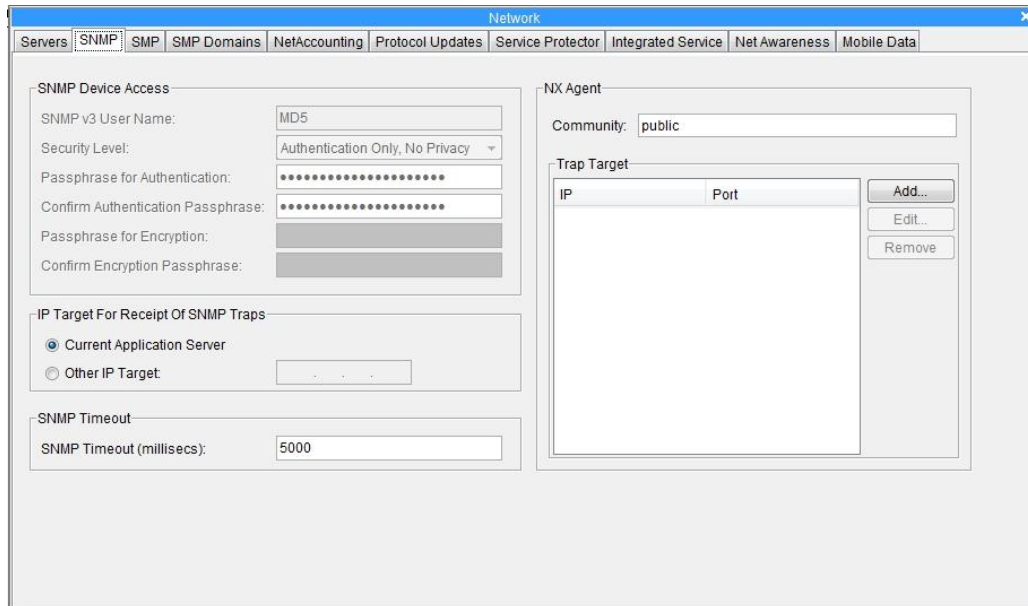


Figure 3-17: Network Configuration – SNMP

The **SNMP** tab includes the following parameters:

PARAMETER	DEFINITION
SNMP v3 User Name	The user name defined for the SNMP Server.
Security Level	The level of security for communications between the NetXplorer and NetEnforcer or Service Gateways: Authentication Only, No Privacy: Implements authentication without requiring encryption. No Authentication, No Privacy: Implements neither authentication nor encryption.
Passphrase for Authentication / Confirm Authentication Passphrase	The passphrase for authentication, entered twice for confirmation purposes. NOTE These parameters are enabled only if the selected security level includes authentication.
Passphrase for Encryption / Confirm Encryption Passphrase	The passphrase for encryption, entered twice for confirmation purposes. NOTE These parameters are enabled only if the selected security level includes encryption (Privacy).
IP Target for Receipt of SNMP Traps	The Application Server where SNMP traps are to be sent. The current server can be selected or the IP address of another server can be entered.
SNMP Timeout	The SNMP timeout may be entered, in milliseconds.
NX Agent	This field lists any NMS units that the NetXplorer will send specific external traps to, as selected in Event Types Configuration (see page 6-2). To add an NMS, click the Add button and enter the IP address and target port. These values may be changed using the Edit button.

WARNING Upon saving any changes made in the **SNMP** panel, all **NetEnforcer** or **Service Gateway SNMP** agents **MUST** have the same user name, passphrase for authentication (if relevant), and passphrase for encryption (if relevant) as indicated in the panel. If not, **SNMP** communications failure will result. For information on how to set the **SNMP** on the **NetEnforcer** or **Service Gateway**, contact **Allot Customer Support** at support@allot.com.

SMP

The **SMP** tab allows the definition of SMP IP Domains, Service Plans and Server Parameters, for use with the Allot Subscriber Management Platform. You can also define Session parameters and billing information from the SMP tab. For further information see the SMP User Guide.

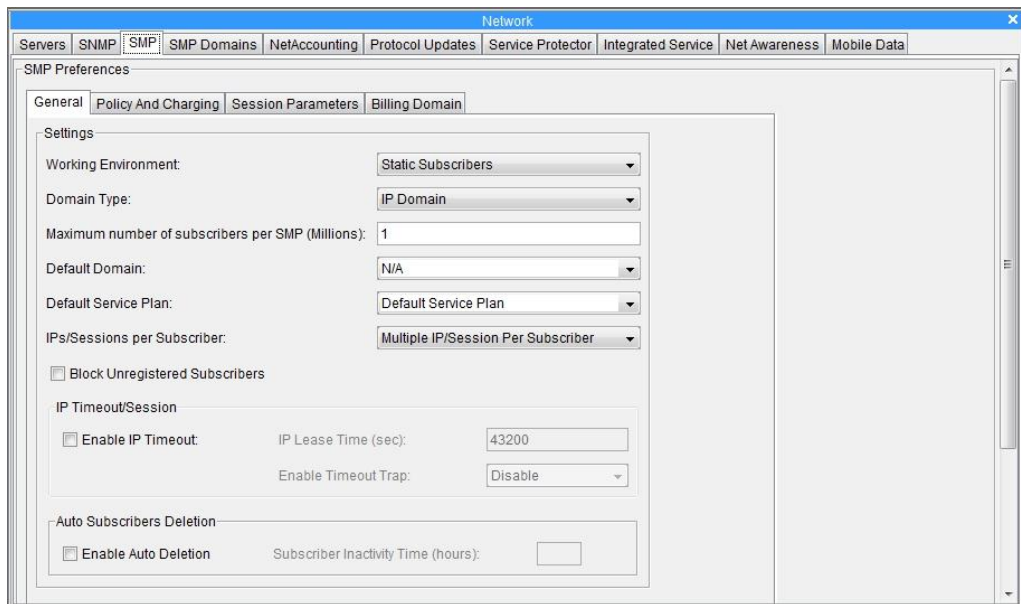


Figure 3-18: Network Configuration - SMP tab

NOTE This feature is only available with the appropriate key.

SMP Domains

The **SMP Domains** tab allows the definition of SMP IP Domains and SMP Subscriber Domains, for use with the Allot Subscriber Management Platform. For further information see the SMP User Guide.

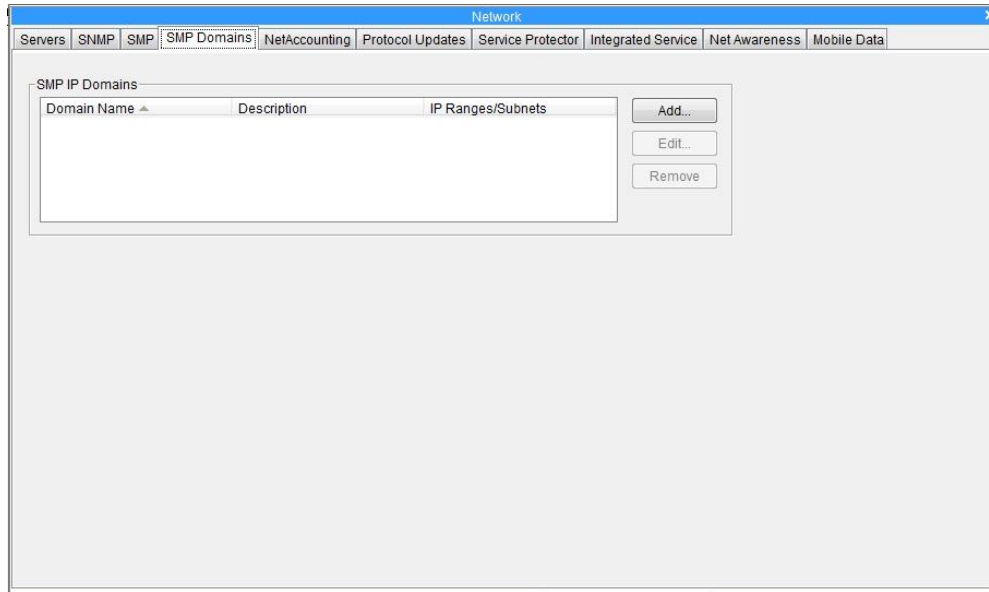


Figure 3-19: Network Configuration - SMP Domains tab

NOTE This feature is only available with the appropriate key.

NetAccounting

The NetAccounting tab has parameters for enabling and configuring NetXplorer’s centralized accounting management system. NetAccounting collects and consolidates data from multiple NetEnforcer or Service Gateway devices to enable users to produce consolidated reports.

NetAccounting records contain the following information:

- Subscriber ID
- Service (i.e. HTTP, P2P, etc.)
- Bytes In
- Bytes Out

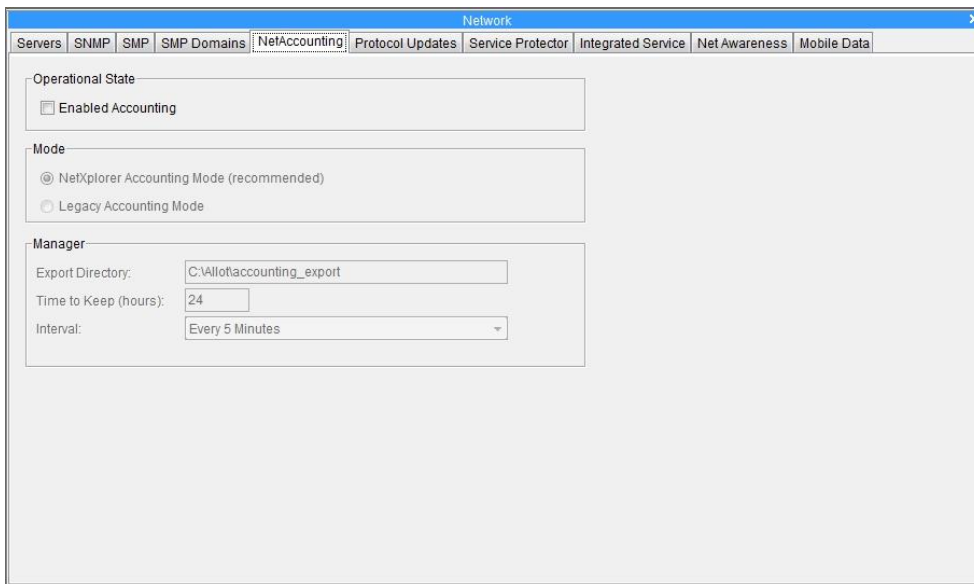


Figure 3-20: Network Configuration - Accounting tab

NOTE This feature is only available with the appropriate key.

The **Accounting** tab includes the following parameters:

PARAMETER	DEFINITION
Enabled Accounting	Enables Accounting if the correct key has been entered for the NetXplorer Server and the Accounting software has been installed.
NetXplorer Accounting Mode	Activates the NetXplorer Accounting Mode.

PARAMETER	DEFINITION
Legacy Accounting Mode	Activates the NetEnforcer Accounting Mode. For more information concerning Legacy Accounting see the appropriate NetEnforcer Hardware Guide for your device(s).
Export Directory	Defines the location of the Export Directory, where the processed files containing the collected Accounting information are located.
Time to Keep	The time period (in hours) that the Accounting Manager holds the processed information (24 hour default).
Interval	Defines the time interval that the SMP accumulates the raw Accounting data before transferring it to the Accounting Manager for processing (Every 5 minutes is the default).

Protocol Updates

The **Protocol Updates** tab includes parameters that select how often the Protocol Update feature checks to see if a new Protocol Pack is available for the Service Catalog of the NetXplorer and how those updates are handled.

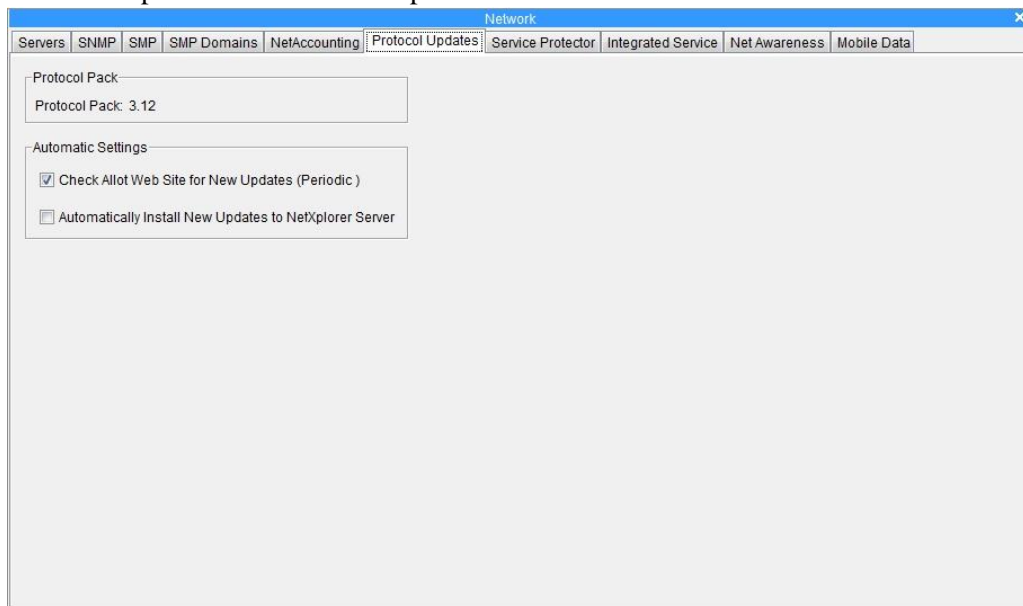


Figure 3-21: Network Configuration – Protocol Updates tab

NOTE This feature is only available with the appropriate key.

PARAMETER	DEFINITION
Protocol Pack	The number of the Protocol Pack currently installed on the NetXplorer Server.
Check Allot Web Site for New Updates (Periodic)	Defines how often the Allot Web Site is checked for new updates.
Automatically Install New Updates to NetXplorer Server	Enables NetXplorer to automatically install and new Updates onto the Server (but not individual NetEnforcer or Service Gateways).

Service Protector

The **Service Protector** tab allows a ServiceProtector unit to be defined for the Network. Enter the IP, User Name and Password of the desired ServiceProtector.

Once a valid Service Protector has been entered in the Service protector tab, the GUI for that device can be opened from the Tools menu by selecting **Open ServiceProtector**.

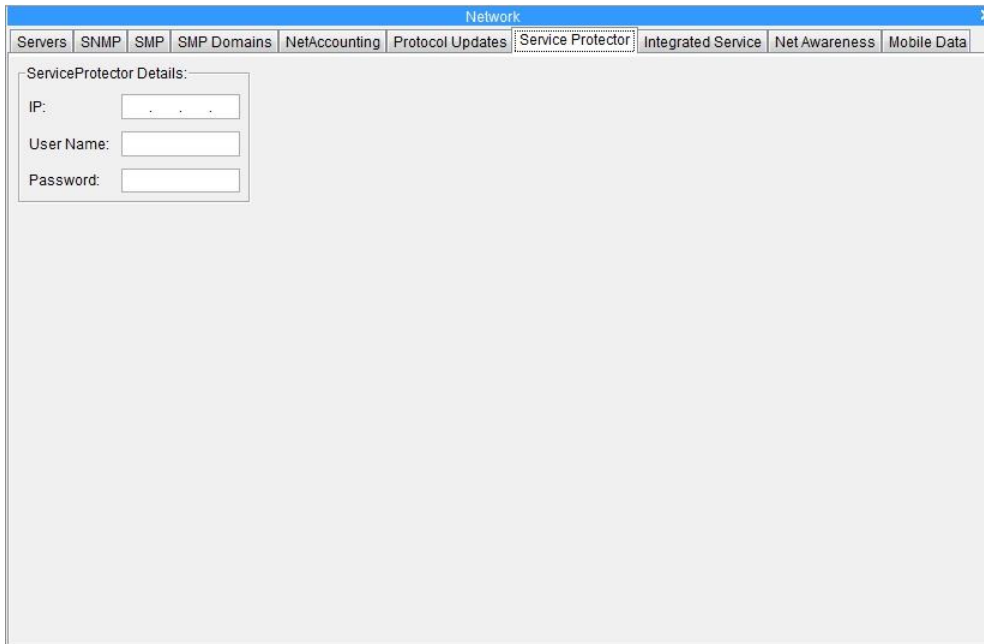


Figure 3-22: Network Configuration – Service Protector tab

Integrated Service

The **Integrated Service** tab has parameters for enabling and configuring two services: WebSafe and HTTP Monitoring. Both WebSafe and HTTP Monitoring are only available on devices running AOS software.

NOTES **WebSafe is only available with the appropriate key.**

Both WebSafe and HTTP Monitoring are only available on NetEnforcers or Service Gateways running AOS (Allot Operating System).

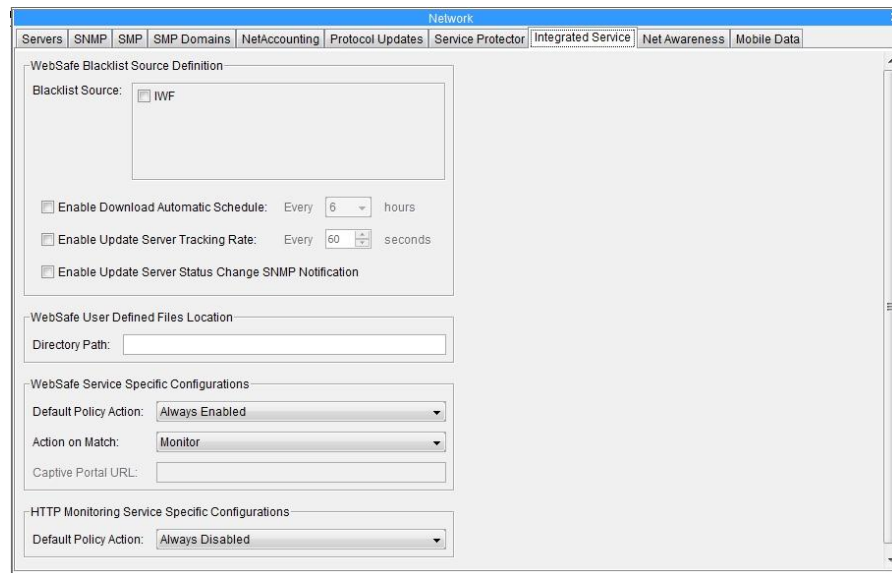


Figure 3-23: Network Configuration – Integrated Service tab

The **Integrated Service** tab includes the following parameters:

NOTE **In order for the entire tab to be displayed, please close the Logs Pane at the bottom of the GUI.**

PARAMETER	DEFINITION
WebSafe Blacklist Source Definition	<p>Manages available external sources for blacklists. Some of these sources may require additional subscriptions.</p> <ul style="list-style-type: none"> • Blacklist Sources: Select the checkboxes of available Blacklists you wish to enable. If you have purchased the license for a particular blacklist, checking this blacklist source will enable your NetXplorer to download this regularly updated list from Allot. • Enable Download Automatic Schedule: Select the checkbox if you wish the available blacklists to be updated on a specific schedule. Use the drop down menu to select how often they should be updated. • Enable Update Server Tracking Rate: Select the checkbox to enable NetXplorer to regularly confirm that the update server is available. Use the drop-down menu to select how often the NetXplorer attempts to contact the update server. • Enable Update Server Status Change SNMP Notification: Select this checkbox to enable NetXplorer to send a notification should the update server be unavailable.
WebSafe User Defined Files Location	<p>Defines the location of three user created files:</p> <ul style="list-style-type: none"> • Black lists (operator_bl.url) • White lists (operator_wl.url) • Warning Page (warning.html) – the HTML file displayed when a user is blocked or redirected.

PARAMETER	DEFINITION
WebSafe Service Specific Configurations	<p>Defines the behavior of WebSafe.</p> <ul style="list-style-type: none"> • Default Enforcement Policy Action: Sets the default behavior (Always Enabled, Always Disabled, Enforcement Policy Based) of WebSafe. <p>Always Enabled: This service applies to all traffic running through the NetEnforcer or Service Gateway</p> <p>Always Disabled: This service is currently not applied to any traffic running through the NetEnforcer or Service Gateway</p> <p>Enforcement Policy Based: This service will only be applied to Lines, Pipes or VCs for which the service has been activated in the Enforcement Policy</p> <ul style="list-style-type: none"> • Action on Match: Defines what WebSafe does when a URL is found on the Blacklist (Monitor only, Block (drops the session), Block and send subscriber a warning page, Block and redirect to a captive portal). • Captive Portal URL: Sets the location of the Captive Portal.
HTTP Monitoring Service Specific Configurations	<p>Defines the default behavior (Always Enabled, Always Disabled, Enforcement Policy Based) of HTTP Monitoring.</p> <ul style="list-style-type: none"> • Always Enabled: This service applies to all traffic running through the NetEnforcer or Service Gateway • Always Disabled: This service is currently not applied to any traffic running through the NetEnforcer or Service Gateway • Enforcement Policy Based: This service will only be applied to Lines, Pipes or VCs for which the service has been activated in the Enforcement Policy. <p>The data collected by HTTP Monitoring can be seen in the HTTP Report (see page 7-41)</p>

WebSafe

If a user requests a forbidden page, WebSafe processes the request and extracts the URL. The URL is then matched to the blacklist (which may be user defined, or downloaded from a third party source such as the Internet Watch Forum, IWF). If the URL is found on the blacklist AND is not on the whitelist, WebSafe performs an action (for example, to block access to this URL and send a warning page).

The black list, white list and warning page together make up the Operation Files. If an **NX-WS-IWF** license is purchased, and the IWF blacklist source is chosen from the integrated service tab, the WebSafe Operation Files will be downloaded to the following default directory on the NetXplorer server (which will be created the first time the files are downloaded): **\Allot\netxplorer\jboss-5.1.0.GA\server\allot\webSafe**. You can change the location from the **WebSafe User Defined Files Location** field in the Integrated Service tab.

To manually update the blacklist:

1. Write a text file including the URLs of those websites you wish to block, following the format below



```
www.badsite.com
http://otherbadsite.com
www.morebadsite.net/1/movie1.html
http://mybad.com:80/myBadDir/
http://www.badsite.com:8080
http://www.verybadsite.com:80/index.html
```

Figure 3-24: WebSafe Blacklist/Whitelist Format

NOTE Any legal URLs are acceptable (there should be no white spaces within paths). WebSafe considers **www.badsite.com** and **badsite.com** to be different sites. The URL entered may be with or without the **http://** prefix. URL paths (after domain name) may include anything. **HTTPS and FTP sites are not currently supported.**

2. Save the text file as **operator_bl.url**.
3. Create a new folder on the NX server (e.g: **C:\Allot\netxplorer\jboss-5.1.0.GA\server\allot\webSafe**) and enter the path to this folder in the **directory path** field on the integrated service tab
4. Upload the blacklist file to the specified location

5. The NX Server then securely distributes this file to the Allot NetEnforcer and Service Gateway units automatically.

To manually update the whitelist:

1. Write a text file including the URLs of those websites you wish to always allow, following the format in Figure 3-24.

NOTE Any legal URLs are acceptable (there should be no white spaces within paths). WebSafe considers `www.badsite.com` and `badsite.com` to be different sites. The URL entered may be with or without the `http://` prefix. URL paths (after domain name) may include anything. HTTPS and FTP sites are not currently supported.

2. Save the text file as `operator_wl.url`.
3. Upload the blacklist file to the location which you designated in the **directory path** field on the integrated service tab
4. The NX Server then securely distributes this file to the Allot NetEnforcer and Service Gateway units automatically.

Alternatively, if the appropriate license has been purchased, white and blacklists lists can be updated automatically. WebSafe integrates with an external blacklist resource (such as the IWF). The device license enables regular updates from the NetXplorer Server and the NetXplorer then securely distributes the file to the Allot NetEnforcer or Service Gateway units.

In addition to the automatic process which is defined in the Integrated Service tab and determines how often black list and white list files are downloaded from an external server (where relevant) and distributed to the NetEnforcer or Service Gateway devices, the operator can also distribute the files manually at any fixed moment in time by choosing Tools > Websafe > Distribute Operator Files. When working with an SG-Sigma, the operator files will be distributed to each Core Controller blade.

The Blacklist source definition enables the operator to define an external blacklist source, and then to determine how often to download the list and how to track the server availability.

NOTE The `operator_bl.url` & `operator_wl.url` that you create on the NetXplorer will appear without the “.url” suffix. Do not add the “.url” suffix twice to the files twice.

To create a warning page:

The option to **Block and send warning page** refers to the **warning page** located on the NetXplorer server.

1. Write an HTML file including the text you wish to appear when a user tries to access a site on the blacklist.

NOTE **Warning.html must be less than 900 bytes. Any HTML syntax may be used (e.g: reference to scripts, images).**

2. Save the HTML file as **warning.html**.
3. Upload the warning page to the folder which you defined in the directory path field on the integrated service tab (e.g:
C:\Allot\netxplorer\jboss-5.1.0.GA\server\allot\webSafe)

NOTE **If you add a new warning.html file to the NetXplorer this will replace the default Allot warning file with no option to revert to the default warning page.**

4. The NX Server then securely distributes this file to the Allot NetEnforcer and Service Gateway units automatically.

Net Awareness

The **Net Awareness** tab allows SMP users to assign alternate Service Plans for when their mobile networks indicate congestion. This feature is for users in SMP deployments who have purchased a CellWise License. Net Awareness is only available on devices running AOS software. For further information see the Appendix F in the SMP User Guide.

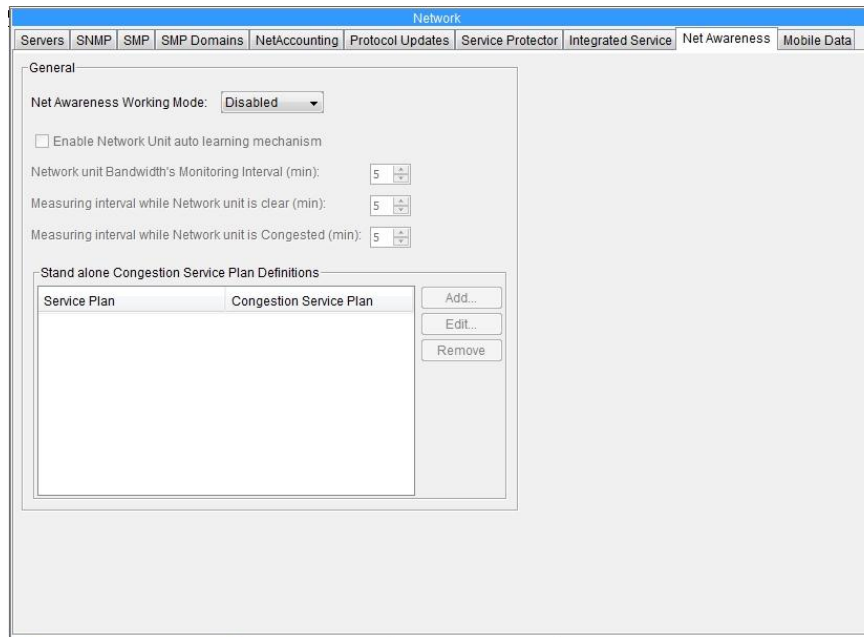


Figure 3-25: Network Configuration – Net Awareness tab

NOTE **This feature is only available with the appropriate key and on NetEnforcers or Service Gateways running AOS (Allot Operating System).**

Mobile Data

The **Mobile Data** tab allows users with a Mobile Analytics license to configure their SGSN list as well as to enable and define data export parameters. This feature requires the SMP and a license that enables Mobile Analytics

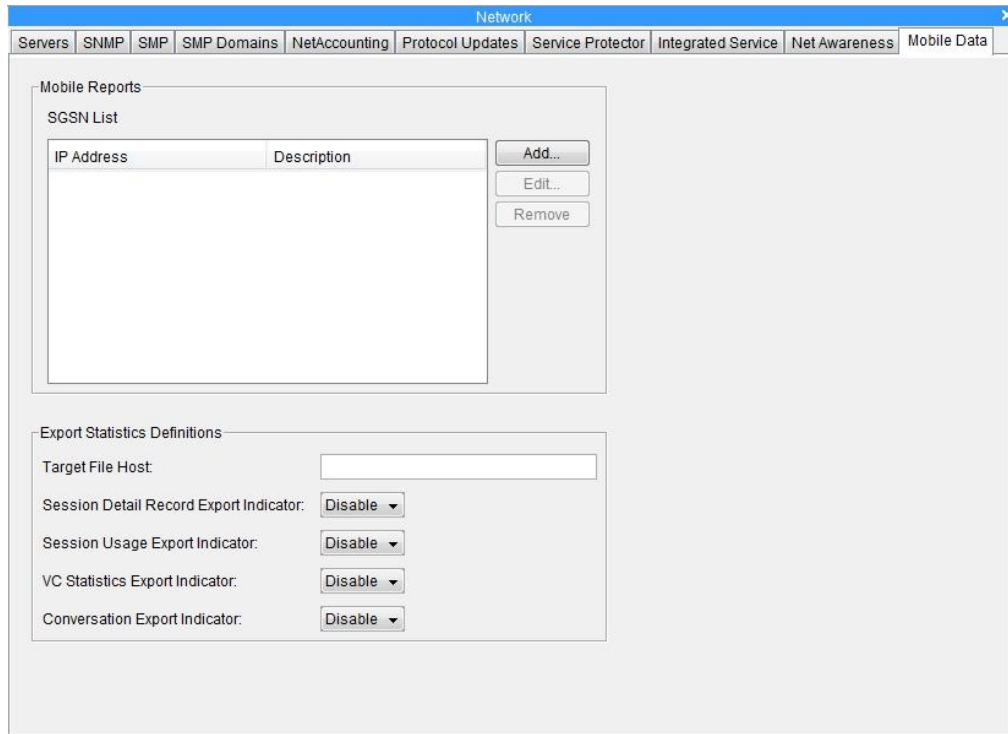


Figure 3-26: Network Configuration – Mobile Data tab

NOTE This feature is only available with the appropriate key and on NetEnforcers or Service Gateways running AOS (Allot Operating System).

Asymmetrical Traffic

NOTE Asymmetrical Traffic is only available on NetEnforcers or Service Gateways running AOS (Allot Operating System) software.

In some network topologies the traffic flows of a single connection can take different paths in the upstream and the downstream directions. This can lead to a situation where one Service Gateway or NetEnforcer on the network sees one flow of the connection while another Service Gateway or NetEnforcer that is located remotely sees the complementary flow of the same connection. Since the DPI should inspect both flows of the connection for maximum accuracy, this leads to a poor identification of the applications running in the network.

Asymmetric Traffic is designed to significantly increase DPI accuracy by allowing Service Gateway or NetEnforcer devices to share information concerning connections. This will ensure that two different flows may be identified as part of the same connection, even when their traffic is handled by different Service Gateways or NetEnforcers. Ideally, using Asymmetric Traffic should provide the same percentage of DPI accuracy with remotely located devices as is found when a single device sees both sides of the connection.

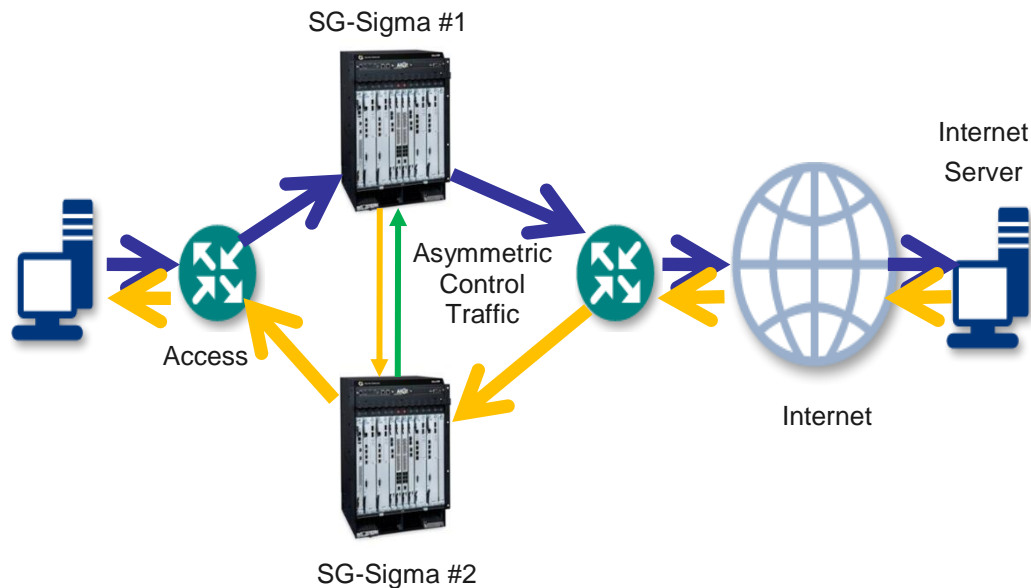


Figure 3-27: Asymmetry Network Diagram

Guidelines

Asymmetric Traffic information is synched between all NetEnforcers or Service Gateways that belong to the same Asymmetric Device Group (ADG) which is configured via NetXplorer. All NetEnforcers or Service Gateways in an ADG must be assigned to the same NetXplorer installation and each NetXplorer may support up to eight ADGs.

An ADG can include co-located devices (e.g. SG1 & SG2, SG3 & SG4) and remotely located devices (devices in POP1 and devices in POP2). Co-located devices are connected with intra-site asymmetric control link. This link passes control information between the co-located devices to sync the DPI information while remotely located devices are connected over an L2/L3 network.

Each ADG may be configured with up to eight devices and has a group ID of 0 through 7. Each device configured to an ADG has a local ID of 0 through 7. Therefore a Service Gateway or NetEnforcer may have a local ID of 1 in ADG 0.

Asymmetric Configuration

The following steps must be taken in order to configure Asymmetric Traffic.

To define an Asymmetric Device Group (ADG):

1. Right click on the Network in the Navigation pane and select **Asymmetry Configuration**.

OR

Highlight the Network in the Navigation pane and select **Asymmetry Configuration** from the View menu.

The Asymmetry Configuration dialog appears.

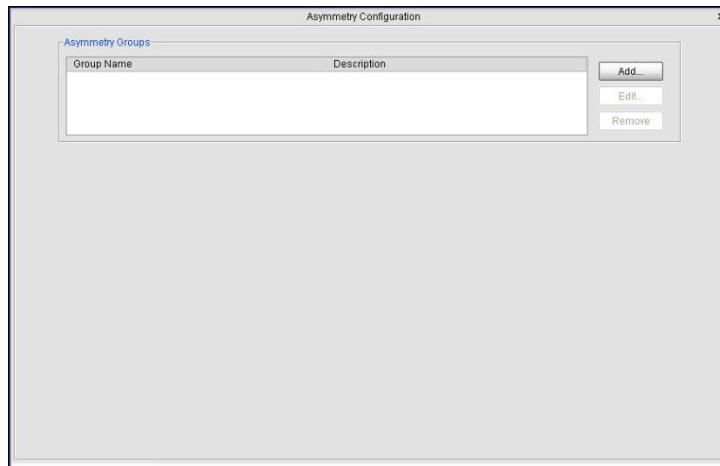


Figure 3-28: Asymmetry Configuration dialog

2. In the Asymmetry Groups field you see any ADGs currently configured on the NetXplorer. Select an ADG and click **Edit** to alter the configuration, or add/remove devices from an existing ADG.
3. To create a new ADG, click **Add**.

The Asymmetry Group – New dialog appears.

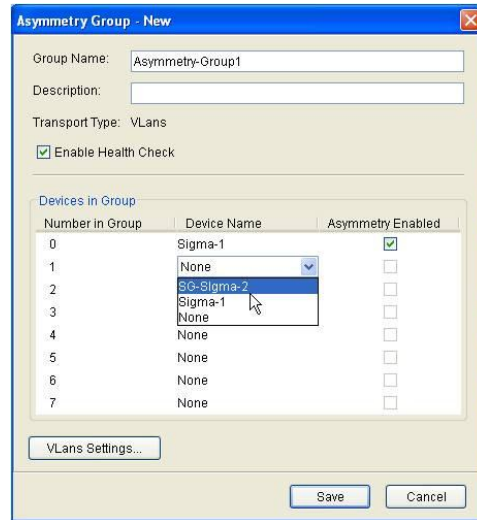


Figure 3-29: Asymmetry Group - New dialog

4. Enter a **Group Name** and **Description** in the appropriate fields.
5. Select the **Enable Health Check** checkbox if you wish NetXplorer to automatically confirm the health of all devices in the ADG.
6. Select the devices to add to the group from the drop down menus. An ADG may include up to eight devices. The Device ID will be established based on the order you place them in inside the ADG. For example, if the Sigma 1 selected as Number in Group 0 will have a Device ID of 0 for the purposes of Asymmetry.
7. Select the **Asymmetry Enabled** checkbox for each device.
8. Click the **VLans Settings** button to edit the VLAN configuration.

The Vlan Settings dialog appears.

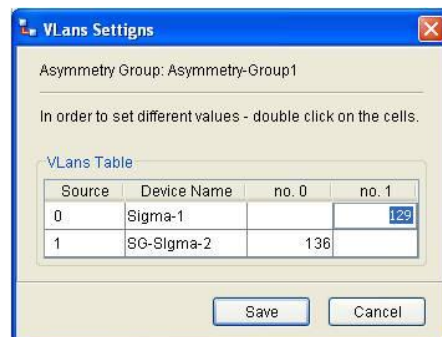


Figure 3-30: VLans Settings dialog

9. A VLAN must be set for each connection between any two devices in the group. Each direction must have a VLAN to be used for Asymmetric control messages (however the same number can be used for both directions)
10. Double click in a field to enter a new VLAN number.
11. Click **Save** to save the information and return to the Asymmetry Group – New dialog.
12. Click **Save** to save the new ADG.

Chapter 4: Defining Catalog Entries

Working with Catalogs

Catalogs contain the values available when defining policies in the Enforcement Policy Editor. For example, when selecting the **Internal** condition of a Pipe, Virtual Channel or Filter, the possible values are the entries in the Host Catalog. You can add, change or delete entries in Catalogs. Entries are comprehensive sets of parameters with logical names. These logical names then become the possible values available in the Enforcement Policy Editor.

A Catalog Entity, such as a specific host or Quality of Service definition, can be defined once in the appropriate Catalog, and then used many times in the Enforcement Policy Editor.

Catalog entries are defined for the entire system and are distributed to all devices in the system. Any changes to the catalog are applied globally throughout the system. Host catalog entries are the only entries that can be defined for specific devices as Private Host entries. These Private Host entries are only distributed to that specific device.

Catalog entries can be managed only by users assigned Regular or Administrator permissions.

NetXplorer includes the following Catalogs:

- **Host Catalog:** The entries in the Host Catalog are the possible values for the **Internal** and **External** conditions defined for a Pipe, Virtual Channel and Filter. The Internal and External define the source and destination of the traffic. Refer to *Host Catalog*, page 4-5.
- **Service Catalog:** The entries in the Service Catalog are the possible values for the **Service** condition defined for a Pipe, Virtual Channel and Filter. The Service represents the protocols relevant to a connection. Refer to *Service Catalog*, page 4-17.
- **Time Catalog:** The entries in the Time Catalog are the possible values for the **Time** condition defined for a Pipe, Virtual Channel and Filter. The Time defines the applicability of a Pipe, Virtual Channel or Filter during certain time periods. Refer to *Time Catalog*, page 4-42.
- **ToS Catalog:** The entries in the ToS Catalog are the possible values for the **ToS** condition defined for a Pipe, Virtual Channel and Filter. The ToS is the ToS byte contained in the IP header of the packet. ToS entries are also used in QoS Catalog entry definitions. In addition, ToS is available as an Action in the Enforcement Policy. Refer to *Type of Service Catalog*, page 4-45.

- **Encapsulation Catalog:** The entries in the Encapsulation Catalog are the possible **GREs** and **VLAN ID** and the User Priority. Refer to *Encapsulation Catalog*, page 4-47.
- **QoS Catalog:** The entries in the QoS Catalog are the possible values for the **Quality of Service** action defined for a Line, Pipe and Virtual Channel. The Quality of Service allocates bandwidth and traffic priority. Refer to *Quality of Service Catalog*, page 4-51.
- **Service Activation Catalog:** The entries in the Service Activation Catalog define values for integrated services and enable you to create service chains. They are only relevant if you have Traffic Steering enabled. Refer to Service Activation Catalog on page 4-65.
- **DoS Catalog:** The entries in the DoS Catalog enable you to control the number of connections and the rate of connections established per Enforcement Policy. Refer to *DoS Catalog*, page 4-65.
- **Quota Catalog:** The entries in the Quota Catalog define Quota Management parameters. These are only relevant if you have Subscriber Management enabled. Refer to *Quota Catalog* on page 4-80.
- **Service Plan Catalog:** The entries in the Service Plan Catalog define Service Plans which may be assigned to individual subscribers. These are only relevant if you have Subscriber Management enabled. Refer to *Service Plan Catalog* on page 4-83.
- **Interface Catalog:** The entries in the Interface Catalog define individual physical ports or groups of ports which may be assigned to policies. Refer to *Interface Catalog* on page 4-91.
- **Charging Application Catalog:** The entries in the Charging Application Catalog define applications and groups of applications for the purpose of assigning them to charging plans. These are only relevant if you have Subscriber Management enabled. Refer to *Charging Application Catalog* on page 4-93.
- **Charging Plan Catalog:** The entries in the Charging Plan Catalog define Charging Plans to be used by service providers. These are only relevant if you have Subscriber Management enabled. Refer to *Charging Plan Catalog* on page 4-95.
- **Mobile Device Catalog:** The Mobile Device Catalog allows you to load and access a Mobile Device Database for use with the Mobile Analytics Feature. This is only relevant if you have both Subscriber Management and Mobile Analytics enabled. Refer to *Mobile Device Catalog* on page 4-98.

Each Catalog has its own editor where you can add new entries and modify existing entries.


Catalog Icons

The following icons are used throughout NetXplorer to represent the different types of catalogs:

	Host		Encapsulation
	Service		Quality of Service
	Time		DoS
	ToS		Quota
	Service Activation		Service Plan
	Interface		Charging Apps
	Charging Plans		Mobile Device

Accessing Catalogs

Catalogs can be accessed in the following ways:

- By selecting the Catalogs tab in the Navigation pane and selecting the required catalog from the list displayed in the Navigation pane.
- By clicking  on the toolbar and selecting the required catalog from the dropdown menu.

All Catalogs have some common fields and functionality, which are described in this section. A sample Catalog is shown below:

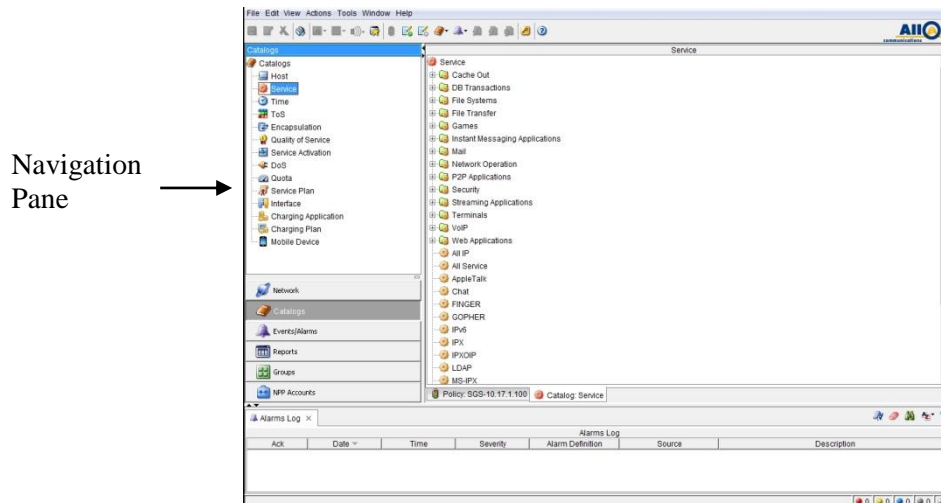


Figure 4-1: Sample Catalog

The Navigation pane displays a list of the current entries defined in the Catalog. Selecting an entry in the Navigation pane displays the associated catalog entries in the Application Details pane.

Buttons relevant to the active Catalog appear in the Quick Access Toolbar in the upper right hand corner of the NetXplorer GUI.

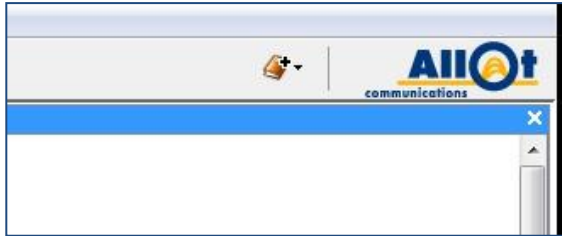


Figure 4-2: Quick Access Toolbar – Catalog Editor

Deleting Entries from a Catalog

You can delete unnecessary entries from a catalog.

NOTE **Catalog entries that are referenced in a Enforcement Policy definition cannot be deleted from a Catalog. In addition, certain reserved entries also cannot be deleted.**

To delete an entry from a Catalog:

1. Select and right-click the catalog entry in the Application Details pane and select **Delete** from the popup menu.

OR

Select the catalog entry in the Application Details pane and then select **Delete** from the Edit menu.

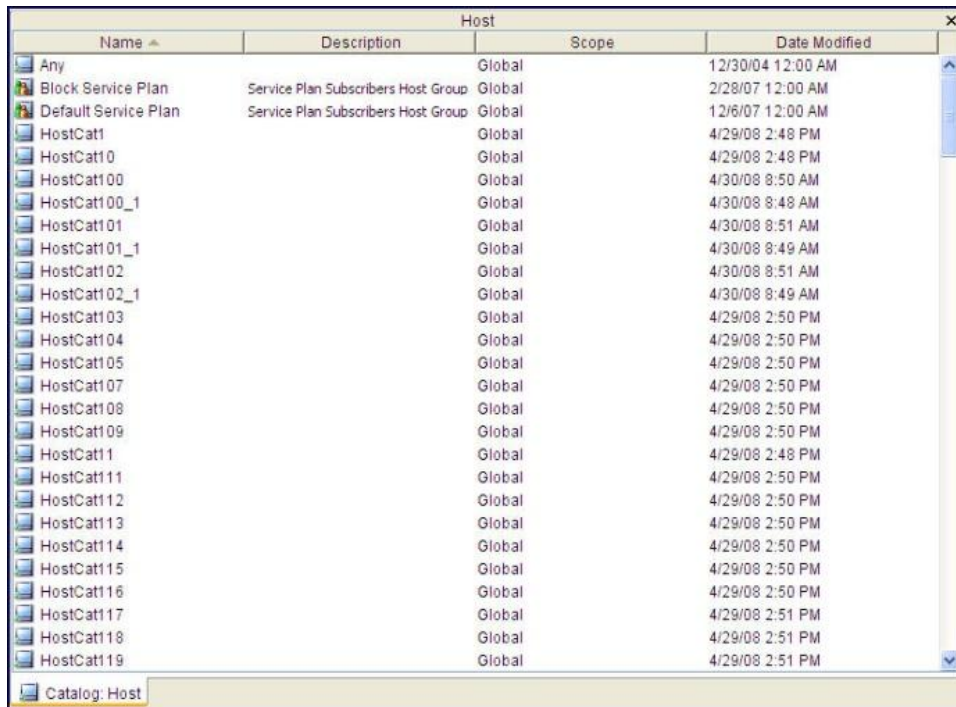
A confirmation message is displayed.
2. Click **Yes** to confirm the deletion. The entry is no longer displayed in the Application Details pane.

Host Catalog

The Host Catalog contains entries that are the possible values for the Internal and External conditions of a Line, Pipe, Virtual Channel or Filter.

A Host Catalog entry's scope can be defined for the entire system or for a specific device.

A sample Host Catalog is shown below:



Name	Description	Scope	Date Modified
Any		Global	12/30/04 12:00 AM
Block Service Plan	Service Plan Subscribers Host Group	Global	2/28/07 12:00 AM
Default Service Plan	Service Plan Subscribers Host Group	Global	12/6/07 12:00 AM
HostCat1		Global	4/29/08 2:48 PM
HostCat10		Global	4/29/08 2:48 PM
HostCat100		Global	4/30/08 8:50 AM
HostCat100_1		Global	4/30/08 8:48 AM
HostCat101		Global	4/30/08 8:51 AM
HostCat101_1		Global	4/30/08 8:49 AM
HostCat102		Global	4/30/08 8:51 AM
HostCat102_1		Global	4/30/08 8:49 AM
HostCat103		Global	4/29/08 2:50 PM
HostCat104		Global	4/29/08 2:50 PM
HostCat105		Global	4/29/08 2:50 PM
HostCat107		Global	4/29/08 2:50 PM
HostCat108		Global	4/29/08 2:50 PM
HostCat109		Global	4/29/08 2:50 PM
HostCat11		Global	4/29/08 2:48 PM
HostCat111		Global	4/29/08 2:50 PM
HostCat112		Global	4/29/08 2:50 PM
HostCat113		Global	4/29/08 2:50 PM
HostCat114		Global	4/29/08 2:50 PM
HostCat115		Global	4/29/08 2:50 PM
HostCat116		Global	4/29/08 2:50 PM
HostCat117		Global	4/29/08 2:51 PM
HostCat118		Global	4/29/08 2:51 PM
HostCat119		Global	4/29/08 2:51 PM

Figure 4-3: Host Catalog

NOTE The Any entry is protected, meaning the definitions for this entry cannot be modified.

Once you have defined the hosts in a host list, you can group several host lists together in one Catalog entry called **Host Group**.

Defining Host Lists

A host list is a list of one or more hosts.

Hosts can be network IP addresses, IP address ranges, host names and IP subnet addresses. Following are examples of host entries:

- **Host Name:** If NetXplorer is configured to support DNS, you can use logical DNS names. Only supported on NetEnforcer AC-400 and AC-800 units.

- **IP Address:** The IP address of a host. For example, 172.16.1.31.
- **IP Subnet:** For example, 10.10.10.0 with a subnet mask of 255.255.255.0.
- **IP Range:** A range of IP addresses. For example, 10.1.2.3-10.1.3.7 means the ranges 10.1.2.3-10.1.2.255 and 10.1.3.1-10.1.3.7.
- **MAC Address:** The MAC address of a host. Only supported on NetEnforcer AC-400 and AC-800 units.

It is possible to import large groups of hosts from an external text file. The user updates this text file and the NetXplorer checks for changes every 10 minutes.

NOTE **The default value of 10 minutes can be changed. Contact Allot Customer Support to enable this change.**

Types of Host Lists

There are 3 different methods for importing external text files. The user can create:

- A new external text file host list
- A new external text file host group
- A new dynamic external text file host group

The dynamic external text file host group functionality was developed to help customers who wish regularly to use particularly large text files containing tens of thousands of entries.

With the regular external text file host group we can only support a few thousand hosts, but the Dynamic version enables us to support many more.

There are however, several restrictions when using the dynamic mechanism:

- It can only be used to support internal hosts.
- It is not supported in the NetEnforcer AC-400 and AC-800 series.
- It only supports individual IPs (ranges and subnets will be ignored)

Note that another side effect of the dynamic system is that the IPs updated with the Dynamic text file are deleted when the NetEnforcer or Service Gateway reboots. The NetXplorer server will update the IPs again after approximately 10 minutes, but until then there will be no rule matching to the pipes and VCs in the Enforcement Policy that use those text files in their conditions.

TYPE OF EXTERNAL TEXT FILE	LIST OR GROUP	NUMBER OF ENTRIES	SUPPORTED ENTRIES	SUPPORTED PRODUCTS	TYPES OF HOSTS
External text file host list	List	Several thousand only	Address	All products	Internal

TYPE OF EXTERNAL TEXT FILE	LIST OR GROUP	NUMBER OF ENTRIES	SUPPORTED ENTRIES	SUPPORTED PRODUCTS	TYPES OF HOSTS
External text file host group	Group		Subnet Range Name		External
Dynamic external text file host group	Group	<p>100,000 for the AC-1000 series</p> <p>160,000 for the AC-1400, AC-2500, AC-3000 series</p> <p>400,000 for the AC-5000 series, the AC-10040 and the AC-10100</p> <p>800,000 for the AC-10200</p> <p>1,600,000 for the SG-Sigma (fully populated)</p>	Address	All Products Except AC-400/AC-800	Internal

To define a host list:

1. Select and right-click **Hosts** in the Navigation pane and select **New Host List** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New Host List** from the popup menu.

The Host List Entry Properties dialog is displayed.

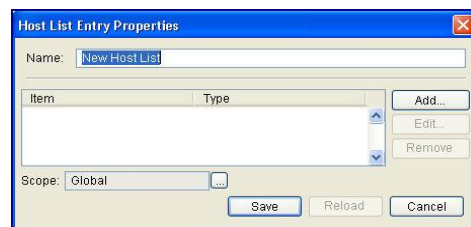


Figure 4-4: Host List Entry Properties – New Host List

2. Enter the name of the host entry in the **Name** field.
3. Click **Add** to add items to the Host List. The Add Host Item dialog is displayed.

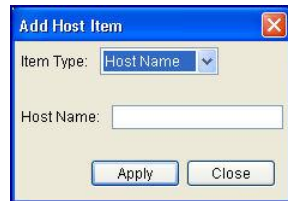


Figure 4-5: Add Host Item

4. From the **Item Type** dropdown list, select the type of item to be included in the host list (Host Name, IP Address, IP Subnet, IP Range, or MAC Address).
5. Define the additional parameters in the dialog. The parameters change according to the selected Item Type. For example, if you are configuring the IP Address, the one additional parameter is defined in the dialog - the IP Address; if you are configuring the IP Range, two parameters are defined – the From and To IP addresses.
6. Click **Apply**. The item is added to the Host List.
7. Click **Close** to return to the Host Properties dialog.
8. To set the scope of the entry to a specific device, click the **Scope** browse button.

The Entry Scope Properties dialog is displayed.



Figure 4-6: Entry Scope Properties

NOTE Scope can only be disabled when defining a new host entry. After saving a new Host Entry the scope field is inaccessible.

9. To make the entry available for all devices, select **Global** (the default).

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

10. Click **OK**. The Host Entry Properties dialog is redisplayed.

- In the Host Entry Properties dialog, click **Save** to save the entry.

NOTE The list of entries in the Hosts List can be sorted by clicking on any column header. For example, click **Type** to sort the list according to item type.

- To edit a Host List entry, select the entry in the Host Entry Properties dialog and click **Edit**. Edit the properties in the Edit Host Item dialog and click **Save**.
- To delete a Host List entry, select the entry in the Host Entry Properties dialog and click **Remove**.

To import an external host list:

- Select and right-click **Hosts** in the Navigation pane and select **New External Text File Host List** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New External Text File Host List** from the popup menu.

OR

Select **Hosts** in the Navigation Pane select **New External Text File Host List** from the Actions menu.

The External Text File Host List Entry Properties dialog is displayed.

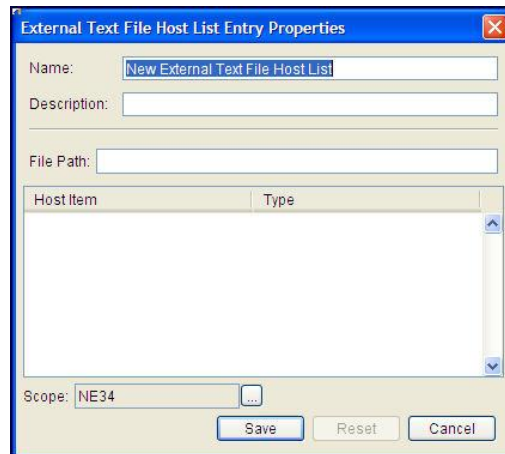


Figure 4-7: External Text File Host List Entry Properties

- Edit the name of the group in the **Name** field, if required.
- Enter a description of the Host Group in the appropriate field.

4. Enter the full file path of the external file. The file can be located only on the local machine.
5. To set the scope of the entry, click the **Scope** browse button. The Entry Scope Properties dialog is displayed.

To make the entry available for all devices, select **Global**.

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

6. Click **OK**. The External File Host List Entry Properties dialog is redisplayed.
7. In the External File Host List Entry Properties dialog, click **Save** to save the entry.

The file is automatically checked for any changes every five minutes by the NetXplorer. The file will only be uploaded again by the NetXplorer if a change is detected.

Grouping Hosts

A Host Group is a collection of previously defined Host Catalog entries of **Host List** type grouped together in an additional entry. This eliminates the need to create several similar Pipes, Virtual Channels or Conditions for hosts. For example, you can create a group of hosts, called Division 1. Division 1 can contain three Host List catalog entries: Department A (employees a, b and c), Department B (employees d, e and f) and Department C (employees g, h and j).

Host Groups may be created from previously defined Host Catalog entries, or imported as a text file.

To group Host Catalog entries:

1. Select and right-click **Hosts** in the Navigation pane and select **New Host Group** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New Host Group** from the popup menu.

The Host Group Entry Properties dialog is displayed.

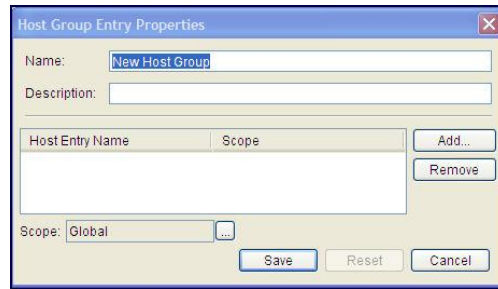


Figure 4-8: Host Group Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. Click **Add** to add items to the Host List. The Add Group Items dialog is displayed.

The Add Group Items dialog lists all available Host List catalog entries that can be added to the host group.

4. Select one or more entries and click **OK** to add them to the Host Group. The Host Group Entry Properties dialog is redisplayed.

To set the scope of the entry to a specific device, click the **Scope** browse button. The Entry Scope Properties dialog is displayed.

To make the entry available for all devices, select **Global**.

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

5. Click **OK**. The Host Group Entry Properties dialog is redisplayed.
6. In the Host Group Entry Properties dialog, click **Save** to save the entry.

To import a Host Group from an external text file:

1. Select and right-click **Hosts** in the Navigation pane and select **New External Text File Host Group** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New External Text File Host Group** from the popup menu.

OR

Select Hosts in the Navigation Pane select **New External Text File Host Group** from the Actions menu.

The External File Host Group Entry Properties dialog is displayed.

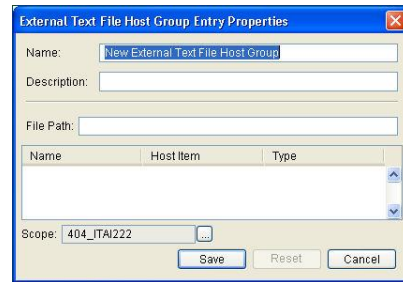


Figure 4-9: External Text File Host Group Entry Properties

2. Edit the name of the list in the **Name** field, if required.
3. Enter a description of the list in the appropriate field.
4. Enter the full file path of the external file. The file can be located on any machine that the NetXplorer Server can access.
5. To set the scope of the entry, click the **Scope** browse button. The Entry Scope Properties dialog is displayed.

To make the entry available for all devices, select **Global**.

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

6. Click **OK**. The External Text File Host Group Entry Properties dialog is redisplayed.
7. In the External Text File Host Group Entry Properties dialog, click **Save** to save the entry.

The file is automatically checked every five minutes for any changes by the NetXplorer. The file will only be uploaded again by the NetXplorer if a change is detected.

To import a Host Group from a dynamic external text file:

A Dynamic Host Group is recommended for very large Host Groups, in order to improve system performance.

1. Select and right-click **Hosts** in the Navigation pane and select **New Dynamic External Text File Host Group** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New Dynamic External Text File Host Group** from the popup menu.

OR

Select Hosts in the Navigation Pane select **New Dynamic External Text File Host Group** from the Actions menu.

The External File Host Group Entry Properties dialog is displayed.

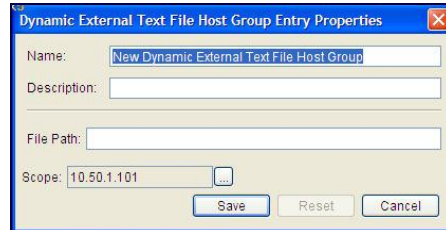


Figure 4-10: Dynamic External Text File Host Group Entry Properties

2. Edit the name of the list in the **Name** field, if required.
3. Enter a description of the list in the appropriate field.
4. Enter the full file path of the dynamic external file. The file can be located on any machine that the NetXplorer Server can access.
5. To set the scope of the entry, click the **Scope** browse button. The Entry Scope Properties dialog is displayed.

To make the entry available for all devices, select **Global**.

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

6. Click **OK**. The Dynamic External Text File Host Group Entry Properties dialog is redisplayed.
7. In the Dynamic External Text File Host Group Entry Properties dialog, click **Save** to save the entry.

The file is automatically checked for any changes every five minutes by the NetXplorer. The file will only be uploaded again by the NetXplorer if a change is detected.

Creating a Host Text File

There are four types of hosts that can be created using the external data source feature: IPaddr, IPrange, IPsubnet and hostnames.

Create a file according to the guidelines defined below:

NOTE This method creates individual hosts with corresponding names but they are all added to a single group. They cannot be separated.

- **Delimiter:** semicolon
- **Text File Format:**
Name:Type
<hostlist name>;1.1.1.1 → an IPaddr host
<hostlist name>;1.1.1.0/255.255.255.0 → an IPsubnet host
<hostlist name>;5.5.5.5-6.6.6.6 → an IPrange host
<hostlist name>;XXXXXXXXXXXXX → a Hostname Host

Creating a Host Group Text File

- Text File Format

```
HL1;1.1.1.1  
HL1;1.1.1.2  
HL1;1.1.1.3  
HL2;1.1.2.1  
HL2;1.1.2.2  
HL2;1.1.2.3
```

Once added to the NetXplorer, the Host-Group outlined above will be created with two Host-Lists - HL1 and HL2.

Each of the Host-Lists shown above is defined with 3 IP addresses.

Subscriber Host Groups

To define a subscriber host group:

1. Select and right-click **Hosts** in the Navigation pane and select **New Subscriber Host Group** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New Subscriber Host Group** from the popup menu.

The Subscriber Host Group Entry Properties dialog is displayed.

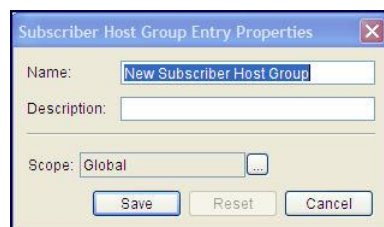


Figure 4-11: Subscriber Host Group Entry Properties

2. Edit the name of the group in the **Name** field, if required.
3. Enter a description of the Subscriber Host Group in the appropriate field.
4. To set the scope of the entry, click the **Scope** browse button. The Entry Scope Properties dialog is displayed.

To make the entry available for all devices, select **Global**.

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

5. Click **OK**. The Subscriber Host Group Entry Properties dialog is redisplayed.
6. In the Subscriber Host Group Entry Properties dialog, click **Save** to save the entry.

Country Classification

To define a country classification:

1. Select and right-click **Hosts** in the Navigation pane and select **New Country Classification** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **New Country Classification** from the popup menu.

The Country Classification Entry Properties dialog is displayed.

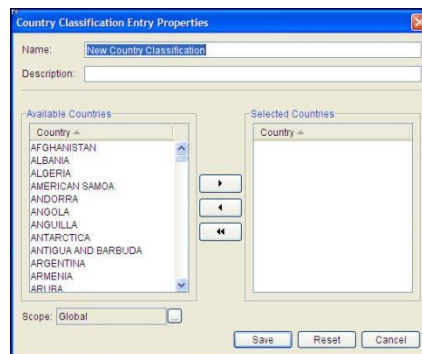


Figure 4-12: Country Classification Entry Properties

2. Edit the name of the group in the **Name** field, if required.

3. Enter a description of the Country Classification in the appropriate field.
4. Use the arrow keys to select the countries that will be included in the new classification entry, moving countries from the **Available Countries** list to the **Selected Countries** list.
5. To set the scope of the entry, click the **Scope** browse button. The Entry Scope Properties dialog is displayed.

To make the entry available for all devices, select **Global**.

OR

To make the entry available to a selected device only, select **Specific Device** and then select the device from the dropdown list.

6. Click **OK**. The Country Classification Entry Properties dialog is redisplayed.
7. In the Country Classification Entry Properties dialog, click **Save** to save the entry.

In order for Country Classification to operate, the NetXplorer Server must have an active internet connection. If such a connection is not possible, use the following procedure to enable Country Classification.

To define a country classification without an internet connection:

1. Erase all files from <Allot home folder>:\Allot\netxplorer\jboss-4.0.2\server\allot\groups
2. Request the file IP-COUNTRY-FULL.zip from Allot Customer Support at support@allot.com and unzip it into <Allot home folder>:\Allot\netxplorer\jboss-4.0.2\server\allot\groups.
3. Stop & start the NetXplorer server service (**Start>Control Panel>Administrative Tools>Services**).
4. Wait several minutes and then check the folder <Allot home folder>:\Allot\netxplorer\jboss-4.0.2\server\allot\groups, and make sure the files were extracted.
5. Re-open the NetXplorer GUI, and confirm that you can create country classification entries. If not, contact support@allot.com.

Searching for Hosts

It is possible to search for a previously configured Host Entry.

To search for a Host Entry:

1. Select and right-click **Hosts** in the Navigation pane and select **Host Search** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Host Catalog and select **Host Search** from the popup menu.

The External File Host Group Entry Properties dialog is displayed.

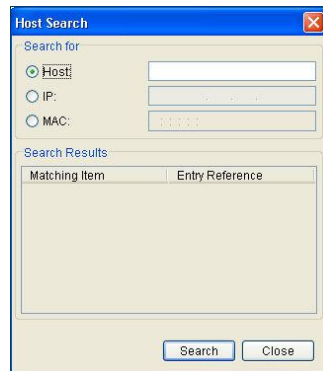


Figure 4-13: Host Search Dialog

A Host Entry can be searched for by Host Name, IP or MAC address.

2. Click **Search**. Any results are shown in the Search Results list.
3. Click Close to close the dialog.

Service Catalog

The Service Catalog contains entries that are the possible values for the Service of a Enforcement Policy. The Service defines the protocol of the connection passing through a NetEnforcer or Service Gateway. The entries are applications or protocol specifications, including network protocols, transport protocols and application protocols.

The Service Catalog contains two types of objects: services and service groups.

Services are the protocol or application-based criteria for traffic classification. A service can exist in only one location in the hierarchy at any given time. Depending on the type of service, specific content entries can be defined in order to enable the Enforcement Policy assignment and monitoring at the content level.

Service Groups enable you to efficiently assign policies multiple services, instead of having to define separate policies on a service-by-service basis. Service groups also enable you to generate reports for specific groups of services. A Service Group can contain services or additional Service Groups, but each service can appear in only one group. You can create up to four group levels. For example, Service Group 1, might comprise two Service Groups, A and B. The services in Service Group A could be subdivided into another set of Service Groups, which in turn would contain services. In addition, services can be assigned at various levels in the hierarchy.

NOTE The “Cache out” Service Group enables the user to configure a different Enforcement Policy for MediaSwift cache out traffic (for example: shaping P2P traffic on the internet link while enabling P2P traffic which returns from the MediaSwift cache to pass directly to subscribers without shaping). This capability is supported for both internal and external MediaSwift.

Services are easily moved between Service Groups. Any content previously defined for a service moves together with the service.

A sample Service Catalog is shown below:

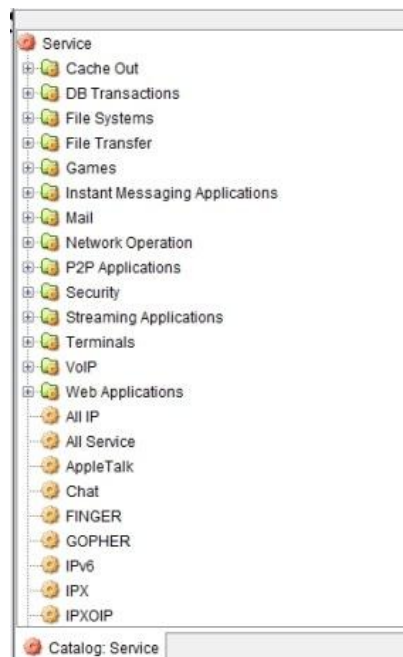






Figure 4-14: Service Catalog

From the Service Catalog, you can define the following:

- Service Groups
- Services
- Content (if supported, for the service type)

The following icons are used to represent the different types of Service Catalogs entries:

-  Service Group
-  Service
-  Content
-  HTTP UDS (Only available on devices running AOS software)

Defining a Service

Defining a Service enables you to assign policies to more than one service at a time. A Service can contain services or additional service groups.

Applications are used to further define services. An application is a unique identifier. For example, if HTTP is the application type and port X is configured as the standard port for HTTP traffic, then by default the traffic on that port is classified as HTTP. Application packet received on port Z is attributed to a different service.

Assigning applications to services enables NetXplorer to look for the best match and not simply classify traffic according to the order of criteria in policies.

The port/service assignment can be manually configured or you can select from a library of preconfigured entries.

To add a service:

1. Select and right-click **Services** in the Navigation pane and select **New Service** from the popup menu.

OR

In the Application Details pane, select and right-click an entry in the Services Catalog and select **New Service** from the popup menu.

OR

Select **New Service** from the Actions menu.

The Service Entry Properties dialog is displayed.

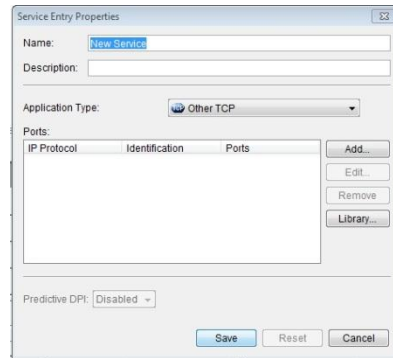


Figure 4-15: Service Entry Properties

2. Complete the **Name** and **Description** fields, if required.
3. Select the basic application type from the **Application Type** dropdown list. Other TCP is selected by Default.
4. For TCP or UDP-based protocols, manually configure the port properties for the application by clicking Add. The Port Properties dialog is displayed.

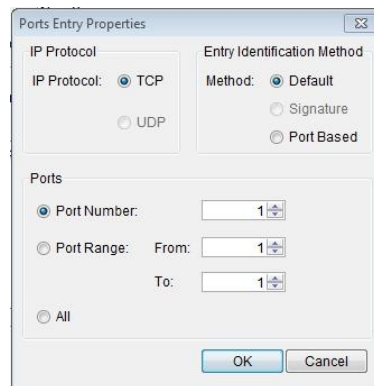


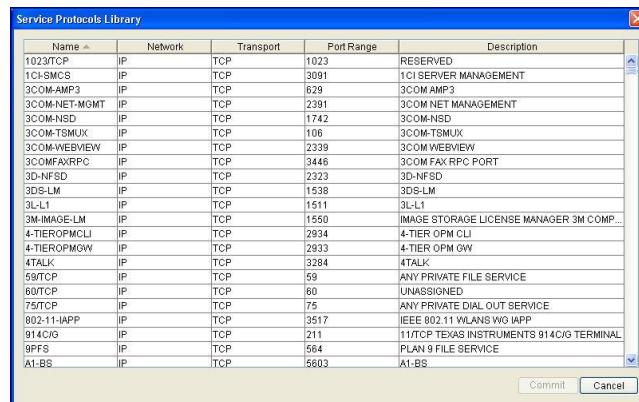
Figure 4-16: Ports Entry Properties – New Service

5. In the IP Protocol area, select the relevant protocol type, **TCP** or **UDP**.
6. In the Entry Identification Method area, select the method used to identify traffic, as follows:
 - **Port-based:** Identifies the traffic according to the destination port, regardless of the application.
 - **Signature:** Identifies the traffic according to the signature of origin, regardless of the application.
 - **Default:** Identifies the traffic by signature. If the signature is not recognized, then the traffic is identified according to the port used, regardless of the application.

- In the Ports area, configure the ports to be assigned to the service. You can configure a single port by selecting **Port Number** and entering the port number, or you can configure a range of consecutive ports by selecting **Port Range** and entering the first and last ports in the range in the **From** and **To** fields, respectively.

NOTE Multiple, non-consecutive ports must be configured separately.

- The **Predictive DPI** field is disabled by default. For more information contact Allot Customer Support.
- Click **OK**. The Service Entry Properties dialog is redisplayed.
- To select a publicly recognized port assignment for the application, click **Library...** in Service Entry Properties dialog. The Service Protocols Library dialog is displayed.



Name	Network	Transport	Port Range	Description
1023TCP	IP	TCP	1023	RESERVED
1CI-SMCS	IP	TCP	3091	1CI SERVER MANAGEMENT
3COM-AMP3	IP	TCP	629	3COM AMP3
3COM-NET-MGMT	IP	TCP	2391	3COM NET MANAGEMENT
3COM-NSD	IP	TCP	1742	3COM-NSD
3COM-TSMUX	IP	TCP	106	3COM-TSMUX
3COM-WEBVIEW	IP	TCP	2339	3COM WEBVIEW
3COM-FAXRPC	IP	TCP	3446	3COM FAX RPC PORT
3D-NFSD	IP	TCP	2323	3D-NFSD
3DS-LM	IP	TCP	1538	3DS-LM
3L-L1	IP	TCP	1511	3L-L1
3M-IMAGE-LM	IP	TCP	1550	IMAGE STORAGE LICENSE MANAGER 3M COMP...
4-TIEROPMCLI	IP	TCP	2934	4-TIER OPM CLI
4-TIEROPMGW	IP	TCP	2933	4-TIER OPM GW
4TALK	IP	TCP	3284	4TALK
59TCP	IP	TCP	59	ANY PRIVATE FILE SERVICE
60TCP	IP	TCP	60	UNASSIGNED
75TCP	IP	TCP	75	ANY PRIVATE DIAL OUT SERVICE
802-11-IAPP	IP	TCP	3517	IEEE 802.11 WLANS WIG IAPP
914C/G	IP	TCP	211	11/TCP TEXAS INSTRUMENTS 914C/G TERMINAL
9PFS	IP	TCP	564	PLAN 9 FILE SERVICE
A1-BS	IP	TCP	5603	A1-BS

Figure 4-17: Service Protocol Library

- Select an entry in the library and click **Commit**. The selected entries are added to the Ports list in the Service Entry Properties dialog.
- Click **Save** in the Service Entry Properties dialog to save the changes.

Defining a Service Group

Defining a Service Group enables you to define a Pipe or Virtual Channel so as to have more than one service associated with it. A Service Group can contain services.

To define a service group:

- Right-click **Services** in the Navigation pane and select **Add Service Group** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Services Catalog and select **New Service Group** from the popup menu.
OR

Select **New Service Group** from the Actions menu.

The Service Entry Properties dialog is displayed.

2. Edit the name of the entry in the **Name** field, if required.
3. Click **Add** to add items to the Service Entry Name List. The Add Group Items dialog is displayed.

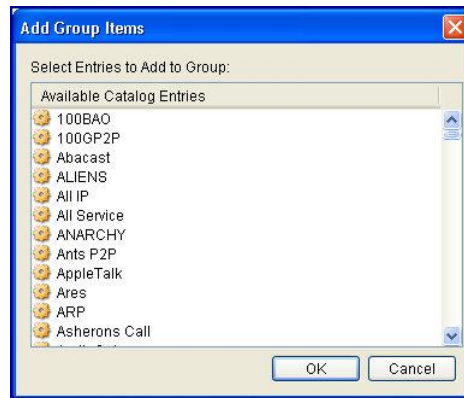


Figure 4-18: Add Group Items

4. Select one or more services using standard Windows multiple selection methods, and click **OK**. The services are added to the Service Entry Name list in the Service Entry Properties dialog.

NOTE If you select a service that has already been assigned to another group, it is moved to the new location together with all of its associated content.

5. Click **Save** to save the new Service Group.

To remove a service from the Service Catalog:

1. Select and right-click the Service in the Service Catalog and then select **Delete** from the popup menu.

OR

Select the Service and then select **Delete** from the Edit menu.

OR

Select the Service and then click  on the toolbar.

A confirmation dialog is displayed.

2. Click **Yes** to confirm the deletion. The service is removed from the Service Catalog.

Assigning Services to a Service Group

You can add or remove services from existing service groups.

If you add a service to a Service Group that is in use in an existing Enforcement Policy, the Enforcement Policy is automatically updated to include the additional service.

To add a service to an existing Service Group:

1. Select and right-click the Service Group in the Service Catalog and then select **Properties** from the popup menu.

OR

Select the Service Group and then select **Properties** from the Actions menu.

The Service Entry Properties dialog is displayed.

2. Click **Add** to add additional service(s) to the Service Group. The Add Group Items dialog is displayed.
3. Select one or more services using standard Windows multiple selection methods, and click **OK**. The services are added to the Service Entry Name list in the Service Entry Properties dialog.

NOTE If you select a service that has already been assigned to another group, it is moved to the new location together with all of its associated content.

4. Click **Save** to update the Service Group.

To remove a service from a Service Group:

1. Right-click the Service Group in the Service Catalog and then select **Properties** from the popup menu.

OR

Select Service Group and then select **Properties** from the Actions menu.

The Service Entry Properties dialog is displayed.

2. Select a service from the Service Entry Name list and click **Remove**. The service is removed from the Service Entry Name list in the Service Entry Properties dialog.
3. Click **Save** to save your changes.

Changing the Location of a Service

You can move a service from one service group to another, or to outside groups altogether.

To move a service:

1. In the Application Details pane, select and right-click the entry you wish to move in the Services Catalog and select **Move** from the popup menu.



Figure 4-19: Move Service Wizard – Select Source

The Move Service Wizard is displayed.

2. Select the target service or service group to which you wish to move the service, and click **Save**. The location of the service is changed in the service hierarchy in the Service Catalog accordingly.

Adding Content

You can add or remove content from existing services, for example some file transfer and VoIP services, depending on the type of entry.

NOTE This feature is not available on NetEnforcers or Service Gateways running AOS software, with the exception of the following VoIP protocols: RTP, SIP-RTP and H.323-RTP, all of which can be classified by codec.

If you add content to a service that is in use in an existing Enforcement Policy, the Enforcement Policy is automatically updated to include the content.

To add content to service:

1. Right-click the Service root node or a Group node in the Service Catalog and then select **New Content** from the popup menu.

OR

Select the Service root node or a Group node and then select **New Content** from the Actions menu.

OR

Select **New Content** from the Actions menu.

The Service Entry Properties dialog is displayed.

The screenshot shows a dialog box titled "Content Entry Properties". It has a close button in the top right corner. The "Name" field contains "New Content". The "Description" field is empty. The "Service" dropdown menu is set to "100BAO". Below this is a table with two columns: "Type" and "Value". To the right of the table are three buttons: "Add...", "Edit..", and "Remove". At the bottom of the dialog, there is a "Predictive DPI" dropdown menu set to "Disabled", and three buttons: "Save", "Reset", and "Cancel".

Figure 4-20: Service Entry Properties – New Content

2. Click **Add** to add content to the Service. The Content Properties dialog is displayed.
3. Select the type of content from the Content Type dropdown list, for example (relevant to the example shown), File Name or Command.

NOTE The available content types vary according to the service type. For example for FTP service the available content types are File Name or Command.

4. Select the content value from the **Value** dropdown list.

OR

Click the Browse button and define the content values in the Application Type Content Editor.

NOTE The format of the Value field varies according to the selected type of content.

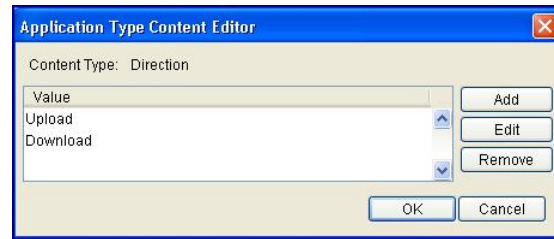


Figure 4-21: Application Type Content Editor

5. To define content values in the Application Type Content Editor, click **Add**. The Content Value Properties dialog is displayed.
6. Enter the required value in the Value field and click **OK**. The Application Type Content Editor is redisplayed.
7. Click **OK** in the Application Type Content Editor to redisplay the Content Properties dialog. The new content value is now available for selection from the **Value** dropdown list.
8. Verify that required value is selected and click **OK**. The Service Entry Properties dialog is redisplayed.
9. The **Predictive DPI** field is disabled by default. For more information contact Allot Customer Support.
10. Click **Save** in the Service Entry Properties to add the content.


To remove a content entry from the Service Catalog:

1. Right-click the Content entry in the Service Catalog and then select **Delete** from the popup menu.

OR

Select the Content entry and then select **Delete** from the Edit menu

OR

Select the Content Entry and then click  on the toolbar.

A confirmation dialog is displayed.
2. Click **Yes** to confirm the deletion. The service is removed from the Service Catalog.

Adding User Defined Signatures

You can create HTTP User Defined Signatures (UDS) that define certain HTTP content. Once defined a UDS is a service in its own right and is not part of another service such as HTTP.

NOTES This feature is only available on NetEnforcers or Service Gateways running AOS (Allot Operating System).

Before creating a User Defined Signature the feature must be enabled individually for each NetEnforcer from the Networking tab in the NetEnforcer's Configuration window. See p. 3-17 for details.

It is impossible to set priority between User Defined Signatures therefore the UDS with the most content key matches has priority in most situations. However, if two User Defined Signatures have the same number of content key matches, the UDS with a content key match earlier in the packet will have priority.

To create a UDS catalog entry:

1. Right-click **Services** in the Navigation pane and select **Add HTTP UDS** from the popup menu.

OR

In the Details pane, right-click an entry in the Services Catalog and select **New HTTP UDS** from the popup menu.

OR

Select **New HTTP UDS** from the Actions menu.

The Service Entry Properties dialog is displayed.

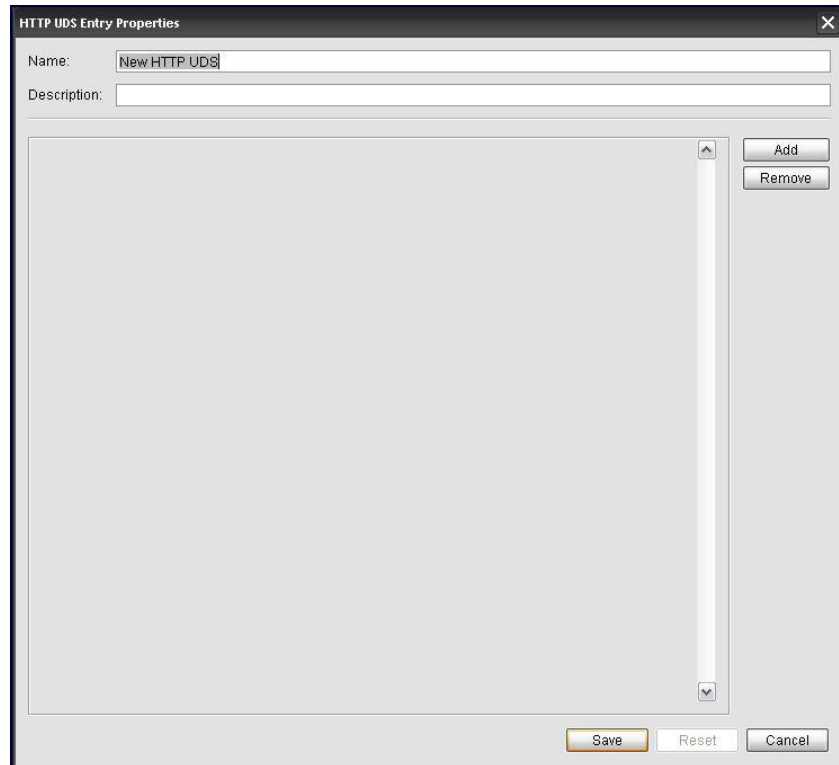


Figure 4-22: HTTP UDS Entry Properties

2. Enter a Name and Description if required.
3. Click **Add** to add Content Keys to the signature. Each time Add is clicked, a new Content Key field is opened. Select the Content Key desired from the drop down menu.

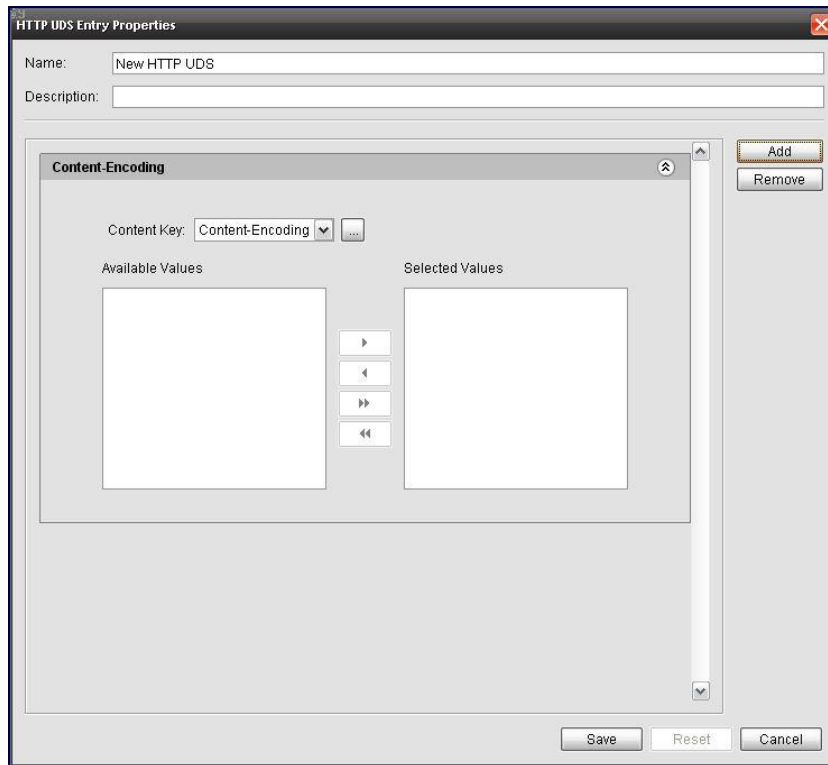


Figure 4-23: HTTP UDS Entry Properties -Add

4. Possible content keys include Content – Encoding, Content – Length, Content – Type, Hosts, Location, Method, Referer, URL, and User-Agent.

HEADER	DESCRIPTION	EXAMPLES	VALUE TYPE
Host	The domain name of the server requested	www.cnn.com www.ynetnews.com NOTE Avoid adding overlapping services to the Available Values list, such as www.cnn .com and *cnn.com.	Free text
Method	The desired action to be performed on the resource identified by the Request-URI	GET, CONNECT, POST	Predefined values to select

HEADER	DESCRIPTION	EXAMPLES	VALUE TYPE
Referer	This is the address of the previous web page from which a link to the currently requested page was followed.	When opening cnn.com from a google search the “Referer” will show: http://www.google.com/search?hl=en&q=cnn.com&rlz=117RNTN_en <CR> <LF>	Free text
URL (URI)	A Uniform Resource Locator (URL) is a Uniform Resource Identifier (URI) that specifies where an identified resource is available and the mechanism for retrieving it	When opening the Tolly Report from http://www.allot.com then the “URI” is: /Tolly_Report.html	Free text
User-Agent	Contains information about the web-browser or the type of mobile handset originating the request.	Browser e.g: Mozilla/5.0 Mobile handset e.g: “Nokia...”	Free text
Content-Encoding	The type of encoding used on the data	gzip	Free text
Content-Length	The length of the response body in octets (8-bit bytes)	254	“greater than” or “lower than” Integer
Content-Type	The MIME type of this content (Multipurpose Internet Mail Extensions)	text/html image/gif image/jpeg	Predefined values to select
Location	An alternate location for the returned data	http://edition.cnn.com http://www.bbc.co.uk/	Free text

NOTE Each field in a UDS may contain a maximum of 69 characters.

5. Each content key will have values listed in the Available Values field. Use the arrow keys to move them back and forth from the Selected Values field.
6. Click the Browse button next to the Content Key field to open the Edit Content Values dialog and add custom values.



Figure 4-24: Edit Content Values dialog

7. Click **Remove** to delete a selected Content Key.
8. Click **Save** to save the any changes to the Content Key and return to the HTTP UDS Entry Properties dialog.
9. Click **Save** in the Service Entry Properties to add the content.

Wildcards

The following characters may be used as wildcards when entering Content Keys:

- Any “Free text” defined in any of the keys will match the relevant header if it starts with the same string (“abc” will match any header starting with “abc”)
- An asterisk “*” may be added only to the beginning of a string to indicate that the string may be any place in the header and not only in the beginning (“*abc” will match any header with “abc” in it)
- “\?” may be added to the string to match a single character (“ab\?c” will match any header starting with “ab” which then has a single character followed by the character “c”)

Protocol Updates

NOTE Protocol Updates are only available to those users with the appropriate license key entered to enable the feature.

Overview

Service Catalog entries may be updated from Allot Communication Website where the latest available Service Catalog information is maintained.

NetXplorer periodically checks Allot's website for the latest available Protocol Packs. You can then update Service Catalog entries on the NetXplorer Server and install any changes on selected or all NetEnforcer or Service Gateway devices, as required.

The NetXplorer's installation of Protocol Pack updates may be configured to be done automatically or manually.

NetXplorer provides a **rollback** mechanism that enables you to return to a previous version of the appropriate Service Catalog entries.

The Protocol Update procedure involves two tasks:

- Updating the NetXplorer Service Catalog entries with changes in application types, services and service groups via a Protocol Pack
- Updating the NetEnforcer or Service Gateway device protocol changes installed on the NetXplorer

To update Service Catalogs, you select the appropriate option from the NetXplorer Tools menu, and the Protocol Update wizard guides you through the NetXplorer Server and NetEnforcer or Service Gateway update processes:

Where necessary, you can also update Service Catalog entries from local media, such as CDs and disc drives.

Automatic Protocol Updates

You can configure NetXplorer to check the Allot Website periodically for new Protocol Packs and automatically update NetXplorer Server.

The system default is “**Check Allot Website for New Updates (Periodically)**” option. By retaining this option, whenever new Service Catalog entries are available, NetXplorer send an alert message to the Alarms Log.

The frequency of the checks is system defined and cannot be configured by users.

Updating the NetXplorer Server

The NetXplorer Protocol Update mechanism allows users to automatically update the NetXplorer Server with new Service Catalog information. However, to update NetEnforcer or Service Gateway Devices, you need to update selected NetEnforcer or Service Gateway device(s) manually.

Although the “Update Wizard” can guide you through both update processes, you maintain control of update versioning on the NetEnforcer or Service Gateway(s).

To configure automatic Protocol Updates:

1. Open NetXplorer.
2. In the Navigation pane, right-click the Network in the Navigation tree and select **Configuration** from the popup menu. The tabbed Network window is displayed.
3. Open the **Protocol Updates** tab.

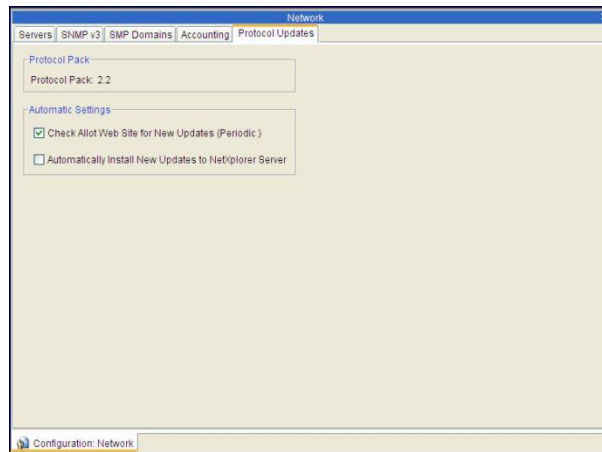


Figure 4-25: Service Catalog Web Updates Configuration tab

4. The Protocol Pack version currently installed on the NetXplorer is displayed.
5. Select the Check Allot Web Site for New Updates (Periodic) option to allow the NetXplorer to automatically check if a more recent Protocol Pack is available. This option is selected by default.
6. If you wish to have downloads automatically installed on the NetXplorer Server, select the **Automatically Install New Updates to NetXplorer Server....**option.

(If you wish to manually install packages to the NetXplorer Server using the Service Catalog Web Update Wizard, do *not* select this option).

7. Click **Save** in the Toolbar to save any changes.

When you select the “Automatically Install....” option, an alarm advice entry appears in the Alarms Log when a new Protocol Pack is installed.

To update selected NetEnforcer devices, see the Updating Service Catalogs on NetEnforcer or Service Gateways section.

Manual Protocol Updates

The NetXplorer Protocol Update mechanism allows users to manually update the NetXplorer Server with new Service Catalog Plan (SPC) package information.

To enable this option, clear the **Automatically Install New Updates on the NetXplorer Server** option.

By retaining the **Check Allot Web Site for New Updates (Periodically)**” option, whenever new Service Catalog entries are available, NetXplorer sends an alert message to the Alarms Log.

After viewing this Info alert in the Alarms Log, you can decide when to update the NetXplorer Server’s Service Catalog entries.

The “Update Wizard” guides you through manually updating the NetXplorer Server and maintaining version control when updating SRCs on selected NetEnforcer or Service Gateway(s).

Viewing the Protocol Pack Version

Before you update a NetEnforcer or Service Gateway Service Catalog, you can view the Protocol Pack version that is currently loaded on the NetEnforcer or Service Gateway Device.

To view the Protocol Pack version running on a device:

1. In the Navigation pane, right-click the appropriate device in the Navigation tree and select **Configuration** from the popup menu. The tabbed Network window is displayed.
2. Choose the Identification & Key tab:
3. The version of Protocol Pack installed on the device appears in the IDs area of the window

Updating the NetXplorer

Once you have received an Alert advising that NetXplorer Service Catalog updates are available, you perform the Protocol Update by using the appropriate NetXplorer Tools menu options.

The Protocol Update mechanism enables you to perform updates on both the NetXplorer Server and any NetEnforcers or Service Gateways using the Update Wizard.

Whenever you use the Update Wizard, NetXplorer checks the Service Catalogs on both the NetXplorer Server and NetEnforcer or Service Gateway(s). If the most current versions have already been installed on NetXplorer Server and NetEnforcer or Service Gateway Devices, you are informed that there is no need to continue the update.

To perform Protocol Updates from the Allot website:

1. After you view the Alarm Log advice that "...new Web updates are available for download...." line, click on the Network icons and choose the **From Allot Website** option from the Tools Protocol Updates sub-menu.

The Service Catalog Update Wizard Introduction window is displayed.

2. To check the last version on the NetXplorer Server (and NetEnforcer or Service Gateways) click the **Check for Updates** button.

The Protocol Update Wizard Pending Changes window is displayed:

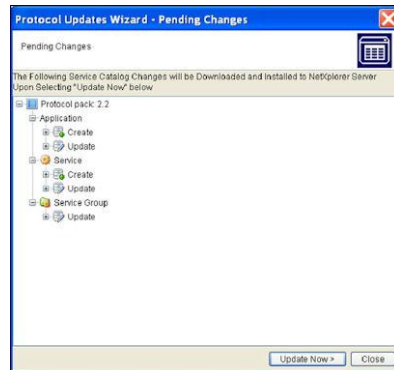


Figure 4-26: Protocol Update – Pending Changes

3. To install the pending update on the NetXplorer Server, click the **Update Now** button.

NOTE You cannot select individual packages to be installed here. To cancel the update, click the **Close** button.

4. After clicking the **Update Now** button, the Wizard Installation to NetXplorer Version Summary window is displayed detailing the results of the update/install operation:

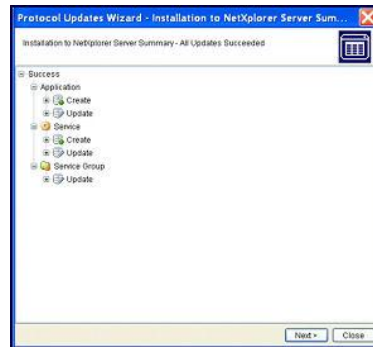


Figure 4-27: Protocol Update – Installation to NetXplorer Server Summary

5. To complete the NetXplorer Server update, click **Next**.
The Protocol Update Wizard Summary window is displayed.
6. At this stage you can stop the “Update to the NetXplorer Server” process by clicking the **Close** button in the wizard.
7. Click **Save**.

Updating Service Catalogs on NetEnforcer or Service Gateways

After manually updating the Protocol Pack on the NetXplorer Server, you can install the updates to one or several NetEnforcers or Service Gateways, as required.

You install updates to NetEnforcer or Service Gateway(s) choosing the Install to Device option from the Tools Protocol Updates sub-menu

To install a Protocol Update on a NetEnforcer or Service Gateway:

1. Click on the Network icon in the Network navigation pane and choose the **Install to Devices** option from the Tools Service Catalog Web Updates sub-menu.

The Protocol Update Wizard – Installation to Devices window is displayed:

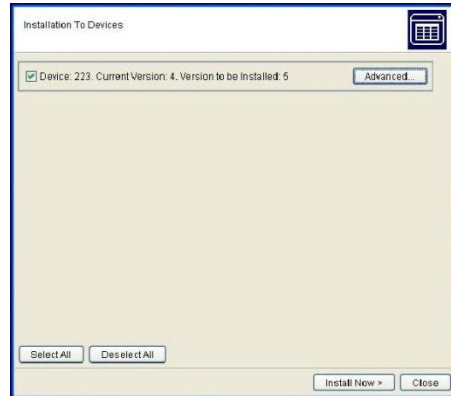
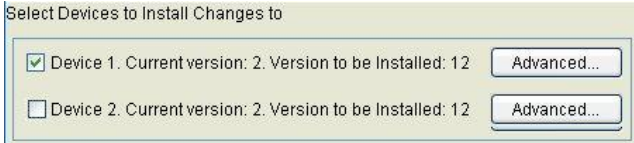


Figure 4-28: Protocol Update Wizard – Installation to Devices

BUTTON	DETAILS
Advanced	<p>Displays the Version to Install Device dialog that contains details of the pending changes for the version to be installed on the selected box. You can select specific boxes by selecting or clearing the Device check box:</p> 
Select All	Select all Devices and versions in the “Installation to Devices” window.
Deselect All	Clear selection of all Devices and versions in the “Installation to Devices” window.
Install Now	To install the version to be installed to specific NetEnforcer or Service Gateway(s). Depending on the size and number of updates, there may be a time delay before the “Summary” window is displayed.

- To install the latest version to the selected NetEnforcer or Service Gateway device(s), click the **Install Now** button.

The Service Catalog Web Update Wizard - Installation to NetXplorer Server – Summary window is displayed.

- To complete the NetEnforcer or Service Gateway Service Catalog update, click **Next**.

The Protocol Update Wizard Summary window with “Update Completely Successful.....” is displayed.

- Click Close and enable a Save option.

If you select the Install to Devices option from the Tools Protocol Updates sub-menu, and an update has already taken place, the Wizard will inform you that there are no devices to update.

Advanced Protocol Updating on NetEnforcer or Service Gateways

You can use the **Advanced** button in the Protocol Update Wizard – Installation to Devices window (see Step 3 in the Updating Service Catalogs on NetEnforcer or Service Gateways section) to install a specific version on a selected NetEnforcer or Service Gateway. In the case, for example, where several versions of the Protocol Pack have been loaded on the NetXplorer Server and only one of these versions is needed to be downloaded to a specific NetEnforcer or Service Gateway.

The Version to Install to Device allows you to:

- Choose the version of the Protocol Pack you wish to install
- View the details of the update

To view the details of the changes, you selected the required version using the combo-box direction arrows.

To install a specific Protocol Pack to a NetEnforcer or Service Gateway:

1. Click on the Network icon in the Network navigation pane and choose the Install to Devices option from the Tools Service Catalog Web Updates sub-menu.

The Protocol Update Wizard – Installation to Devices window is displayed.

2. Select (or clear) the Device check box and click the **Advanced** button.

The Version to Install to Device dialog is displayed.

3. To view previous versions, click on the up or down combo-box direction arrows.

The details in the Pending Changes for Version ...will change accordingly.

4. To confirm the version that you wish to install on NetEnforcer, click **OK**.

You return to the Catalog Update Wizard – Installation to Devices window.

5. To install the selected version, click **Install Now**.

The Protocol Update Wizard - Installation to NetXplorer Server – Devices Summary window is displayed.

6. To complete the NetEnforcer Service Catalog update, click **Next**.

The Protocol Update Wizard Summary window with “Update Completely Successful.....” is displayed.

7. Click **Close** and enable a **Save** option.

Updating the Service Catalog from a Local Source

If the NetXplorer does not have Internet connectivity, first download the protocol pack from Allot's website and then install it on the NetXplorer Server manually. In this case, please follow this procedure:

To download and install a Protocol Pack from a local source:

1. Login to <http://www.allot.com/support> . From the “registrations” tab, open the registration for the relevant device. If an APU is available you can click on the “download APU” field.
2. Copy the APU files from the relevant APU folder to the NetXplorer server and place them in C:\APU (create the folder if needed)
3. Confirm that there is a file named **web_update_site.xml** in the same location. This file defines the current Protocol Pack version and the next one to be installed.
4. On the NetXplorer GUI select **Tools > Protocol Updates > From Local Package**.

The Protocol Updates Wizard – Introduction dialog appears.

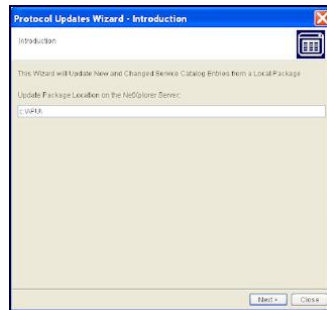


Figure 4-29: Version to Install to Device

5. Type in the Protocol Pack path (C:\APU) and click **Next**.
The Protocol Update Wizard Pending Changes window is displayed:



Figure 4-30: Protocol Update – Pending Changes

6. To install the pending update on the NetXplorer Server, click the **Update Now** button.

NOTE You cannot select individual packages to be installed here. To cancel the update, click the **Close** button.

7. After clicking the **Update Now** button, the Wizard Installation to NetXplorer Version Summary window is displayed detailing the results of the update/install operation:

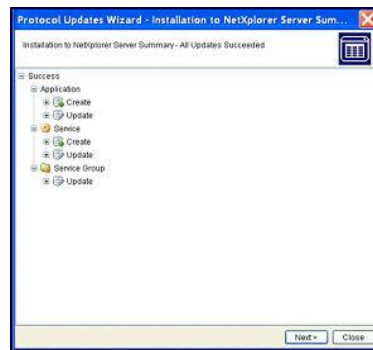


Figure 4-31: Protocol Update – Installation to NetXplorer Server Summary

8. To complete the NetXplorer Server update, click **Next**.
The Protocol Update Wizard Summary window is displayed.
9. At this stage you can stop the “Update to the NetXplorer Server” process by clicking the **Close** button in the wizard.
10. Click **Save**.

Rollback Operations

NetXplorer provides a **rollback** mechanism that enables you to return to the previous version of the appropriate Service Catalog entries.

The Services Catalog Web rollback allows you to:

- Rollback the NetXplorer Server Service Catalog entries
- Rollback the NetEnforcer or Service Gateway Device Service Catalog entries

To rollback to a previous Protocol Pack version on the NetXplorer Server:

1. Select the Network icon in the NetXplorer Navigation pane and choose the **Rollback NetXplorer Server to Previous Version** option from the Tools Protocol Updates sub-menu.

The Protocol Update Wizard – Rollback NetXplorer Rollback to Previous Version window is displayed.

2. Click the **Next** button and the NetXplorer Server Service Catalog validation check is enabled.

The Protocol Update Wizard – Rollback NetXplorer – Pending Changes window is displayed.

3. To restore the previous version click the **Rollback Now** button.

The Rollback to Previous Version Summary window is displayed showing a successful result.

4. Click the **Next** button.

The Protocol Update Wizard – Summary “Rollback Completely successful” window is displayed.

5. To exit the wizard, click **Close**.
6. Click **Save**.

To rollback to a previous Service Catalog on a NetEnforcer or Service Gateway Device:

1. Select the appropriate Device(s) in the NetXplorer Navigation pane and choose **Rollback Devices to Previous Version** from the **Tools > Protocol Updates** sub-menu.

The Protocol Update Wizard Rollback to Previous Version window is displayed.

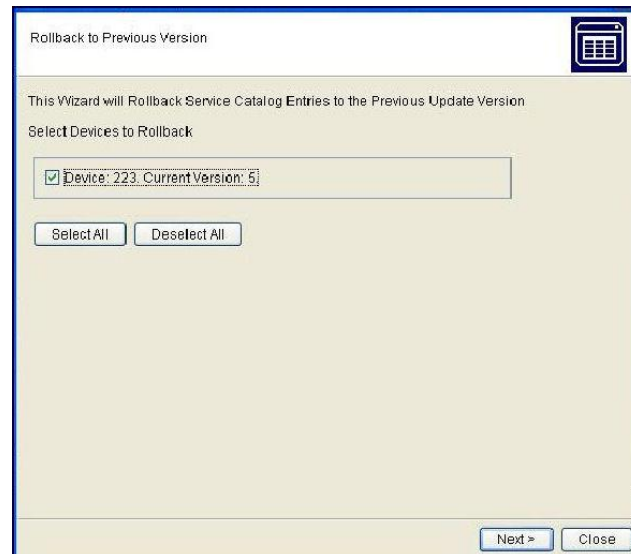


Figure 4-32: Protocol Update Wizard – Rollback Devices – Rollback to Previous Version

2. Click the **Next** button.
The Protocol Update Wizard – Rollback NetXplorer – Pending Changes window is displayed.
3. To return to the previous Service Catalog, click the **Rollback Now** button.
The Rollback to Previous Version Summary window is displayed showing a successful result.
4. Click the **Next** button and to exit the wizard, click **Close** in the Wizard’s Rollback to Previous Version Summary window.
5. Click **Save**.

NOTE If you wish to perform a rollback to even earlier Protocol Pack versions, for example from 1.5 to 1.3, repeat the “rollback operating instructions” twice.

Time Catalog

The Time Catalog contains entries that are the possible values for the time condition of a Pipe or Virtual Channel.

NOTE The Anytime entry is Protected, meaning the definitions for this entry cannot be modified.

Time periods can have ranges of hours and minutes in which they are active, or they can be active during whole days. An entry in the Time Catalog has one or several time periods when policies assigned this entry are active.

To define a time period:

1. Select and right-click **Time** in the Navigation pane and select **New Time** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Time Catalog and select **New Time** from the popup menu.

The Time Entry Properties dialog is displayed.

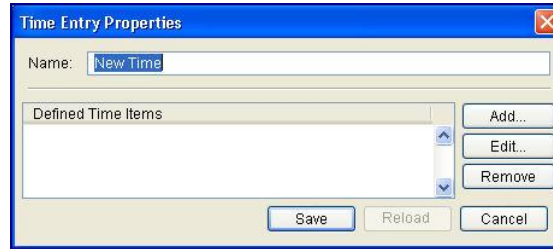


Figure 4-33: Time Entry Properties

2. Edit the name of the entry in the **Name** field, if required.
3. Click **Add**. The Add Time Item dialog is displayed.

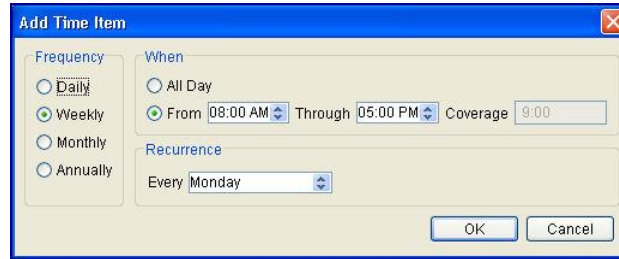


Figure 4-34: Add Time Item

4. In the **Frequency** area, select the frequency of the time period. The options are as follows:

Daily	A period of time that occurs on a daily basis.
Weekly	A period of time that occurs on a weekly basis. For example, Monday from 8:00 to 17:00.
Monthly	A period of time that occurs on a monthly basis. For example, the 15 th day of the month.

Annually A period of time that occurs on an annual basis. For example, January 1st may be defined as a yearly event.

The parameters in the **When** area vary according to frequency. Select the time span according to the frequency selected in the previous step, as follows:

If you set the frequency to **Daily**, select from the following options:

- All day** Sets the time period as active for the whole day.
- From – Through** Enables you to select the exact time that the period will begin, and the exact time that it will end.

If you set the frequency to **Weekly**, select the day of the week for the time period from the dropdown list in the **Day of Week** field and the time span from the dropdown list in the **When** field, as described in step 5.

If you set the frequency to **Monthly**, select the day of the month for the time period from the **Day of Month** field and the time span from the dropdown list in the **When** field, as described in step 5.

If you set the frequency to **Annually**, select the month for the time period from the dropdown list in the **Month** field, select the day of the month from the **Day of Month** field, and the time span from the dropdown list in the **When** field, as described in step 5.

5. Click **OK**. The specified time period is displayed in the Time Entry Properties dialog.
6. Repeat steps 3 through 9 to add additional time periods as required.
7. In the Time Properties Entry, click **Save** to save the entry.

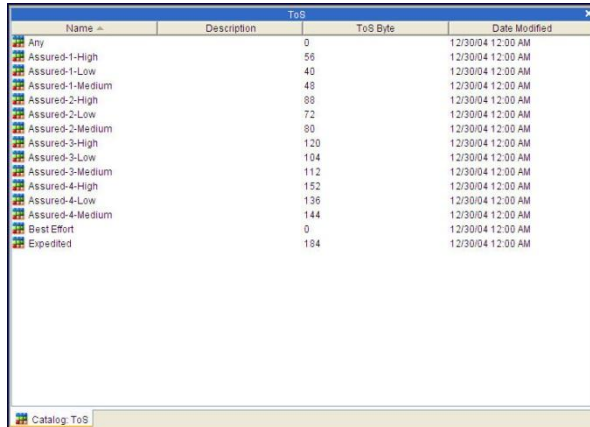
NOTE You can edit or delete the time periods using the **Edit** and **Remove** buttons in the Time Entry Properties dialog.

TIP Adding a new Enforcement Policy with time-dependent traffic classification is effective only on new connection attempts. Any existing connection that may fall under that Enforcement Policy continues to pass under its original Enforcement Policy. If a **Reject** or **Drop** action is specified, these actions are applied only to new connection attempts.

NOTE A discrete time range cannot be created. For example, March 15, 2001 from 2:00 PM through 5:00 PM cannot be created. However, it can be approximated by Yearly, March 15, 2:00 PM through 5:00 PM.

ToS (Type of Service) Catalog

The ToS Catalog contains entries that are the possible values for the ToS condition of a Pipe, Virtual Channel or Filter. A sample ToS Catalog is shown below:



Name	Description	ToS Byte	Date Modified
Any		0	12/30/04 12:00 AM
Assured-1-High		56	12/30/04 12:00 AM
Assured-1-Low		40	12/30/04 12:00 AM
Assured-1-Medium		48	12/30/04 12:00 AM
Assured-2-High		88	12/30/04 12:00 AM
Assured-2-Low		72	12/30/04 12:00 AM
Assured-2-Medium		80	12/30/04 12:00 AM
Assured-3-High		120	12/30/04 12:00 AM
Assured-3-Low		104	12/30/04 12:00 AM
Assured-3-Medium		112	12/30/04 12:00 AM
Assured-4-High		152	12/30/04 12:00 AM
Assured-4-Low		136	12/30/04 12:00 AM
Assured-4-Medium		144	12/30/04 12:00 AM
Best Effort		0	12/30/04 12:00 AM
Expedited		184	12/30/04 12:00 AM

Figure 4-35: Sample ToS Catalog

NOTE All of the entries in Figure 4-35 are predefined public domain ToS definitions and are protected, meaning that they cannot be modified.

The ToS is a byte in the IP header of a packet that contains information about routing recommendations. The NetEnforcer or Service Gateway classifies traffic based on the ToS byte marking contained in the IP headers of the packets passing through it. Differentiated Services standard, for example, defines ToS byte marking for traffic classification. Using Differentiated Services, the ToS header can have three major traffic classes: Expedited, Assured Forwarding and Best Effort. Assured Forwarding includes a priority class and drop precedence level (making a total of 12 combinations). All of these ToS byte markings are predefined in the ToS Catalog.

Further information regarding ToS standards can be found at www.ietf.org/rfc/rfc2475.txt.

NetXplorer also supports ToS classification by User Defined ToS Entry, which can be used to classify traffic marked per Cisco Precedence Bits method.

In the ToS Catalog, you can view the properties of predefined entries and create entries that classify the ToS byte using User Defined ToS Entry.

To view predefined entries:

1. In the ToS Catalog, select a predefined entry and then select **Properties** from the Actions menu.

OR

In the Application Details pane, right-click a predefined entry in the ToS catalog and select **Properties** from the popup menu.

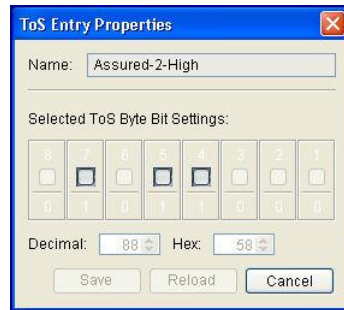


Figure 4-36: ToS Catalog – Predefined Entry Properties

NOTE Predefined public domain ToS entries cannot be modified.

User Defined ToS Entry

ToS classification using free format enables you to classify traffic marked according to the Cisco Precedence Bits method.

To define a ToS using User Defined ToS Entry:

1. Select and right-click **ToS** in the Navigation pane and select **New ToS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the ToS Catalog and select **New ToS** from the popup menu.

The ToS Entry Properties dialog is displayed.



Figure 4-37: ToS Entry Properties

2. Edit the name of the entry in the **Name** field, if required.
3. Define the ToS by inserting bit values in one of the following ways:
 - Click the bit value field boxes (zero is indicated as gray and black as one); the decimal equivalent is displayed in the Selected ToS Byte

- Enter the decimal or hexadecimal representation of the bit in the **Dec** or **Hex** fields, respectively.
4. Click **Save**. The new entry is saved in the ToS Catalog.

Encapsulation Catalog

The Encapsulation catalog contains GRE and VLAN entities defined in the IEEE 802.1 Standard.

Defining VLANs

NetEnforcer or Service Gateway supports VLAN traffic classification according to VLAN ID (VLAN Identifier) tags, consisting of 12 bits, and according to tagging priority bits, consisting of three bits. These definitions are set in the VLAN Catalog, as shown below:

According to the policies you define, NetXplorer assigns each packet a mapping priority and QoS definition.

The VLAN definition value is comprised as follows:

- Bits 1 – 12 specify the VLAN ID.
- Bit 13 is the reserved bit.
- Bits 14 – 16 specify the user priority (where 7 is highest priority, and 1 is lowest priority).

User can Create/Edit:

- Catalog that contains only User Priority without VLAN ID by checking the Any VLAN ID check box.
- Catalog that contains only VLAN ID without User Priority by checking the User Priority check box.
- Catalog that doesn't contain VLAN ID or User Priority by checking both boxes. (This is useful if user wants to edit the VLAN catalog from the Enforcement Policy Editor to work with/without VLAN).

To create a VLAN Catalog entry:

1. Select and right-click **Encapsulation** in the Navigation pane and select **New VLAN** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Encapsulation Catalog and select **New VLAN** from the popup menu.

OR

Select **Encapsulation** in the Navigation pane when Catalogs are displayed and select **New VLAN** from the Actions menu.

The VLAN Entry Properties dialog is displayed.

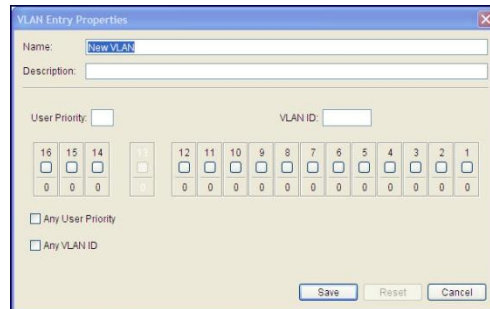


Figure 4-38: VLAN Entry Properties dialog

2. Complete the **Name** and **Description** fields, if required.
3. Confirm that the **User Priority** and/or **Any VLAN ID** checkboxes are clear (default) to insert new bit values.
4. Insert bit values in one of the following ways:
 - Insert a decimal value in the **User Priority** and/or **VLAN ID** fields; the binary equivalent is displayed in the bit value fields.
 - Click the bit value field boxes (zero is indicated as gray and black as one); the decimal equivalent is displayed in the **User Priority** and **VLAN ID** fields.
5. Click **Save**. The new entry is saved in the Encapsulation Catalog.

Defining GREs

To create a GRE Catalog entry:

1. Select and right-click **Encapsulation** in the Navigation pane and select **New GRE** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Encapsulation Catalog and select **New GRE** from the popup menu.

OR

Select and **Encapsulation** in the Navigation pane and select **New GRE** from the Actions menu.

The GRE Entry Properties dialog is displayed.

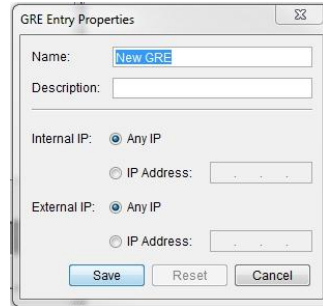


Figure 4-39: GRE Entry Properties dialog

2. Complete the **Name** and **Description** fields, if required.
3. Define an Internal (source) IP for the GRE by selecting the relevant radio button. You may select Any IP (which will include GRE tunnels originating from all internal IPs) or enter a specific IP.
4. Define an External (destination) IP for the GRE by selecting the relevant radio button. You may select Any IP (which will include GRE tunnels going to all external IPs) or enter a specific IP.
5. Click **Save**. The new entry is saved in the Encapsulation Catalog.

Defining Encapsulation Groups

To create an Encapsulation Group Catalog entry:

1. Select and right-click **Encapsulation** in the Navigation pane and select **New Encapsulation Group** from the popup menu. Define if you wish a **New VLAN Group** or a **New GRE Group**.

OR

In the Application Details pane, right-click an entry in the Encapsulation Catalog and select **New Encapsulation Group** from the popup menu. Define if you wish a **New VLAN Group** or a **New GRE Group**.

OR

Select **Encapsulation** in the Navigation pane and **New Encapsulation Group** from the Actions menu. Define if you wish a **New VLAN Group** or a **New GRE Group**.

Either the GRE Group Entry Properties or the VLAN Group Entry Properties dialog is displayed.

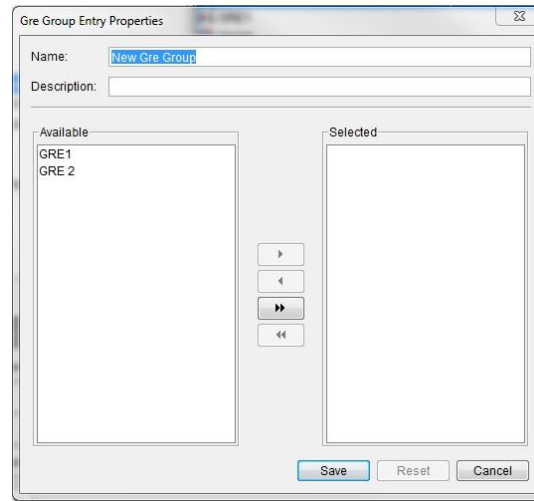
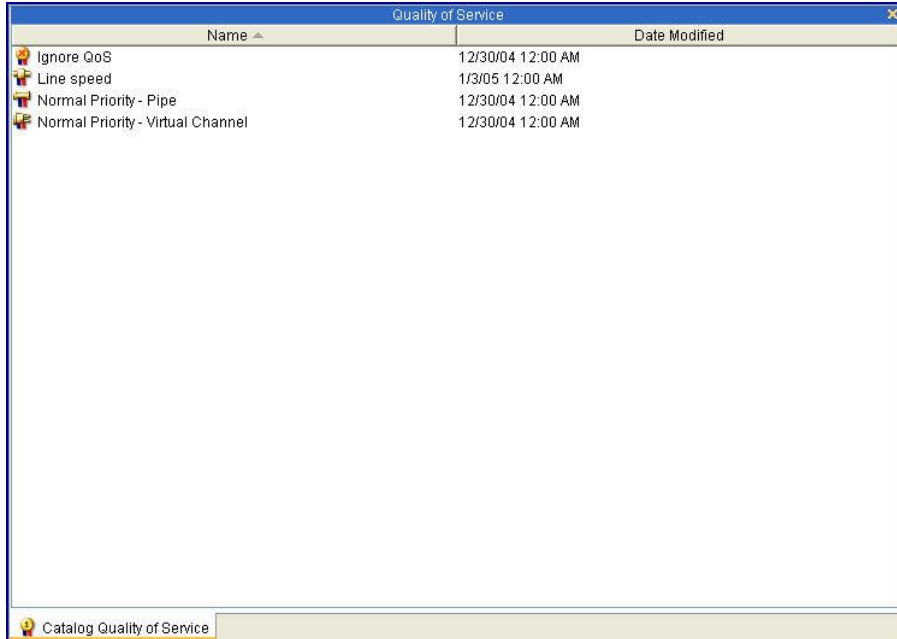


Figure 4-40: GRE Entry Properties dialog

2. Complete the **Name** and **Description** fields, if required.
3. Select GREs or VLANS in the Available list and use the arrow keys to move them into the Selected list.
4. Click **Save**. The new Group entry is saved in the Encapsulation Catalog.

Quality of Service Catalog

The QoS Catalog contains entries that are the possible values for the Quality of Service action. This is the QoS applied to traffic when it meets the definitions of a Enforcement Policy. A list of the default QoS Catalogs is shown below:



Name	Date Modified
Ignore QoS	12/30/04 12:00 AM
Line speed	1/3/05 12:00 AM
Normal Priority - Pipe	12/30/04 12:00 AM
Normal Priority - Virtual Channel	12/30/04 12:00 AM

Figure 4-41: Default QoS Catalog

NOTE The Ignore QoS, Line speed, Normal Priority – Pipe and Normal Priority - Virtual Channel entries are protected, meaning the definitions for these entries cannot be modified.

The QoS Catalog enables you to define QoS for a Line, Pipe or Virtual Channel. Six different types of QoS Catalogs can be defined:

- Line QoS
- Pipe QoS
- Virtual Channel QoS
- Line Enhanced QoS
- Pipe Enhanced QoS
- Virtual Channel Enhanced QoS

If you are building a Enforcement Policy on a NetEnforcer or Service Gateway product running AOS software (e.g: SG-Sigma or AC-10000 series) then you should use only Enhanced Line, Enhanced Pipe and Enhanced Virtual Channel Catalogs.

If you are building a Enforcement Policy on a NetEnforcer or Service Gateway that does NOT run AOS software (e.g: AC-800 or SG-Omega series) then you should use only Line, Pipe or Virtual Channel QoS.

In the Quality of Service Catalog, there is a pre-defined entry called **Ignore QoS** that you cannot delete or create additional entries that ignore QoS.

You can give the same QoS definitions to both directions of traffic, or define QoS parameters for both directions independently.

TIP **A priority definition implies a relative bandwidth allocation relationship to other defined priorities. It does not indicate absolute bandwidth allocations. If you require absolute bandwidth allocation, refer to the descriptions of the minimum, maximum and guaranteed bandwidth fields.**

Ignoring Quality of Service

The inbound and outbound traffic bypasses NetEnforcer or Service Gateway's QoS mechanism if the **Ignore QoS** option is selected, thereby potentially saving physical bandwidth for other traffic. However, using **Ignore QoS** in a Enforcement Policy definition leads to an attempt to satisfy any bandwidth request. This may adversely affect other bandwidth definitions.

TIP: **This option is normally used in networks where internal traffic stays within the LAN domain, for example, when DMZ-bound traffic stays local and is not destined to go on the physical WAN bandwidth.**

To view the Ignore QoS entry:

- In the Application Details pane, right-click **Ignore QoS** in the QoS Catalog and select **Properties** from the popup menu. A warning is displayed in the Definition pane of the QoS Catalog.

Defining QoS for Lines

Entries in the QoS Catalog that are defined for Lines are available when assigning QoS to Lines in the Enforcement Policy Editor.

To define QoS for a Line:

NOTE **If your NetEnforcers or Service Gateways are running AOS (Allot Operating System), you should not use Line QoS Catalogs. Instead, use Enhanced QoS Line Catalogs.**

1. Select and right-click **QoS** in the Navigation pane and select **New Line QoS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the QoS Catalog and select **New Line QoS** from the popup menu.

The Line QoS Entry Properties dialog is displayed.

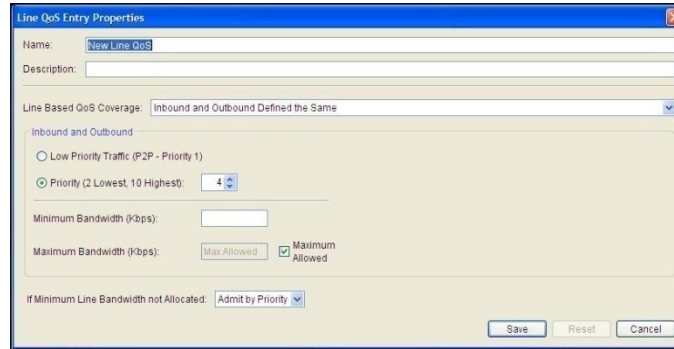


Figure 4-42: New Line QoS Entry Properties

2. Edit the name and description of the entry, if required.
3. From the **Line-based QoS Coverage** dropdown list select one of the three options:
 - **Inbound and Outbound Defined the Same:** Define QoS for both the inbound and outbound traffic together. This option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical.
 - **Each Direction Defined Separately:** Define QoS for the inbound and outbound traffic individually (instead of the **General** tab, the **Inbound** tab and the **Outbound** tab appear).
 - **Half Duplex Line:** Define QoS for a half-duplex Line.
4. In the **Inbound and Outbound** area, define the Quality of Service as follows:
 - Select Low Priority Traffic (Priority 1) or complete the **Priority** field by selecting a priority between 2 and 10 (highest).
 - (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the minimum bandwidth that will be assigned to the Pipe. As long as there is traffic requiring bandwidth in this channel, the bandwidth allocated will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the traffic priority, should there be competition for the bandwidth.
 - (Optional) In the **Maximum Bandwidth (Kbits/sec)** field, enter the maximum bandwidth assigned to the entire Pipe. The total bandwidth of all traffic allocated in this Pipe will not exceed this limit. The **Maximum** checkbox must be open in order to set this value.

- Configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:
 - **Admit by Priority:** Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
 - **Reject:** All packets are dropped. In TCP, an RST packet is sent to the client and the user may see the message Connection Closed by Server.
 - **Drop:** All packets are dropped. The user is disconnected and may see the message Connection timed-out.

NOTE The Drop option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).

5. Click **Save** The new entry is saved in the QoS Catalog.

To define Enhanced QoS for a Line:

NOTE Enhanced QoS should only be used for creating a Enforcement Policy for NetEnforcers or Service Gateways running AOS (Allot Operating System).

1. Select and right-click **QoS** in the Navigation pane and select **New Line Enhanced QoS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the QoS Catalog and select **New Line Enhanced QoS** from the popup menu.

The Line Enhanced QoS Entry Properties dialog is displayed.

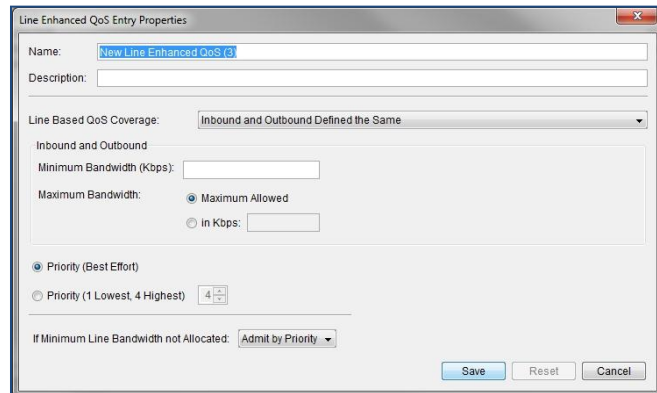


Figure 4-43: Line Enhanced QoS Entry Properties

2. Edit the name and description of the entry, if required.
3. From the **Line-based QoS Coverage** dropdown list select one of the options:

- **Inbound and Outbound Defined the Same:** Define QoS for both the inbound and outbound traffic together. This option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical.
 - **Each Direction Defined Separately:** Define QoS for the inbound and outbound traffic individually (instead of the **General** tab, the **Inbound** tab and the **Outbound** tab appear).
4. In the **Inbound and Outbound** area, define the Quality of Service as follows:
- (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the minimum bandwidth that will be assigned to the Line. As long as there is traffic requiring bandwidth in this channel, the bandwidth allocated will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the traffic priority, should there be competition for the bandwidth.
 - (Optional) In the **Maximum Bandwidth** field, you may opt to assign this Line the maximum Bandwidth allowed, to enter the maximum bandwidth that will be assigned to the Line in Kbits/sec, or to enter a percentage of all the Bandwidth going through the NetEnforcer or Service Gateway to assign to the Line. The total bandwidth of all traffic allocated in this Line will not exceed this limit.

NOTE The ability to define the maximum bandwidth by percentage is disabled and will not appear in the GUI by default. To enable this feature contact Allot Customer Support at support@allot.com.

WARNING In order for the maximum bandwidth by percentage entry to operate correctly on a line, there must some traffic running in at least one of the lines for which bandwidth by percentage is NOT defined. If no traffic is running on any of the other lines, the mechanism will not work. In order to avoid this situation, Allot recommends to assign a minimum QoS catalog entry together with the maximum percentage entry (on the same line).

- Select **Priority (Best Effort)** or complete the **Priority** field by selecting a priority between 1 and 4 (highest). If all objects in the same Enforcement Policy level are set to **Best Effort** there will be no prioritization between objects. The more traffic an object requires, the more bandwidth that will be allocated to it, subject to the amount of free bandwidth available.

NOTE Allot does not recommend using **Priority (Best Effort)** if other elements have **Priorities 1 to 4** assigned. In such situations an element which has been assigned **Priority (Best Effort)** may receive a very low percentage of the available bandwidth.

- Configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:

- **Admit by Priority:** Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
- **Drop:** All packets are dropped. The user is disconnected and may see the message Connection timed-out.

NOTE The Drop option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).

5. Click **Save** The new entry is saved in the QoS Catalog.

Defining QoS for Pipes

Entries in the QoS Catalog that are defined for Pipes are available when assigning QoS to Pipes in the Enforcement Policy Editor.

To define QoS for Pipes:

NOTE If your NetEnforcers or Service Gateways are running AOS (Allot Operating System), you should not use Pipe QoS Catalogs. Instead, use Enhanced QoS Pipe Catalogs.

1. Right click and then select **New Pipe QoS** from the popup menu. The Quality of Service Entry Properties dialog is displayed.

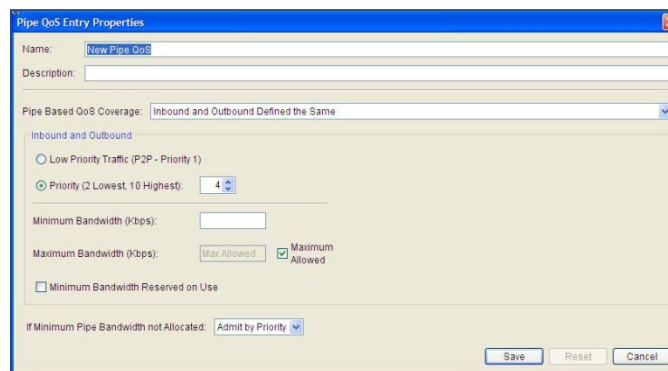


Figure 4-44: Defining QoS for Pipes

2. Edit the name and description of the entry, if required.
3. From the **Pipe-based QoS Coverage** dropdown list select one of the following options:
 - **Both Directions Defined the Same:** Define QoS for both the inbound and outbound traffic together. This option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical. Continue with step 4 below.
 - **Each Direction Defined Separately:** Define QoS for the inbound and outbound traffic individually. Continue with step 4 below.
 - **Half Duplex Pipe:** Define QoS for a half-duplex Pipe.

4. In the **Inbound and Outbound** area, define the Quality of Service as follows:
 - Select Low Priority Traffic (Priority 1) or complete the **Priority** field by selecting a priority between 2 and 10 (highest).
 - (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the minimum bandwidth that will be assigned to the Pipe. As long as there is traffic requiring bandwidth in this channel, the bandwidth allocated will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the traffic priority, should there be competition for the bandwidth.
 - (Optional) In the **Maximum Bandwidth (Kbits/sec)** field, enter the maximum bandwidth assigned to the entire Pipe. The total bandwidth of all traffic allocated in this Pipe will not exceed this limit. The **Maximum** checkbox must be open in order to set this value.
 - Select the **Minimum Bandwidth Reserved on Use** checkbox to reserve the full minimum amount of bandwidth for any future traffic in the Pipe, even when the full minimum bandwidth is not currently required. The actual reservation occurs when the first connection is established within a Pipe.

NOTE **To specify a guaranteed bandwidth for a Pipe, specify the same minimum and maximum bandwidth, for example, 100Kbps.**

5. For a **Half-Duplex Pipe**, define the Quality of Service as follows:
 - In the **Priority** field, select a priority between 1 (lowest) and 10 (highest).
 - In the **Available Bandwidth (Kbits/sec)** field, enter the bandwidth assigned to the entire Pipe. The total bandwidth of all traffic allocated in this Pipe will not exceed this limit.
6. Configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:
 - **Admit by Priority:** Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
 - **Reject:** All packets are dropped. In TCP, an RST packet is sent to the client and the user may see the message **Connection Closed by Server**.
 - **Drop:** All packets are dropped. The user is disconnected and may see the message **Connection timed-out**.

NOTE **The Drop option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).**

7. Click **Save**. The new entry (entries) is saved in the QoS Catalog.

To define Enhanced QoS for Pipes:

NOTE Enhanced QoS should only be used for creating a Enforcement Policy for NetEnforcers or Service Gateways running AOS (Allot Operating System).

1. Select and right-click **QoS** in the Navigation pane and select **New Pipe Enhanced QoS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the QoS Catalog and select **New Pipe Enhanced QoS** from the popup menu.

The Pipe Enhanced QoS Entry Properties dialog is displayed.

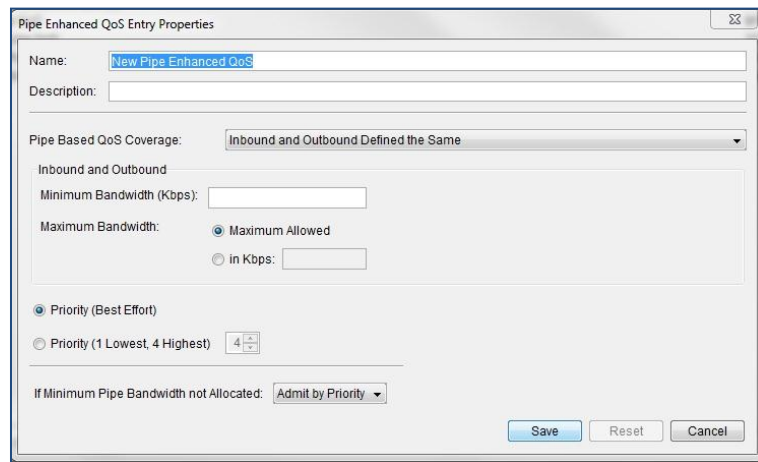


Figure 4-45: Pipe Enhanced QoS Entry Properties

2. Edit the name and description of the entry, if required.
3. From the **Pipe-based QoS Coverage** dropdown list select one of the following options:
 - **Both Directions Defined the Same:** Define QoS for both the inbound and outbound traffic together. This option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical. Continue with step 4 below.
 - **Each Direction Defined Separately:** Define QoS for the inbound and outbound traffic individually. Continue with step 4 below.
4. In the **Inbound and Outbound** area, define the Quality of Service as follows:

- (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the minimum bandwidth that will be assigned to the Pipe. As long as there is traffic requiring bandwidth in this channel, the bandwidth allocated will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the traffic priority, should there be competition for the bandwidth.
- (Optional) In the **Maximum Bandwidth** field, you may opt to assign this Pipe the maximum Bandwidth allowed, to enter the maximum bandwidth that will be assigned to the Pipe in Kbits/sec, or to enter a percentage of all the Bandwidth going through the Line to assign to the Pipe. The total bandwidth of all traffic allocated in this Pipe will not exceed this limit.

NOTE The ability to define the maximum bandwidth by percentage is disabled and will not appear in the GUI by default. To enable this feature contact Allot Customer Support at support@allot.com.

WARNING In order for the maximum bandwidth by percentage entry to operate correctly on a line, there must some traffic running in at least one of the pipes for which bandwidth by percentage is NOT defined. If no traffic is running on any of the other pipes, the mechanism will not work. In order to avoid this situation, Allot recommends to assign a minimum QoS catalog entry together with the maximum percentage entry (on the same pipe).

- Select **Priority (Best Effort)** or complete the **Priority** field by selecting a priority between 1 and 4 (highest). If all objects in the same Enforcement Policy level are set to **Best Effort** there will be no prioritization between objects. The more traffic an object requires, the more bandwidth that will be allocated to it subject to the amount of free bandwidth available.

NOTE Allot does not recommend using **Priority (Best Effort)** if other elements have **Priorities 1 to 4** assigned. In such situations an element which has been assigned **Priority (Best Effort)** may receive a very low percentage of the available bandwidth.

5. Configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:
 - **Admit by Priority:** Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
 - **Drop:** All packets are dropped. The user is disconnected and may see the message **Connection timed-out**.

NOTE The **Drop** option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).

6. Click **Save**. The new entry (entries) is saved in the QoS Catalog.

Defining QoS for Virtual Channels

Entries in the QoS Catalog that are defined for Virtual Channels are available when assigning QoS to Virtual Channels in the Enforcement Policy Editor.

To define QoS for Virtual Channels:

NOTE If your NetEnforcers or Service Gateways are running AOS (Allot Operating System), you should not use Virtual Channel QoS Catalogs. Instead, use Enhanced QoS Virtual Channel Catalogs.

1. Select and right-click **QoS** in the Navigation pane and select **New Virtual Channel QoS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the QoS Catalog and select **New Virtual Channel QoS** from the popup menu.

The Quality of Service Entry Properties dialog is displayed.

Figure 4-46: Virtual Channel QoS Entry Properties

2. Edit the name of the entry, if required.
3. From the **Virtual Channel-based QoS Coverage** dropdown list, select whether you want to define QoS for inbound and outbound together or separately. If you select **Both Directions Defined the Same**, you define QoS for both the inbound and outbound traffic. If you select **Each Direction Defined Separately**, you define QoS for the inbound and outbound traffic individually.

TIP The **Both Directions Defined the Same** option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical.

4. In the **Inbound and Outbound** area, define the Quality of Service as follows:
 - Select Low Priority Traffic (Priority 1) or complete the **Priority** field by selecting a priority between 2 and 10 (highest).
 - (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the minimum bandwidth that will be assigned to the Virtual Channel. As long as there is traffic requiring bandwidth in this channel, the bandwidth will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the traffic priority.
 - (Optional) In the **Maximum Bandwidth (Kbits/sec)** field, confirm that the **Maximum** checkbox is clear and enter the maximum bandwidth assigned to the entire Virtual Channel. The total bandwidth of all traffic in this channel will not exceed this limit.

NOTE To specify a guaranteed bandwidth for a Virtual Channel, specify the same Minimum and Maximum bandwidth, for example, 100Kbps.

TIP When working with traffic that consists of very short connections (one or two packets per connection), it is recommended to specify a minimum bandwidth (such as 50Kbps) per Virtual Channel, rather than specifying a priority (such as 6). This is because using minimum bandwidth per Virtual Channel results in a more effective QoS Enforcement Policy.

5. In the **Connections Allocations** area, select either the **Burst** or **CBR** (Constant Bit Rate) radio button to define how the traffic will be shaped.
6. If you selected **Burst** in step 5, enter the following connection-based information in the **Connections Allocations** area:
 - (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the bandwidth that will be assigned to the connection. As long as there is traffic requiring bandwidth in this connection, the bandwidth will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the virtual channel priority.
 - (Optional) In the **Maximum Bandwidth (Kbits/sec)** field, confirm that the **Maximum** checkbox is clear and enter the maximum bandwidth assigned to the entire connection. The total bandwidth of all traffic in this channel will not exceed this limit.
 - (Optional) In the **Burst Size (Kbits/sec)** field, enter the Burst size for the connection. The Burst size setting allows the traffic to exceed the maximum allotted bandwidth (to burst) for a certain fraction of a second, as long as the traffic does not exceed the maximum during the whole period of one second. For example, if you enter a Burst size of 150Kbps and a maximum of 100Kbps, NetXplorer will allow traffic to be 150Kbps for a fraction of a second, as long as the traffic does not exceed the maximum of 100Kbps.

TIP The Burst Size parameter is useful in environments such as satellite communications, where bandwidth is an expensive resource that must be utilized efficiently.

7. If you selected **CBR** in step 5, configure the following parameters in the **Connections Allocations** area:
 - The **CBR (Constant Bit Rate)** setting provides the ability to smooth traffic. Traffic exits the NetEnforcer or Service Gateway at a constant rate defined in the CBR, as long as the traffic entering The NetEnforcer or Service gateway does so at a rate equal to or greater than the CBR. This ensures smoothing for streaming applications. Enter information in the fields, as follows:
 - In the **Guaranteed Bandwidth (KBits/sec)** field, enter the guaranteed bandwidth for the connection. Guaranteed Bandwidth is the minimum bandwidth assigned to each connection in the Virtual Channel. Guaranteed Bandwidth provides the most predictable results for critical traffic and allows other connections to borrow the bandwidth when it is not in use. Guaranteed Bandwidth always supersedes the needs of other, non-guaranteed connections.

TIP This is useful in multimedia applications, such as Voice over IP.

- In the **Delay (Microseconds)** field, enter the delay value. The default delay value is 1 second and is hidden. However, you can specify any delay, as long as it does not exceed 1 second. If you specify a delay other than the default, you need to know your application's buffering capability. The bigger the buffering capability of your application, the larger the delay you can specify. The optimum delay facilitates a better bandwidth management because it sets a lower limit to the Quality of Service mechanism that decides whether to throw away or keep a packet. The objective of setting the optimum delay is to keep jitter at a minimum (0 at best).
8. Configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:
 - **Admit by Priority:** Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
 - **Reject:** All packets are dropped. In TCP, an RST packet is sent to the client and the user may see the message **Connection Closed by Server**.
 - **Drop:** All packets are dropped. The user is disconnected and may see the message **Connection timed-out**.

NOTE The Drop option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).

- Click **Save**. The new entry is saved in the QoS Catalog.

To define Enhanced QoS for Virtual Channels:

NOTE Enhanced QoS should only be used for creating a Enforcement Policy for NetEnforcers or Service Gateways running AOS (Allot Operating System).

- Select and right-click **QoS** in the Navigation pane and select **New Virtual Channel Enhanced QoS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the QoS Catalog and select **New Virtual Channel Enhanced QoS** from the popup menu.

The Quality of Service Entry Properties dialog is displayed.

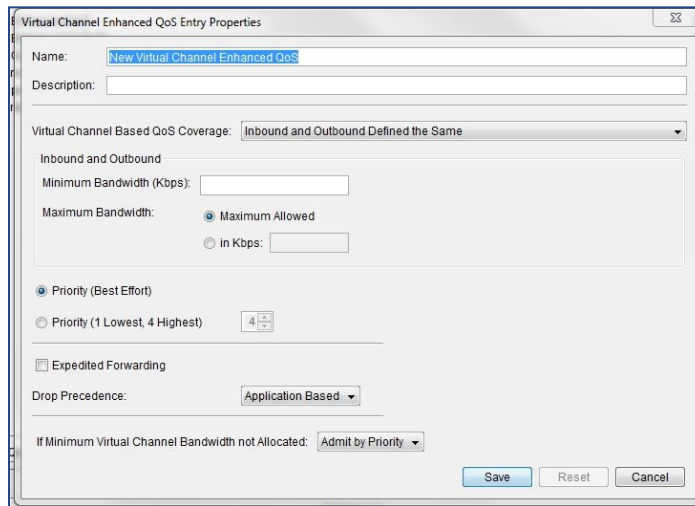


Figure 4-47: Virtual Channel Enhanced QoS Entry Properties

- Edit the name of the entry, if required.
- From the **Virtual Channel-based QoS Coverage** dropdown list, select whether you want to define QoS for inbound and outbound together or separately. If you select **Both Directions Defined the Same**, you define QoS for both the inbound and outbound traffic. If you select **Each Direction Defined Separately**, you define QoS for the inbound and outbound traffic individually.

TIP The **Both Directions Defined the Same** option is normally used in a symmetric environment where inbound and outbound traffic requirements are identical.

- In the **Inbound and Outbound** area, define the Quality of Service as follows:

- (Optional) In the **Minimum Bandwidth (Kbits/sec)** field, enter the minimum bandwidth that will be assigned to the Virtual Channel. As long as there is traffic requiring bandwidth in this channel, the bandwidth will never be lower than this limit. Getting bandwidth above the minimum, however, depends on the traffic priority.
- (Optional) In the **Maximum Bandwidth** field, you may opt to assign this VC the maximum Bandwidth allowed, to enter the maximum bandwidth that will be assigned to the VC in Kbits/sec, or to enter a percentage of all the Bandwidth going through the Pipe to assign to this VC. The total bandwidth of all traffic allocated in this VC will not exceed this limit.

NOTE The ability to define the maximum bandwidth by percentage is disabled and will not appear in the GUI by default. To enable this feature contact Allot Customer Support at support@allot.com

WARNING In order for the maximum bandwidth by percentage entry to operate correctly on a VC, there must some traffic running in at least one of the VCs for which bandwidth by percentage is NOT defined. If no traffic is running on any of the other VCs, the mechanism will not work. In order to avoid this situation, Allot recommends to assign a minimum QoS catalog entry together with the maximum percentage entry (on the same VC).

- Select **Priority (Best Effort)** or complete the **Priority** field by selecting a priority between 1 and 4 (highest). If all objects in the same Enforcement Policy level are set to **Best Effort** there will be no prioritization between objects. The more traffic an object requires, the more bandwidth that will be allocated to it subject to the amount of free bandwidth available.

NOTE Allot does not recommend using **Priority (Best Effort)** if other elements have **Priorities 1 to 4** assigned. In such situations an element which has been assigned **Priority (Best Effort)** may receive a very low percentage of the available bandwidth.

NOTE To specify a guaranteed bandwidth for a Virtual Channel, specify the same **Minimum and Maximum bandwidth**, for example, **100Kbps**.

5. (Optional) Select the **Expedited Forwarding** checkbox when the Virtual Channel is used for jitter or delay sensitive applications such as VoIP. No buffering is used with Expedited Forwarding in order to minimize jitter and delay. All traffic that cannot be allocated the required bandwidth is dropped.
 - Set the bandwidth to be used for the expedited forwarding in the **Expedited Forwarding Bandwidth** field.
 - Click Save. The new Expedited Forwarding QoS entry is saved in the QoS Catalog

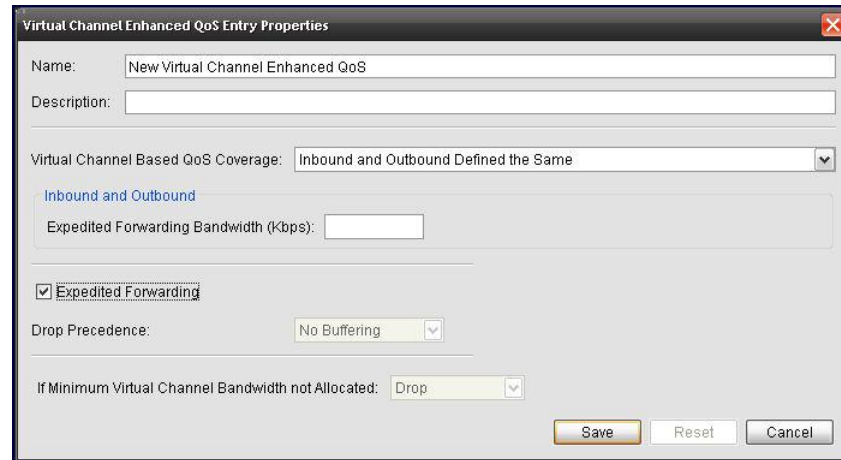


Figure 4-48: Virtual Channel Enhanced QoS Entry Properties – Expedited Forwarding

6. Select a value for **Drop Precedence**, which will dictate the order in which packets will be dropped, if required. If a packet is not transmitted to the network, it will be dropped or buffered. Drop precedence value determines the importance of the packet before making the decision to buffer or not. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

Possible values are No Buffering, Low, Medium, High and Application Based (default).

7. Configure the action to be taken if minimum bandwidth is not allocated, by selecting one of the following options from the designated dropdown list:
 - **Admit by Priority:** Accept the new connection, but do not assign the minimum bandwidth. The new connection gets bandwidth per priority.
 - **Drop:** All packets are dropped. The user is disconnected and may see the message **Connection timed-out**.

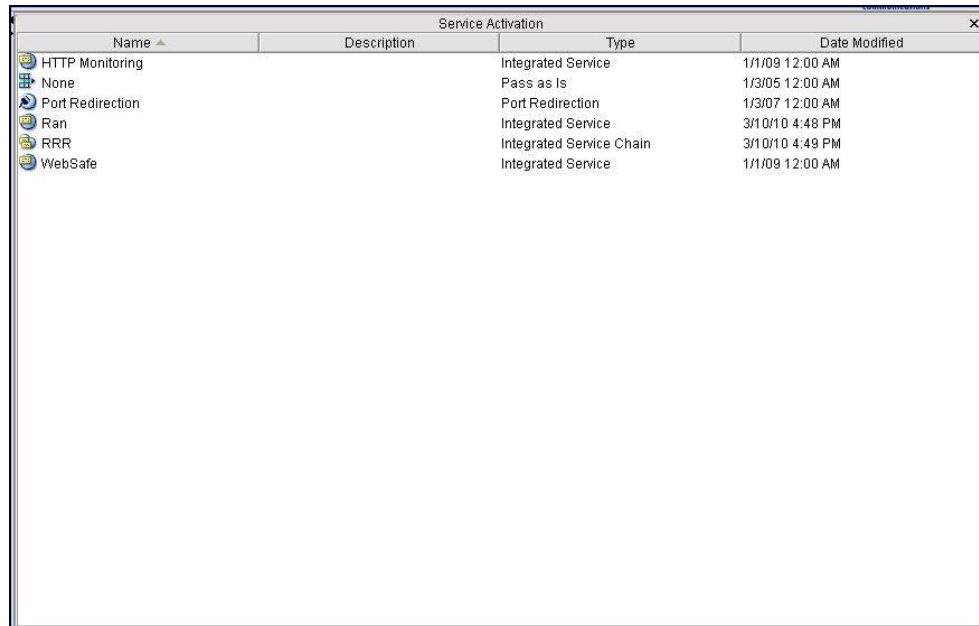
NOTE The Drop option is provided for environments such as UDP where a client does not expect acknowledgements (ACKs).

Click **Save**. The new entry is saved in the QoS Catalog.

Service Activation Catalog

The Service Activation catalog allows the user to define possible traffic or subscriber steering actions that can be used in Enforcement Policy definitions.

Currently redirection to physical port, VLAN, Captive Portal, Local Service or Integrated Service is available, as well as the creation of an Integrated Service Chain.



Name	Description	Type	Date Modified
HTTP Monitoring		Integrated Service	1/1/09 12:00 AM
None		Pass as Is	1/3/05 12:00 AM
Port Redirection		Port Redirection	1/3/07 12:00 AM
Ran		Integrated Service	3/1 0/10 4:48 PM
RRR		Integrated Service Chain	3/1 0/10 4:49 PM
WebSafe		Integrated Service	1/1/09 12:00 AM

Figure 4-49: Service Activation Catalog

Service Activation values can be assigned to any Line, Pipe or VC.

After the relevant entries are created in the Service Activation catalog, the user should create policies and assign to each Enforcement Policy the appropriate Service Activation entry.

Port Redirection

NOTE Port Redirection is only available to those users with the appropriate license key entered to enable the feature.

If you are working with a NetEnforcer or Service Gateway that supports port redirection (e.g: AC-2540), there is no need to define a new catalog entry. The port redirection catalog entry is pre-defined. However, you do need to enable Port Redirection from the Service Activation tab of the device Configuration screen (see 3-23 for details).

Captive Portal

The Captive Portal action is used as part of a rule to redirect traffic to a specific URL. Typically, this action is used in the context of quota based service plans. If a subscriber uses up the assigned daily or monthly quota, that subscriber will be reassigned to a different service plan until the time period is reset, or the subscriber purchases a top-up. Many service providers include a rule in this new service plan which redirects all HTTP traffic to a captive portal. This captive portal can then be used for example to present the subscriber with a new offer to “top up” his existing plan, or perhaps to purchase a new one.

It is possible to have traffic sent to the Captive Portal identified by MSISDN as well as by URI of origin through the use of macros.

For security reasons, the portal may utilize a secured connection (SSL / HTTPS). In such scenarios, the administrator should set the Redirection Protocol to HTTPS.

To define Captive Portal redirection:

1. Select and right-click **Service Activation** in the Navigation pane and select **New Captive Portal** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Activation Catalog and select **New Captive Portal** from the popup menu.

The Captive Portal Entry Properties dialog is displayed.

The screenshot shows a dialog box titled "Captive Portal Entry Properties". It has a close button in the top right corner. The fields are as follows:

- Name:** A text box containing "New Captive Portal".
- Description:** An empty text box.
- URI:** An empty text box.
- Redirection Protocol:** A dropdown menu currently showing "HTTP".
- Http Redirection Fail Action:** A dropdown menu currently showing "Drop".

At the bottom of the dialog are three buttons: "Save", "Reset", and "Cancel".

Figure 4-50: Captive Portal Entry Properties - HTTP

2. Edit the **Name** and **Description** fields, if required.

3. Enter the URI of the portal that traffic is to be redirected to, containing the domain name and the path of the Captive Portal.

Example:

www.captive.com/landpage?ms=

If you wish the traffic sent to the Captive Portal to be identified by MSISDN (subscriber phone number) a macro needs to be added to the URI as follows:

Example:

www.captive.com/landpage?ms={MSISDN}

To identify the original URI of traffic sent to the Captive Portal (so that the traffic may be returned there when released from the Captive Portal) a macro needs to be added to the URI as follows:

Example:

www.captive.com/landpage?ms= {ORIG_URI}

Traffic sent to the Captive Portal may be identified by MSISDN and URI of origin both as follows:

Example:

www.captive.com/landpage?ms={MSISDN}{ORIG_URI}

4. In the **Redirection Protocol** field, select either **HTTP** or **HTTPS** from the drop down menu. If HTTP is selected, you will be prompted to enter an IPv4 or an IPv6 address

The screenshot shows a dialog box titled "Captive Portal Entry Properties". It contains the following fields and controls:

- Name:** Text box containing "New Captive Portal".
- Description:** Empty text box.
- URI:** Empty text box.
- Redirection Protocol:** Dropdown menu with "HTTPS" selected.
- Portal IPv4 address:** Empty text box.
- Portal IPv6 address:** Empty text box.
- Http Redirection Fail Action:** Dropdown menu with "Drop" selected.
- Buttons:** "Save", "Reset", and "Cancel" buttons at the bottom.

Figure 4-51: Captive Portal Entry Properties - HTTPS

NOTE: When using HTTPS, only requests directly designated to the captive portal are supported. An indirect request from the captive portal to other sites is not supported.

- In the **Http Redirection Fail Action** field configure what will be done with non-HTTP traffic passing through this particular pipe or VC (i.e: VoIP traffic). If you select **Pass As Is** from the drop down menu then it will be allowed to pass and reach its destination (i.e: allow VoIP sessions, but redirect HTTP traffic to the active portal). If you select **Drop** then non-HTTP traffic will be blocked.
- Click **Save**. The new entry is saved in the Service Activation Catalog.

NOTES The "redirect to captive portal" action will only redirect the HTTP traffic which is classified into the particular rule to which this action is assigned. If some types of HTTP traffic (e.g: HTTP downloads or particular user defined signatures) are classified into other rules with different actions, then this traffic will not be redirected. Allot therefore recommends that "All Services" be chosen as the service condition for the redirect to captive portal action.

If there is traffic that you do not wish to be redirected to the Captive Portal, be sure that the VCs containing such traffic are above the Captive Portal VC in the Pipe.

The same approach may be used if you wish certain HTTP sites to remain available to users who are being redirected to the Captive Portal. Simply assign the URL you wish to remain accessible to a UDS (see Adding User Defined Signatures on page 4-26), then assign the UDS to a VC above the Captive Portal VC.

VLAN Redirection

To define VLAN redirection:

1. Select and right-click **Service Activation** in the Navigation pane and select **New VLAN Redirection** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Activation Catalog and select **New VLAN Redirection** from the popup menu.

The VLAN Redirection Entry Properties Entry Properties dialog is displayed.

IP	VLAN ID
----	---------

Figure 4-52: VLAN Redirection Entry Properties

2. Edit the **Name** and **Description** fields, if required.

3. Select a **Load Balancing Enforcement Policy** (Hash by Internal IP or Hash by External IP).
4. Select Tracking information in which you can define how the NetXplorer confirms that a service is available on a certain server, including the **Tracking Interface** (In-Band or Management) and the **Tracking Method** (None, Bidirectional Forwarding Detection or Ping).
5. Select the **Rate Limit** you wish on the traffic being redirected (No Limit, Block Server or Rate Limit (kbps), which can be set in the field below).
6. Select a **Service Unavailability Action** in case it is not possible to redirect the traffic to the proper server (Bypass or Drop).
7. Select a **No Server Action**, to tell the NetXplorer what to do with any packets when redirection is not possible (Bypass, Rehash by Available Servers or Drop).
8. Set the **Number of Redundant Servers**, as well as the **Tracking Interval** (The length of time, in seconds, that NetXplorer waits between attempts to contact a server) and **Tracking Timeout** (The length of time, in seconds, that NetXplorer waits before concluding that a server is down).
9. Under Servers, click **Add** to enter the IP and VLAN ID of the target VLAN server.



Figure 4-53: Add VLAN Server

10. Click **Save**. The new entry is saved in the Service Activation Catalog.

Integrated Services

An Integrated Service is made up of one or more Local Services, each of which is assigned to a specific NetEnforcer or Service Gateway. Once all required Local Services have been added to an Integrated Service, the Integrated Service may then be used in Policies.

To define a Local Service:

NOTE This feature is only available on NetEnforcers or Service Gateways running AOS (Allot Operating System). In addition, a traffic steering license is required if traffic is to be steered to external services.

1. Select and right-click **Service Activation** in the Navigation pane and select **New Local Service** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Activation Catalog and select **New Local Service** from the popup menu.

The Local Service Entry Properties dialog is displayed.

Name	Server Deployment
------	-------------------

Figure 4-54: Local Service Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. Select the Device Name the Local Service will be assigned to.

4. Select the **Service Type** (Generic Transparent Redirection, Generic Proxy Redirection, Generic Mirroring, MediaSwift or ServiceProtector).
5. Select the **Service Admin Status** (Active or Inactive).
6. Select a **Load Balancing Method** (Cyclic, Hash by Internal IP or Hash by External IP). Cyclic load balancing is sometimes referred to as “round-robin”
7. Select a **Server Failure Action**, to tell the NetXplorer what to do with any packets when redirection to the selected server is not possible (Bypass, Re-dispatch to Other Server or Block).
8. Select a **Service Unavailability Action** in case there is no possible server to redirect the traffic to (Bypass or Block).
9. Select Tracking information in which you can define how the NetXplorer confirms that a service is available on a certain server, including the **Tracking Interface** (In-Band or Management) and the **Tracking Method** (None, Bidirectional Forwarding Detection, Ping or HTTP Request). If you selected HTTP Request enter a Port number in the relevant field.

NOTE When adding a MediaSwift Local Service, the Tracking Method is automatically set to Bidirectional Forwarding Detection and when adding a ServiceProtector the Tracking Method is automatically set to None. These options cannot be changed by the user.

10. Enter a Local IP Address for use in tracking service availability.
11. Set the **Tracking Interval** (The length of time, in seconds, that NetXplorer waits between attempts to contact a server) and **Tracking Retires** (How many times the NetXplorer will attempt to contact a server before concluding that a server is down).
12. Select a **Server Capacity Reached Action**, to be performed when the maximum redirection capacity has been exceeded (Bypass, Redispatch or Block), the **Minimum Active Servers** and the **Flow Direction**. The feature will be implemented in future releases.
13. Under Servers, click **Add** to enter the details of any target servers.

NOTE Up to 128 servers may be added per Service.

General

Name:

Admin Status:

Deployment:

Server Slot:

Network Configuration

	Internal	External
Mac:	<input type="text" value=": : : : :"/>	<input type="text" value=": : : : :"/>
IPv4:	<input type="text" value=" . . ."/>	<input type="text" value=" . . ."/>
IPv6:	<input type="text"/>	<input type="text"/>

Interface Connectivity

	Internal	External
SFC Port Id/Line:	<input type="button" value="SB_6_L5"/>	<input type="button" value="SB_6_L5"/>
VLAN Tag IPv4:	<input type="button" value="1"/>	<input type="button" value="1"/>
VLAN Tag IPv6:	<input type="button" value="1"/>	<input type="button" value="1"/>

Alternative Connectivity

	Internal	External
SFC Port Id/Line:	<input type="button" value="SB_6_L5"/>	<input type="button" value="SB_6_L5"/>

Figure 4-55: Edit Server

NOTE The fields which appear in this dialog will be dependent on the Deployment options chosen

- Enter a **Name** for the server and set the **Admin Status** to Active or Inactive.
- Set the **Deployment** for Internal, External Switched or External Direct.

- The **Management IP** is entered to enable communication with the NMS.
 - If the **Deployment** is set to Internal, then the Server Slot (9-14) needs to be defined.
 - Set **Network, Interface** and **Alternative Connectivity** (if relevant) for both the Internal and External connection on the server.
 - **Monitoring IP** is used for server tracking and is relevant only for servers whose **Deployment** is set to External Switched or External Direct. It is not relevant when the tracking method is set to Bidirectional Forwarding Detection.
 - MediaSwift Servers are transparent devices on the network so **Mac Internal** and **External** are not supported in these cases.
14. Click **Save**. The new entry is saved in the Service Activation Catalog.

To define an Integrated Service:

NOTE This feature is only available on NetEnforcers or Service Gateways running AOS (Allot Operating System). In addition, a traffic steering license is required if traffic is to be steered to external services.

1. Select and right-click **Service Activation** in the Navigation pane and select **New Integrated Service** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Activation Catalog and select **New Integrated Service** from the popup menu.

The Integrated Service Entry Properties dialog is displayed.

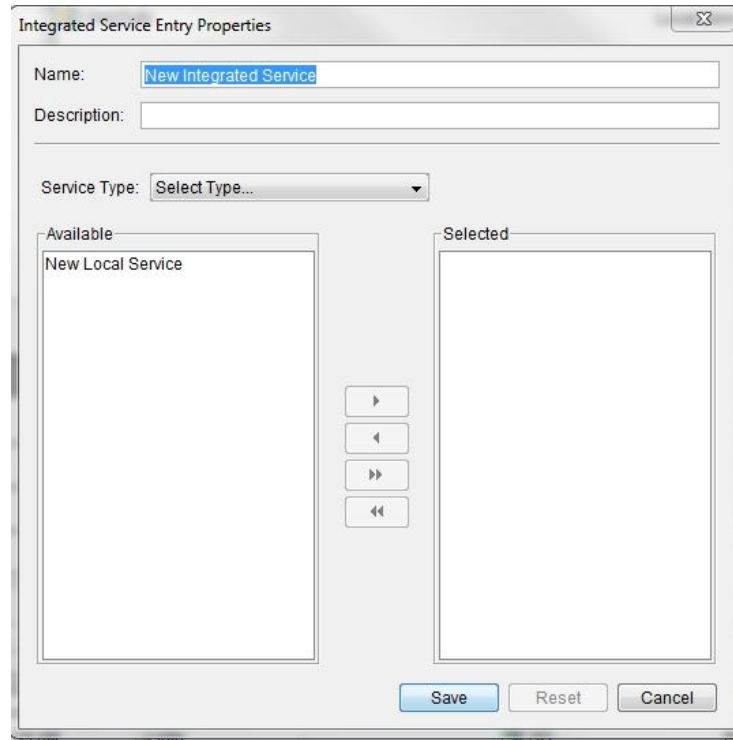


Figure 4-56: Integrated Service Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. Select the **Service Type** (Generic Transparent Redirection, Generic Proxy Redirection, Generic Mirroring, MediaSwift or ServiceProtector).
4. Select the Local Services you wish to add from the **Available** list. Use the arrow keys to move them to the **Selected** list.
5. Click **Save**. The new entry is saved in the Service Activation Catalog and may be used in Policies.

To define an Integrated Service Chain:

An Integrated Service Chain is an optional series of Integrated Services which occur in order and may be assigned to a Enforcement Policy like any other Integrated Service

1. Select and right-click **Service Activation** in the Navigation pane and select **New Integrated Service Chain** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Activation Catalog and select **New Integrated Service Chain** from the popup menu.

The Integrated Service Chain Entry Properties dialog is displayed.

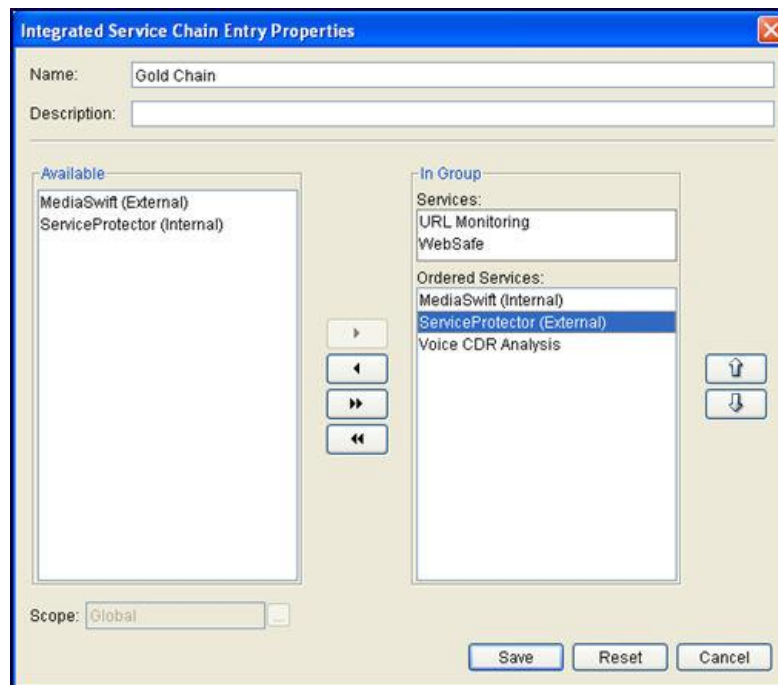


Figure 4-57: Integrated Service Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. Highlight any Integrated Services in the **Available** list and use the arrow keys in the middle of the dialog to transfer them to the In Group list.

NOTE Local Services may not be added directly to an Integrated Service Chain. They must first be added to an Integrated Service then that Integrated Service can be added to an Integrated Service Chain.

4. Within the In Group list, those Integrated Service listed in the Services field are always active and do not need to be put in any order.
5. Using the arrow keys on the left hand side of the dialog, you may adjust those services in the Ordered Services field, to decide which of them take effect first in the chain. The lowermost service in the list will be the first implemented.

NOTE When added to a Service Chain, WebSafe will always be implemented first, regardless of the order.

6. You may set the **Scope** of the Integrated Service Chain in the lower left corner of the dialog box. Click the **Browse** button to open the Scope dialog box and select if you wish the Integrated

Service Chain to be global, available to all devices on the network, or only a specific Device.

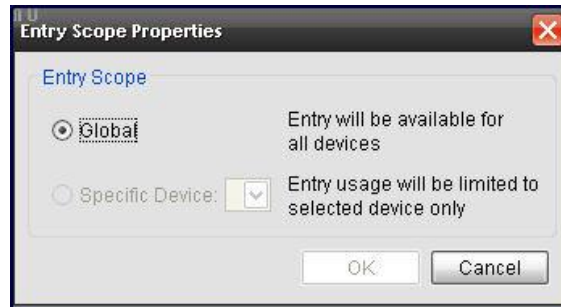


Figure 4-58: Integrated Service Entry Properties

7. Click **Save**. The new entry is saved in the Service Activation Catalog.

DoS Catalog

The DoS (Denial of Service) Catalog enables you to control the number of connections and the rate of connections established per Enforcement Policy.

A sample DoS Catalog is shown below:

The screenshot shows a window titled "DoS" with a table of entries. The table has two columns: "Name" and "Date Modified". The entries are as follows:

Name	Date Modified
ddos	1/22/06 8:04 AM
Dnum60Kcer2K	1/20/06 11:19 AM
dos4	1/20/06 10:35 AM
dos5	1/20/06 10:35 AM
Ignore dos	1/2/05 10:00 PM
MAXcnx20000	1/22/06 8:17 AM

Figure 4-59: DoS Catalog

Each entry indicates the maximum number of connections that can be established, the maximum rate of connections established and what action should be taken if the maximum establishment exceeded or when the maximum of connections exceeded.

You can control the connection rates by setting specific values and assigning the entry to a Line, Pipe or Virtual Channel. For example, you can limit the number of simultaneous connections for specific users by creating a catalog entry and applying the Enforcement Policy to those users.

To define a DoS entry:

1. Select and right-click **DoS** in the Navigation pane and select **New DoS** from the popup menu.

OR

In the Application Details pane, right-click an entry in the DoS Catalog and select **New DoS** from the popup menu.

The DoS Entry Properties dialog is displayed.

Figure 4-60: DoS Entry Properties

2. Edit the name of the entry in the **Name** field, if required.
3. Enter the maximum number of concurrent connections that can be established in the **Maximum Number of Connections** field.
4. Enter the number of connections that can be established per second in the **Maximum Connections Establishment Rate** field.
5. Select the action to be taken if the maximum number of connections or maximum rate of establishing new connections is exceeded from the designated dropdown list:
 - **Reject:** All packets are dropped. In TCP, an RST packet is sent to the client and the user may see the message **Connection Closed by Server**.
 - **Drop:** All packets are dropped. The user is disconnected and may see the message **Connection timed-out**.
6. Click **Save**. The new entry (entries) is saved in the DoS Catalog.

Quota Catalog

NOTE **Quota is only available to those users with the Subscriber Management Platform (SMP) installed and the appropriate license key entered to enable the feature.**

Quotas are usually defined to work in tandem with Service Plans. Defining and enforcing Quotas without different QoS minimum and maximum bandwidths parameters being used in combination only offers restrictive opportunities for SPs to optimize their ARPU. A Quota can be defined based on Volume or based on Time.

For example, if a Monthly quota of 40Gb is selected (based on a Service Plan that also offers a QoS speed of 256 Kbs up to 40 Mb maximum), is exceeded on the 19th day of the month, the Service Plan would only allow the subscriber to have internet access to a maximum of 64 Kbps from the 20th to the 30th of the month. On the 1st of the next month, the subscriber would return to the 256 Kbps speed until the 40 Mb quota is reached.

The Quota Entry Properties dialog default settings are as follows:

- Monthly period starting on the first day of the month
- Quota covering a full month
- Direction of file flow – both in (download) and out (upload)

A Quota Entry may be based on the volume of traffic, or the amount of time the quota lasts.

To define a Volume Based Quota entry:

1. Select and right-click **Quota** in the Navigation pane and select **New Quota** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Quota Catalog and select **New Quota** from the popup menu.

The Quota Entry Properties dialog is displayed.

Figure 4-61: Volume Based Quota Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. Select the **Volume Based** radio button.
4. Enter the time period to be covered by the Quota, **Monthly** or **Daily**.
5. If **Monthly** is selected the following parameters can be selected in the Details area.
 - **Start at X of Every Month** – Select the date in the month when the Quota first takes effect.
 - **Quota Covers the Full Month** – The Quota covers the entire month.
 - **Quota Covers X Through X of Each Week** – Select the days of the week that the Quota is applied (i.e. Monday through Friday).
6. If **Daily** is selected the following parameters can be selected in the Details area.
 - **Quota Covers the Full Day** – The Quota covers the entire day.

- **Quota Covers X Through X of Day** – Select the hours of the day that the Quota is applied (i.e. 8:00 AM through 5:00 PM).
7. Select the direction of traffic the Quota applies to from the drop down menu: **Both (In + Out)**; **Incoming Only**; or **Outgoing Only**.
 8. Enter the amount of traffic the Quota covers, in GBytes, Mbytes or Kbytes.
 9. Click **Save**. The new entry (entries) is saved in the Quota Catalog.

To define a Time Based Quota entry:

1. Select and right-click **Quota** in the Navigation pane and select **New Quota** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Quota Catalog and select **New Quota** from the popup menu.

The Quota Entry Properties dialog is displayed.

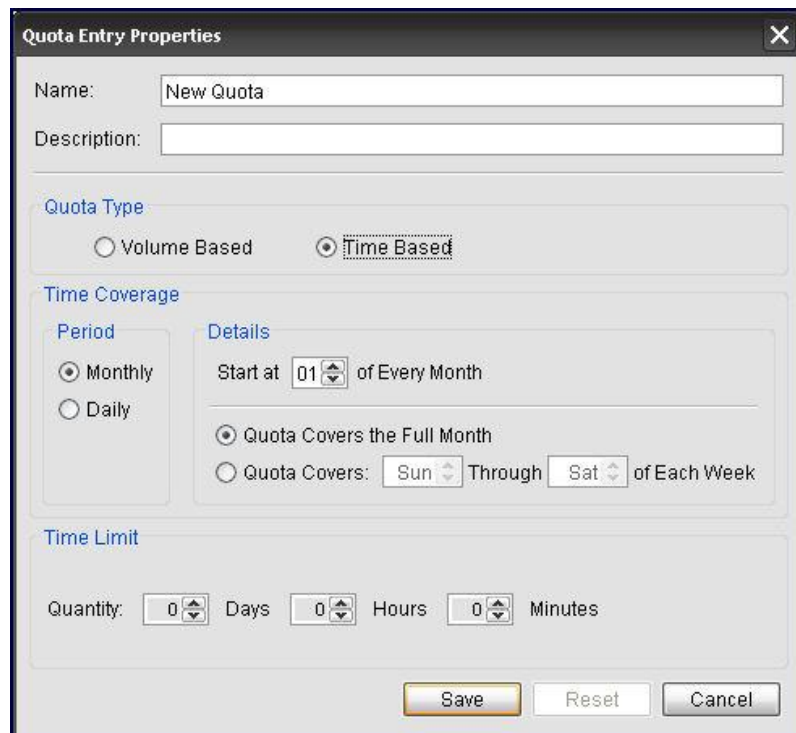


Figure 4-62: Time Based Quota Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. Select the **Time Based** radio button.

4. Enter the time period to be covered by the Quota, **Monthly** or **Daily**.
5. If **Monthly** is selected the following parameters can be selected in the Details area.
 - **Start at X of Every Month** – Select the date in the month when the Quota first takes effect.
 - **Quota Covers the Full Month** – The Quota covers the entire month.
 - **Quota Covers X Through X of Each Week** – Select the days of the week that the Quota is applied (i.e. Monday through Friday).
6. If **Daily** is selected the following parameters can be selected in the Details area.
 - **Quota Covers the Full Day** – The Quota covers the entire day.
 - **Quota Covers X Through X of Day** – Select the hours of the day that the Quota is applied (i.e. 8:00 AM through 5:00 PM).
7. In the Time Limit area, enter the maximum amount of time the Quota can cover, in Days, Hours and Minutes.
8. Click **Save**. The new entry (entries) is saved in the Quota Catalog.

Daily Quota Time Synchronization

Allot's NetXplorer Server settings allow you to define then deploy peak and other hour ranges based on GMT synchronization to the "local" time where the SMP Server are located.

Quota Enforcement Thresholds

Allot's Servers read and collate data every 5 minutes and the maximum time between subscribers reaching and then violating their defined quota is 5 minutes.

Service Plan Catalog

NOTE **Service Plans are only available to those users with the Subscriber Management Platform (SMP) installed and the appropriate license key entered to enable the feature.**

Service plans (with or without quotas) contain QoS Catalog entries that quickly and easily define key parameters for subscriber accounts, for example, minimum and maximum bandwidth.

Service Plans may be created for Pipes or for VCs, depending upon the structure of Enforcement Policy tables. It is possible to define a Pipe Service Plan, where each VC is defined in the Pipe Service Plan and handles a separate application, or to create individual VC Service Plans for each VC.

To create a Pipe Service Plan:

1. Select and right-click **Service Plan** in the Catalogs tab of the Navigation pane and select **New Pipe Service Plan** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Plan Catalog and select **New Pipe Service Plan** from the popup menu.

OR

In the Actions menu, select **New Catalog Entry > New Pipe Service Plan**.

The Pipe Service Plan Entry Properties dialog is displayed open to the General tab.

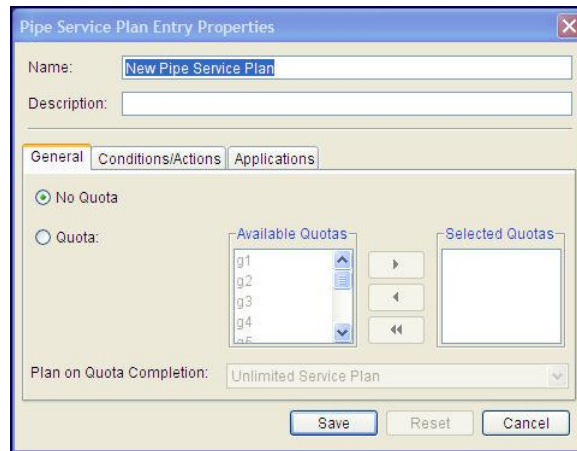


Figure 4-63: Pipe Service Plan Entry Properties - General

2. Edit the **Name** and **Description** fields, if required.
3. In the General tab, define the quota capacity of the Service Plan. You can also select a different service plan that the Enforcement Policy editor enables when the defined Quota threshold is reached.

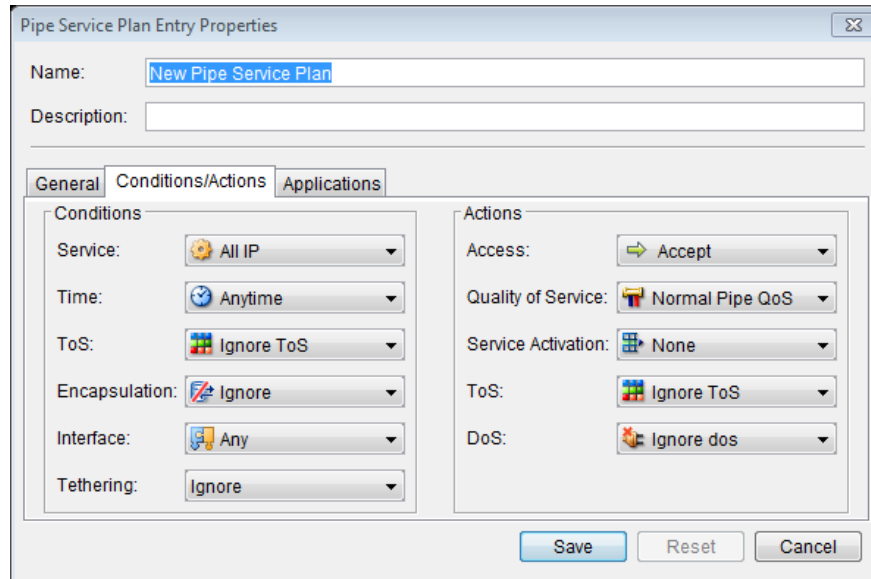


Figure 4-64: Pipe Service Plan Entry Properties – Conditions/Actions

4. Open the Conditions/Actions tabs to set Conditions and Actions for the Service Plan.
 - Conditions can be set for the Pipe as follows:
 - **Service:** Defines the protocols relevant to a connection. Protocols may be TCP and UDP IP type, non-TCP and non-UDP type or non-IP type. TCP and UDP IP protocols are defined based on port type. HTTP protocols may include content definitions, such as specific Web directories, pages, or URL patterns. The default value is **All IP** which covers all protocols.
 - **Time:** Defines the time period during which the traffic is received. For example daily between 8.00 AM and 6.00 PM, Sundays between 12.00 AM and 12.00 PM or on the 1st and 15th of the month. The default value is **Anytime** which covers traffic at any time.
 - **ToS:** Defines the ToS byte contained in the IP headers of the traffic. The default value is **Any** which covers any ToS value.
 - **Encapsulation:** Defines VLAN traffic classification according to VLAN ID (VLAN Identifier) tags, consisting of 12 bits, and according to tagging priority bits, consisting of three bits. Alternatively can be used to classify by GRE tunnel.

- **Interface:** Defines the physical interface or group of interfaces on the In-line platform.
- **Tethering:** Defines whether the rule classifies tethered traffic (set to yes), non-tethered traffic (set to no) or classifies traffic irrespective of whether it is tethered or not (set to ignore, the default value)
- Actions can then be set for when the Conditions of the Service Plan are met, as follows:
 - **Access:** This action determines the access given to traffic. If the Access Control for a Line, Pipe or Virtual Channel is specified as **Reject** or **Drop**, all traffic meeting the Conditions of the Line, Pipe or Virtual Channel is dropped and no other Quality of Service or Connection Control actions are applied. If the Access Control for a Line, Pipe or Virtual Channel is specified as **Bypass** all traffic meeting the Conditions of the Line, Pipe or Virtual Channel goes through but no Quality of Service is applied to it and it does not appear in any monitoring graphs.
 - **Quality of Service:** This action determines the QoS given to traffic. The default Quality of Service action for Lines, Pipes or Virtual Channels is **Normal Priority**, which has Level 4 priority, no bandwidth definitions, no ToS marking and no connection limitations.
 - **Service Activation:** This action steers the traffic to a pre-defined integrated service, Port or URL, when possible.
 - **ToS:** The ToS is a byte in the IP header of a packet that contains information about routing recommendations. NetEnforcer classifies traffic based on the ToS byte marking contained in the IP headers of the packets passing through it.
 - **DoS (Denial of Service):** This action enables you to limit the frequency and number of connections, thereby giving a level of protection from attacks on the network resources (such as internally connected servers). NetXplorer analyzes the distribution of traffic across the various protocols and ports, and admits or drops excess traffic when predefined thresholds have been exceeded.

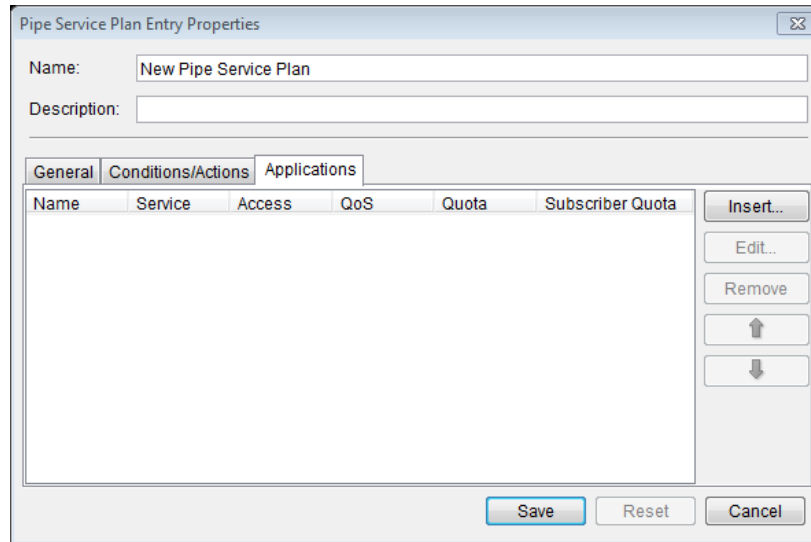


Figure 4-65: Pipe Service Plan Entry Properties – Applications

5. Open the Applications tab to set Applications for the Service Plan.

You add applications to a Pipe Service Plan by inserting Virtual Channel (VC) rows into the Applications area of the Pipe Service Plan Properties dialog:

Using the Arrow buttons in the Applications tab you can:

- Insert applications in the Applications table above or below an existing row.
 - Edit application properties.
 - Remove applications from the table.
 - Move application up and down in the table.
6. Enter the details of Application based VCs into a Pipe Service Plan by clicking Insert in the Applications area to open the Application Properties dialog (see Figure 4-66)

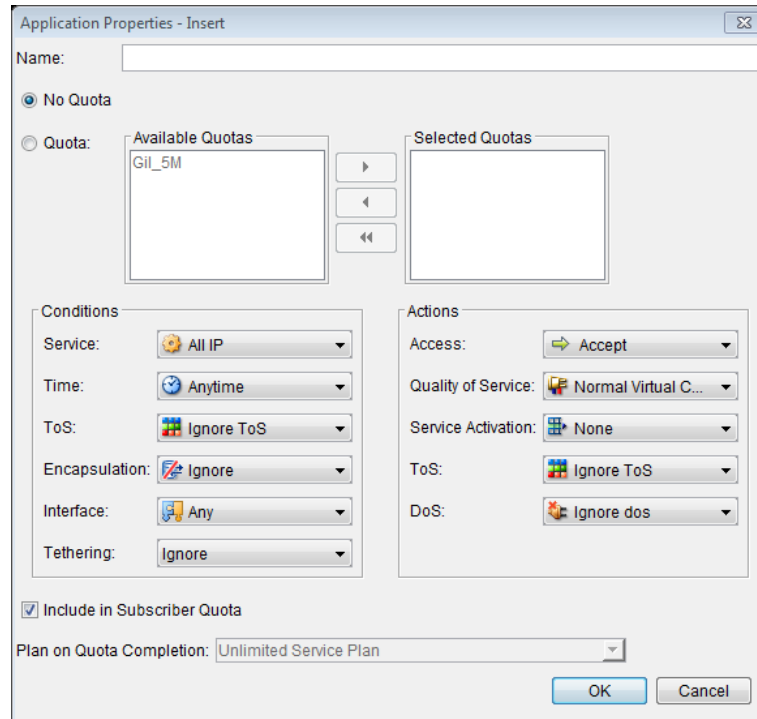


Figure 4-66: Service Plan Application Properties

For details concerning defining Quota, Conditions and Actions for the VC, see steps 3 and 4.

The **Include in Subscriber Quota** checkbox is selected by default. Uncheck this box if you do not wish this application's traffic to be counted against a subscriber's quota.

7. Click **OK** to save the Pipe Service Plan to the Service Plan catalog.

To create a VC Service Plan:

1. Select and right-click **Service Plan** in the Catalogs tab of the Navigation pane and select **New VC Service Plan** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Service Plan Catalog and select **New VC Service Plan** from the popup menu.

OR

In the Actions menu, select **New Catalog Entry > New VC Service Plan**.

The VC Service Plan Entry Properties dialog is displayed open to the General tab.

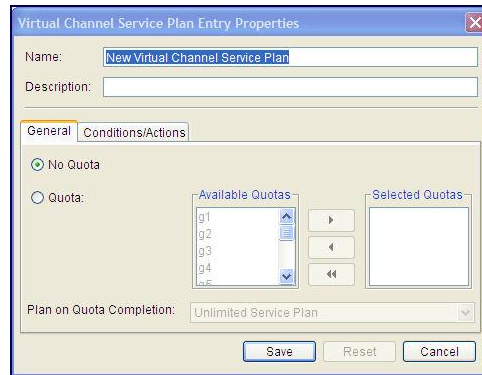


Figure 4-67: VC Service Plan Entry Properties - General

2. Edit the **Name** and **Description** fields, if required.
3. In the General tab, define the quota capacity of the Service Plan. You can also select a different service plan that the Enforcement Policy editor enables when the defined Quota threshold is reached.

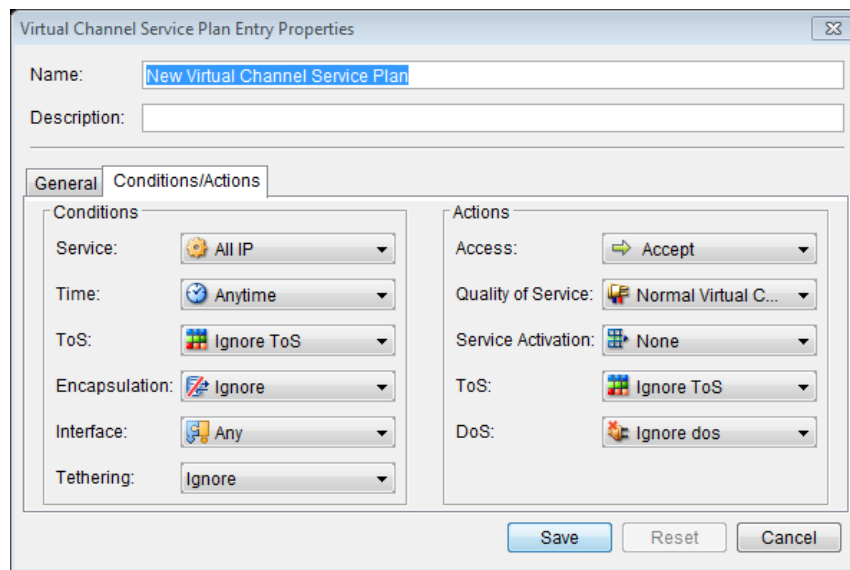


Figure 4-68: VC Service Plan Entry Properties – Conditions/Actions

4. Open the Conditions/Actions tabs to set Conditions and Actions for the Service Plan.
 - Conditions can be set for the VC as follows:
 - **Service:** Defines the protocols relevant to a connection. Protocols may be TCP and UDP IP type, non-TCP and non-UDP type or non-IP type. TCP and UDP IP protocols are defined based on port type. HTTP protocols may include content definitions, such as specific Web

directories, pages, or URL patterns. The default value is **All IP** which covers all protocols.

- **Time:** Defines the time period during which the traffic is received. For example daily between 8.00 AM and 6.00 PM, Sundays between 12.00 AM and 12.00 PM or on the 1st and 15th of the month. The default value is **Anytime** which covers traffic at any time.
- **ToS:** Defines the ToS byte contained in the IP headers of the traffic. The default value is **Any** which covers any ToS value.
- **Encapsulation:** Defines VLAN traffic classification according to VLAN ID (VLAN Identifier) tags, consisting of 12 bits, and according to tagging priority bits, consisting of three bits. Alternatively can be used to classify by GRE tunnel.
- **Interface:** Defines the physical interface or group of interfaces on the In-line platform.
- **Tethering:** Defines whether the rule classifies tethered traffic (set to yes), non-tethered traffic (set to no) or classifies traffic irrespective of whether it is tethered or not (set to ignore, the default value)
- Actions can then be set for when the Conditions of the Service Plan are met, as follows:
 - **Access:** This action determines the access given to traffic. If the Access Control for a Line, Pipe or Virtual Channel is specified as **Reject** or **Drop**, all traffic meeting the Conditions of the Line, Pipe or Virtual Channel is dropped and no other Quality of Service or Connection Control actions are applied. If the Access Control for a Line, Pipe or Virtual Channel is specified as **Bypass** all traffic meeting the Conditions of the Line, Pipe or Virtual Channel goes through but no Quality of Service is applied to it and it does not appear in any monitoring graphs.
 - **Quality of Service:** This action determines the QoS given to traffic. The default Quality of Service action for Lines, Pipes or Virtual Channels is **Normal Priority**, which has Level 4 priority, no bandwidth definitions, no ToS marking and no connection limitations.
 - **Service Activation:** This action steers the traffic to a pre-defined integrated service, Port or URL, when possible.
 - **ToS:** The ToS is a byte in the IP header of a packet that contains information about routing recommendations. NetEnforcer classifies traffic based on the ToS byte marking contained in the IP headers of the packets passing through it.

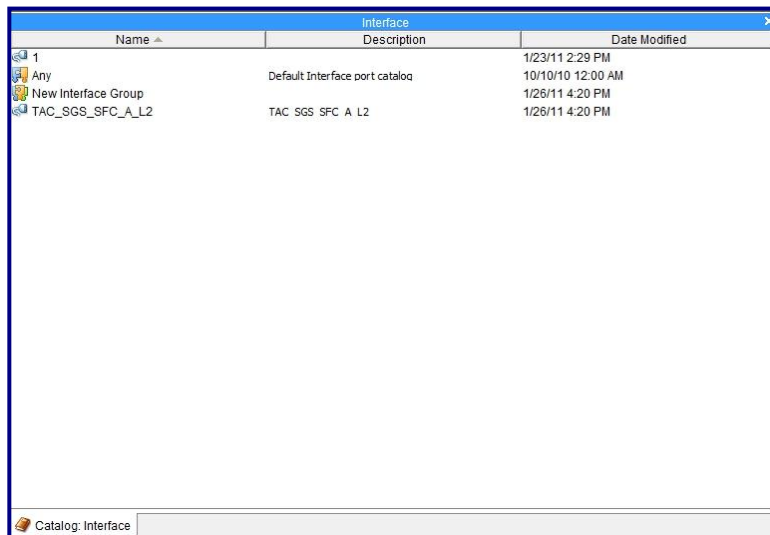
- **DoS (Denial of Service):** This action enables you to limit the frequency and number of connections, thereby giving a level of protection from attacks on the network resources (such as internally connected servers). NetXplorer analyzes the distribution of traffic across the various protocols and ports, and admits or drops excess traffic when predefined thresholds have been exceeded.

Interface Catalog

The Interface Catalog enables you to define individual physical ports or groups of ports (called Interface Groups) on your NetEnforcer or Service Gateway for use in policies.

NOTE This Catalog is only available on NetEnforcer and Service Gateways running AOS11.2 and after.

A sample Interface Catalog is shown below:



Name	Description	Date Modified
1	Default Interface port catalog	1/23/11 2:29 PM
Any		10/10/10 12:00 AM
New Interface Group		1/26/11 4:20 PM
TAC_SGS_SFC_A_L2	TAC SGS SFC A L2	1/26/11 4:20 PM

Figure 4-69: Interface Catalog

To define a physical port:

1. Select and right-click Interface in the Navigation pane and select **New Physical Port** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Interface Catalog and select **New Physical Port** from the popup menu.

OR

Select **Interface** in the Navigation pane when Catalogs are displayed and select **New Physical Port** from the Actions menu.

The Physical Port Entry Properties dialog is displayed.

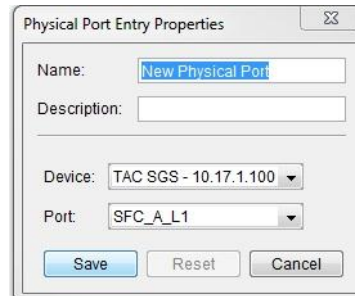


Figure 4-70: Physical Port Entry Properties

2. Select the NetEnforcer or Service Gateway you wish to define a port on in the **Device** drop-down menu.
3. Select the individual port on the selected NetEnforcer or Service Gateway in the **Port** drop-down menu.
4. Click **Save**. The new entry is saved in the Interface Catalog.

To define an interface group:

1. Select and right-click Interface in the Navigation pane and select **New Interface Group** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Interface Catalog and select **New Interface Group** from the popup menu.

OR

Select **Interface** in the Navigation pane when Catalogs are displayed and select **New Interface Group** from the Actions menu.

The Interface Group Entry Properties dialog is displayed.

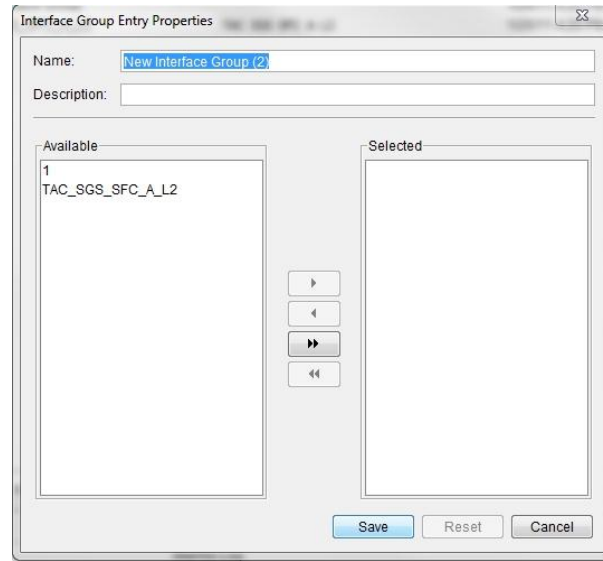


Figure 4-71: Interface Group Entry Properties

2. Select previously defined physical in the Available list and use the arrow keys to move them into the Selected list.
3. Click **Save**. The new entry is saved in the Interface Catalog.

Charging Application Catalog

NOTE Charging Applications are only available to those users with the **Subscriber Management Platform (SMP)** installed and the appropriate **ChargeSmart** license key entered to enable the feature. For more information contact **Allot Customer Support** at support@allot.com.

Charging Applications contain individual Services or Groups of Services which may be assigned to Charging Plans.

For more information about defining Charging Policies in NetXplorer, see the **SMP User Guide**.

Name	Description	Date Modified
App1		4/6/11 6:09 PM
App10		4/10/11 2:36 PM
App11		4/10/11 2:36 PM
App12		4/10/11 2:37 PM
App13		4/10/11 2:37 PM
App14		4/10/11 2:37 PM
App15		4/10/11 2:38 PM
App16		4/10/11 2:38 PM
App17		4/11/11 11:37 AM
App2		4/6/11 2:07 PM
App3		4/6/11 2:07 PM
App4		4/10/11 2:35 PM
App5		4/10/11 2:35 PM
App6		4/10/11 2:35 PM
App7		4/10/11 2:35 PM
App8		4/10/11 2:36 PM
App9		4/10/11 2:36 PM
doc test		5/3/11 3:53 PM
Session	Session level charging	2/8/11 10:00 AM

Figure 4-72: Charging Application Catalog

To create a Charging Application:

1. Select and right-click **Charging Application** in the Catalogs tab of the Navigation pane and select **New Charging Application** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Charging Application Catalog and select **New Charging Application** from the popup menu.

OR

In the Actions menu, select **New Catalog Entry > New Charging Application**.

The Charging Application Entry Properties dialog is displayed.

Figure 4-73: Charging Application Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. In the Application ID field, enter the unique ID number that will identify this Charging Application. The number selected must be coordinated with the other elements of your online and offline charging solution.
4. Select an Offline Unit from the drop down menu, defining on what basis the user will be charged for this Charging Application. Available values are **Volume**, **Time** or **Volume and Time**. This is only relevant in Offline Charging, as in Online Charging this value is defined by an external Server.
5. Add Services to the Charging Application by clicking the **Add** button.

The Add Application Service Items dialog is displayed.

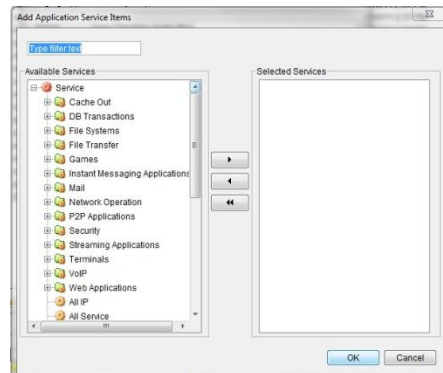


Figure 4-74: Add Application Service Items

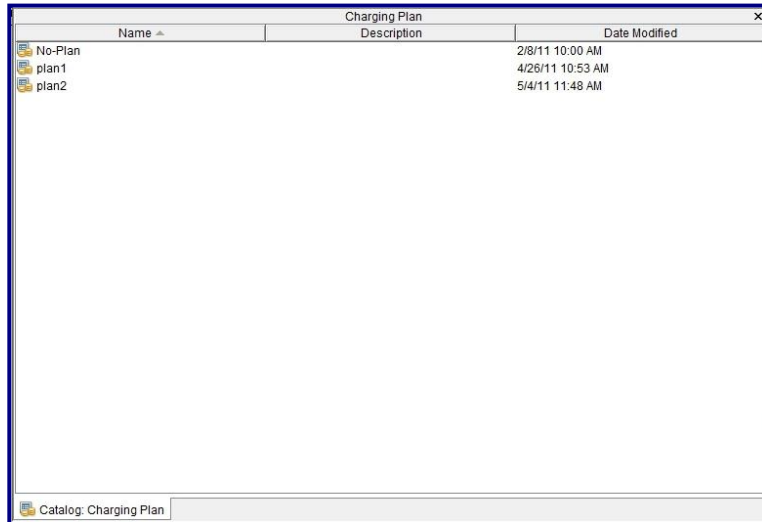
6. Use the Arrow buttons to move Services or Service Groups from the Available Services list to the Selected Services list. Click **OK** to return to the Charging Application Entry Properties dialog.
7. Click Save to save the Charging Application.

Charging Plan Catalog

NOTE Charging Plans are only available to those users with the Subscriber Management Platform (SMP) installed and the appropriate ChargeSmart license key entered to enable the feature. For more information contact Allot Customer Support at support@allot.com.

Charging Plans are the building blocks used to create Online and Offline Charging Policies. Each Charging Plan can contain any number of Charging Applications, defining what Services are covered by the Plan.

For more information about defining Charging Policies in NetXplorer, see the **SMP User Guide**.



Name	Description	Date Modified
No-Plan		2/8/11 10:00 AM
plan1		4/26/11 10:53 AM
plan2		5/4/11 11:48 AM

Figure 4-75: Charging Plan Catalog

The Charging Plan catalog contains one default Charging Plan called No-Plan that may not be edited. The No-Plan Charging Plan contains no charging information.

To create a Charging Plan:

1. Select and right-click **Charging Plan** in the Catalogs tab of the Navigation pane and select **New Charging Plan** from the popup menu.

OR

In the Application Details pane, right-click an entry in the Charging Plan Catalog and select **New Charging Plan** from the popup menu.

OR

In the Actions menu, select **New Catalog Entry > New Charging Plan**.

The Charging Plan Entry Properties dialog is displayed.

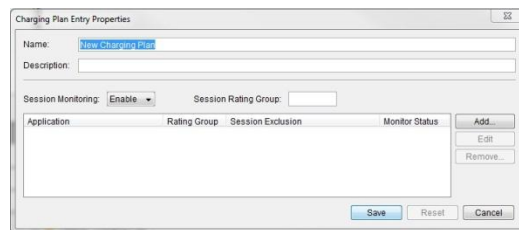


Figure 4-76: Charging Plan Entry Properties

2. Edit the **Name** and **Description** fields, if required.
3. From the **Session Monitoring** drop down menu, you may Enable or Disable the monitoring of this Charging Plan.
4. In the Session Rating field, enter the unique ID number that will identify this Charging Plan. The number selected must be coordinated with the other elements of your online and offline charging solution.
5. Add Charging Applications to the Charging Plan by clicking the **Add** button.

The Add Charging Application Item dialog is displayed.

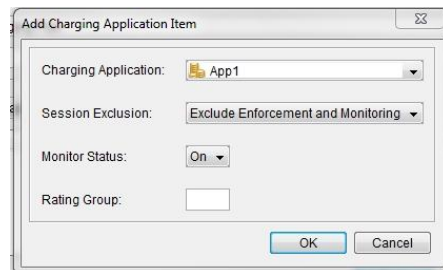


Figure 4-77: Add Charging Application Item dialog

6. In the Charging Application field, select a predefined Charging Application from the drop down menu.
7. In the Session Exclusion field, use the drop down menu to define how the metering of the Charging Application will be handled by the Online or Offline Charging Policy. Options are **Exclude Enforcement and Monitoring**, **Exclude Enforcement**, **Exclude Monitoring** or **Off**. For more information concerning these options, see the SMP User Guide.
8. In Monitor Status, turn monitoring of this Charging Application **On** or **Off**. If it is **Off** and the Charging Plan this Charging Application is assigned to has Session Monitoring set to **Enable**, this Charging Application will not be monitored along with the rest of the Charging Plan.
9. In the Rating Group field enter a unique number to identify this Charging Application in the Charging Policy. This number is different from the Application ID entered when the Charging Application itself was created. The Rating Group number selected must be coordinated with the other elements of your online and offline charging solution. For more information see the *SMP User Guide*.

10. Click **OK** to add the Charging Application to the Charging Plan.
The Charging Application will now appear in the Applications list.
11. Charging Applications in the Applications list may be removed from the Charging Plan or changed using the **Remove** and **Edit** buttons.
12. Click **Save** to add the Charging Plan to the Charging Plan catalog.
13. Clicking **Reset** removes any changes made to the Charging Plan since the last save.

Mobile Device Catalog

NOTE The Mobile Device Catalog is only available to those users with the **Subscriber Management Platform (SMP)** installed and the appropriate **Mobile Analytics license key** entered to enable the feature. For more information contact **Allot Customer Support** at support@allot.com.

The Mobile Device catalog lists the contents of the Mobile Device Database assigned to this NetXplorer.

For more information about using the Mobile Device Catalog in NetXplorer and how to assign a Mobile Device Database, see the **SMP Installation and Administration Guide**.

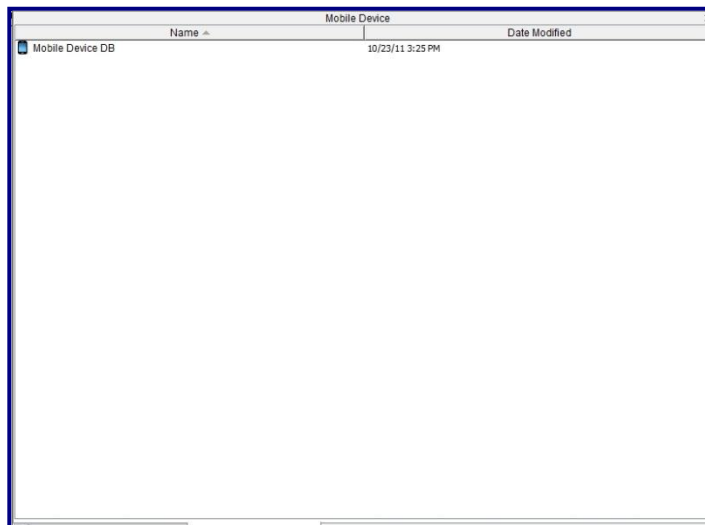


Figure 4-78: Mobile Device Catalog

Chapter 5: Defining Policies

NetXplorer Enforcement Policy

Overview

NetXplorer enables you to classify traffic and enforce Quality of Service according to high-level, easy-to-understand concepts. Traffic can be logically grouped into categories such as Mission Critical, Timing Critical, or Low Priority. These result in the desired network actions when matched to network traffic.

QoS Enforcement Policy consists of a set of Conditions and a set of actions that apply as a consequence of the conditions being satisfied. Traffic is classified using Lines, Pipes and Virtual Channels. A Line, Pipe or Virtual Channel are defined by one or more Conditions and a set of actions. A Line includes one or more Pipes. A Pipe includes one or more Virtual Channels.

A sample Enforcement Policy showing the relationship between Lines, Pipes, Virtual Channels and Conditions is illustrated below:

Identification		Conditions							Actions	
Name	Alarms As...	In Use	Internal	Direction	External	Service	Time	Tethering	Access	Quality of S...
CDMA All Tran		<input checked="" type="checkbox"/>	Any	↔	Any	All IP	Anytime	Ignore	Accept	Normal Line...
aaae.mym		<input checked="" type="checkbox"/>	aaae.my...	↔	Any	All IP	Anytime	Ignore	Accept	Normal Pip...
Encrypt		<input checked="" type="checkbox"/>	Any	↔	Any	SSL	Anytime	Ignore	Accept	Normal Virtu...
Tetherin		<input checked="" type="checkbox"/>	Any	↔	Any	Tethering_TM	Anytime	Ignore	Accept	Normal Virtu...
Android		<input checked="" type="checkbox"/>	Any	↔	Any	Android Mar...	Anytime	Ignore	Accept	Normal Virtu...
Pandora		<input checked="" type="checkbox"/>	Any	↔	Any	Pandora	Anytime	Ignore	Accept	Normal Virtu...
Facebo		<input checked="" type="checkbox"/>	Any	↔	Any	Facebook G...	Anytime	Ignore	Accept	Normal Virtu...
Email		<input checked="" type="checkbox"/>	Any	↔	Any	Mail	Anytime	Ignore	Accept	Normal Virtu...
File Tra		<input checked="" type="checkbox"/>	Any	↔	Any	File Transfer	Anytime	Ignore	Accept	Normal Virtu...
Stream		<input checked="" type="checkbox"/>	Any	↔	Any	Streaming_...	Anytime	Ignore	Accept	Normal Virtu...
Stream		<input checked="" type="checkbox"/>	Any	↔	Any	Streaming A...	Anytime	Ignore	Accept	Normal Virtu...
Browsir		<input checked="" type="checkbox"/>	Any	↔	Any	Web Applica...	Anytime	Ignore	Accept	Normal Virtu...
Fallbac		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Virtu...
aaaf.myme		<input checked="" type="checkbox"/>	aaaf.mym...	↔	Any	All IP	Anytime	Ignore	Accept	Normal Pip...
aaag.mym		<input checked="" type="checkbox"/>	aaag.my...	↔	Any	All IP	Anytime	Ignore	Accept	Normal Pip...
Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Pip...
Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Line...
Fallback		<input checked="" type="checkbox"/>	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Pip...

Figure 5-1: Line/Pipe/Virtual Channel/Condition Relationship

NetXplorer searches the Enforcement Policy table from the top down. As soon as a Line Condition is found to match the connection, NetXplorer looks at no more Lines. Within the matched Line, as soon as a Pipe Condition is found to match the connection, NetXplorer looks at no more Pipes. Similarly, within the matched Pipe, as soon as a Virtual Channel Condition is found to match the connection, NetEnforcer looks no further.

In short, the process of Condition matching is as follows:

- Find the Line Condition that the connection matches.
- Within that Line, find the Pipe Condition that the connection matches.
- Within that Pipe, find the Virtual Channel Condition that the connection matches.

Currently, only one Line is defined for each NetEnforcer, **Fallback Line**. All traffic for the NetEnforcer matches the Fallback Line. A default Pipe is defined for each line, **Fallback Pipe**. If a connection does not match the Conditions of any other Pipes, it matches the **Fallback Pipe**. Furthermore, every Pipe includes a default Virtual Channel, **Fallback**. If a connection does not match the Conditions of any other Virtual Channels within a Pipe, it matches the **Fallback** Virtual Channel.

The Conditions of the **Fallback Line**, **Fallback Pipe** and **Fallback Virtual Channels** cannot be deleted or modified. They allow all traffic to and from all hosts, all of the time.

Actions of Fallback Lines, Pipes, and Virtual Channels can be changed, however. For Pipes & Virtual Channels, all Actions can be changed. For Fallback Line, only the QoS value can be changed.

Enforcement Policy Elements

Lines

A Line represents a physical or logical connection in the system. A Line provides a way of classifying traffic that enables you to divide the total bandwidth and then manage every Line as if it was an independent link. A Line consists of one or more sets of Conditions and a set of actions that apply when any of the Conditions are met.

A Line can aggregate several Pipes, acting like a container of Pipes from a QoS point of view. The Condition of the **Fallback** Line cannot be modified or deleted. A connection coming into NetEnforcer is matched to a Line according to whether the characteristics of the connection match any of the Conditions of the Line. The connection is then further matched to the Conditions of a Pipe under the Line. The actions defined for the Line influence all the Pipes under the Line. The actions defined for a Pipe are enforced together with the actions of the Line.

NOTE When working with the AC-400 or AC-800 series NetEnforcers, no conditions can be set at the line level. The action will be applied when the conditions of the pipes beneath the line are met.

Pipes

A Pipe provides a way of classifying traffic that enables you to divide the total bandwidth and then manage every Pipe as if it was an independent link. A Pipe consists of one or more sets of conditions (Conditions) and a set of actions that apply when any of the Conditions are met. A Pipe can aggregate several Virtual Channels, acting like a container of Virtual Channels from a QoS point of view. When you add a new Pipe, it always includes at least one Virtual Channel, the **Fallback** Virtual Channel. The Condition of the **Fallback** Virtual Channel cannot be modified or deleted. A connection coming into NetXplorer is matched to a Pipe according to whether the characteristics of the connection match any of the Conditions of the Pipe. The connection is then further matched to the Conditions of a Virtual Channel under the Pipe. The actions defined for the Pipe influence all the Virtual Channels under the Pipe. The actions defined for a Virtual Channel are enforced together with the actions of the Pipe.

Virtual Channels

A Virtual Channel provides a way of classifying traffic and consists of one or more sets of conditions (Conditions) and a set of actions that apply when any of the Conditions are met. A Virtual Channel is defined within a Pipe. A connection matched to a Pipe is further matched to a Virtual Channel according to whether the characteristics of the connection match any of the Conditions of the Virtual Channel.

Conditions

Conditions can be defined at Line level, Pipe level or Virtual Channel level. NetXplorer matches connections to Conditions, first at the Line level, then at the Pipe level and then at Virtual Channel level within a Pipe.

- **Alarms Assignment:** Indicates if any alarms have been assigned to that object.
- **In Use:** Enables or disables the relevant object.
- **Internal:** Defines the source of the traffic. For example, specific IPs, MAC addresses, a range of IP addresses, IP Subnet addresses, or host names. The default value is **Any** which covers traffic from any source.
- **Direction:** The direction of the traffic between the selected source and destination (bidirectional, 'Internal to External', or 'External to Internal'). The default value is **bidirectional**.
- **External:** Defines the destination of the traffic. For example, specific IPs, MAC addresses, a range of IP addresses, IP Subnet addresses, or host names. The default value is **Any** which covers traffic to any destination.

- **Service:** Defines the protocols relevant to a connection. Protocols may be TCP and UDP IP type, non-TCP and non-UDP type or non-IP type. TCP and UDP IP protocols are defined based on port type. HTTP protocols may include content definitions, such as specific Web directories, pages, or URL patterns. The default value is **All** which covers all protocols.
- **Time:** Defines the time period during which the traffic is received. For example daily between 8.00 AM and 6.00 PM, Sundays between 12.00 AM and 12.00 PM or on the 1st and 15th of the month. The default value is **Anytime** which covers traffic at any time.
- **Tethering:** This condition does not appear by default and must be added by right clicking in the Enforcement Policy Table, choosing the Table Column Configuration... menu item and selecting the Tethering checkbox. In addition, this option will only appear if supported by the in-line platform and will be greyed out if the in-line platform's current license does not support tethering. If selected, tethering appears as a column in the policy table with the following three possible values for each Line, Pipe or VC: Yes i.e: if this traffic is tethered, No i.e: if this traffic is not tethered or Ignore i.e: not a condition
- **ToS:** Defines the ToS byte contained in the IP headers of the traffic. The default value is **Any** which covers any ToS value.
- **Encapsulation:** Defines VLAN traffic classification according to VLAN ID (VLAN Identifier) tags, consisting of 12 bits, and according to tagging priority bits, consisting of three bits. Alternatively can be used to classify by GRE tunnel.
- **Interface:** Defines the physical interface or group of interfaces on the In-line platform.

When a new Line, Pipe or Virtual Channel is created, it is assigned a default Condition with default values for each condition and you can modify these values as required.

The possible values for each condition are defined in the Catalog entries in the Catalog Editors. A Catalog Editor enables you to give a logical name to a comprehensive set of parameters (a Catalog entry). This logical name then becomes a possible value for a condition. Catalog Editors are described in detail in Chapter 4, Defining Catalog Entries.

TIP

If you classify traffic by a specific connection source (Internal) or connection destination (External), make sure your definition applies to both directions, from the Source to the Destination and from the Destination to the Source. For example, if you define HostName as the Connection Source and Any as the Connection Destination, make sure that the Condition is bi-directional, so that traffic from Any to HostName is also covered.

Actions

Lines, Pipes and Virtual Channels include a set of actions that is assigned to traffic once it meets any of the Conditions defined for the Line, Pipe or Virtual Channel. Only Quality of Service actions can be defined for a Line. There are six actions that can be defined for a Pipe or Virtual Channel: Access Control, Quality of Service, ToS Remarking, DoS, Connection Control and Quota.

The following action types are available, depending on the network element selected:

- **Access:** This action determines the access given to traffic. If the Access Control for a Line, Pipe or Virtual Channel is specified as **Reject** or **Drop**, all traffic meeting the Conditions of the Line, Pipe or Virtual Channel is dropped and no other Quality of Service or Connection Control actions are applied. If the Access Control for a Line, Pipe or Virtual Channel is specified as **Bypass** all traffic meeting the Conditions of the Line, Pipe or Virtual Channel is routed to its destination but no Quality of Service is applied to it and it does not appear in any monitoring graphs.
- **Quality of Service:** This action determines the QoS given to traffic. The default Quality of Service action for Lines, Pipes or Virtual Channels is **Normal Priority**, which has Level 4 priority, no bandwidth definitions, no ToS marking and no connection limitations.
- **ToS Remarking:** The ToS is a byte in the IP header of a packet that contains information about routing recommendations. NetEnforcer classifies traffic based on the ToS byte marking contained in the IP headers of the packets passing through it.
- **DoS (Denial of Service):** This action enables you to limit the frequency and number of connections, thereby giving a level of protection from attacks on the network resources (such as internally connected servers). NetExplorer analyzes the distribution of traffic across the various protocols and ports, and admits or drops excess traffic when predefined thresholds have been exceeded.
- **Service Activation:** This action steers the traffic to a pre-defined integrated service, Port or URL, when possible.
- **Quota:** This action imposes a volume or time-based limit on subscriber activity. The quota may be daily or monthly.

The possible values for each type of action are defined in a Catalog entry in the Catalog Editor. Catalog Editors are described in detail in *Chapter 4, Defining Catalog Entries*.

Using Lines, Pipes, Virtual Channels and Conditions

The following examples show how Lines, Pipes and Virtual Channels might be used:

- An Internet Service Provider sells slices of bandwidth to customers (defined in a Pipe template), each based on the Quality of Service granted to that category of customer (such as Gold, Silver and Bronze customers).
- A university wants to control Internet traffic congestion across the network involving students and faculty, in particular, to limit FTP use and give preferential bandwidth allocation to faculty during weekday hours. The university defines Virtual Channels for faculty usage, student usage, and student usage during night hours. A further Condition is then defined under the student usage Virtual Channel that specifies a different service for students accessing FTP.
- An organization has several links to the Internet. Only one NetEnforcer is required with Pipes defined for every link enabling traffic to be managed on every link independently.

NetXplorer includes a default starting database that contains common types of traffic written in sample Pipes, Virtual Channels and Conditions. You can edit, disable or delete these as required.

Using Templates

Templates enable you to create a "master" Pipe or Virtual Channel that upon saving will create multiple Pipes or Virtual Channels very similar to each other. Templates work with host entries defined in the Host Catalog. For example, if you had a Host Group type entry in the Host Catalog called Gold Customers that consisted of Company X, Company Y and Company Z, you could define a Pipe template to be expanded for Gold Customers. This would result in Pipes being created for Company X, Company Y and Company Z when the Enforcement Policy Editor is saved.

With Host List type entries, templates are only effective when the Host List entry includes more than one host or IP address or a range of IP addresses. For example, creating a Pipe template based on a Host List type entry that includes a range of IP addresses generates a Pipe instance for each IP in the range.

Templates are defined in the process of inserting a Pipe or Virtual Channel. For further details, refer to Defining Pipes, page 5-13.

Order of Enforcement Policy Definitions

Lines, Pipes and Virtual Channels should be defined so that those that are more specific are defined before those that are more general. This is because NetXplorer searches the Enforcement Policy table from the top down. Thus as soon as a Line Condition is found to match the connection, NetEnforcer stops looking at Lines. Similarly, within the matched Line, as soon as a Pipe Condition is found to match the connection, NetXplorer looks no further. For example, if you define a Virtual Channel that includes all HTML (*.html) files, that Virtual Channel must come after a Virtual Channel with a Condition that specifies a specific HTML file. Otherwise, NetXplorer will always arrive at the general Condition first, assign the action defined in the Virtual Channel according to that Condition, and not assign the action defined for the more specific Condition.


NetXplorer Enforcement Policy Editor

You set your QoS Enforcement Policy by defining Lines, Pipes and Virtual Channels in the NetXplorer Enforcement Policy Editor.

To access the Enforcement Policy Editor:

1. From the View menu, select **Enforcement Policy Editor**.

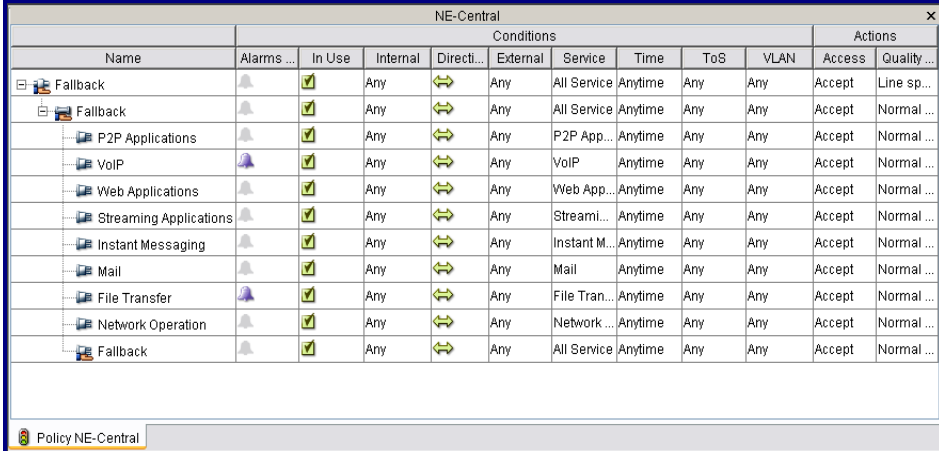
OR

Click  on the toolbar.

OR

Select and right-click a network element in the Network Tree and select **Enforcement Policy Editor** from the popup menu.

The Enforcement Policy Editor is displayed:



Name	Alarms ...	In Use	Internal	Conditions						Actions	
				Directi...	External	Service	Time	ToS	VLAN	Access	Quality ...
[-] Fallback		<input checked="" type="checkbox"/>	Any		Any	All Service	Anytime	Any	Any	Accept	Line sp...
[-] Fallback		<input checked="" type="checkbox"/>	Any		Any	All Service	Anytime	Any	Any	Accept	Normal ...
[-] P2P Applications		<input checked="" type="checkbox"/>	Any		Any	P2P App...	Anytime	Any	Any	Accept	Normal ...
[-] VoIP		<input checked="" type="checkbox"/>	Any		Any	VoIP	Anytime	Any	Any	Accept	Normal ...
[-] Web Applications		<input checked="" type="checkbox"/>	Any		Any	Web App...	Anytime	Any	Any	Accept	Normal ...
[-] Streaming Applications		<input checked="" type="checkbox"/>	Any		Any	Streami...	Anytime	Any	Any	Accept	Normal ...
[-] Instant Messaging		<input checked="" type="checkbox"/>	Any		Any	Instant M...	Anytime	Any	Any	Accept	Normal ...
[-] Mail		<input checked="" type="checkbox"/>	Any		Any	Mail	Anytime	Any	Any	Accept	Normal ...
[-] File Transfer		<input checked="" type="checkbox"/>	Any		Any	File Tran...	Anytime	Any	Any	Accept	Normal ...
[-] Network Operation		<input checked="" type="checkbox"/>	Any		Any	Network ...	Anytime	Any	Any	Accept	Normal ...
[-] Fallback		<input checked="" type="checkbox"/>	Any		Any	All Service	Anytime	Any	Any	Accept	Normal ...



Figure 5-2: Enforcement Policy Editor

2. When the Enforcement Policy Editor is open and a Line, Pipe or Virtual Channel is selected, a set of Quick Access icons appear on the menu bar.
3. The first Condition in the Enforcement Policy Table for any Line, Pipe or VC, **Alarms Assignment**, indicates if there is currently an open alarm assigned to that object. Double click in the Alarms Assignment field to add or edit the Alarms Assignments for that object.
4. The second Condition for any Line, Pipe or VC, **In Use**, indicates if the object is currently enabled. Double click in the field to enable or disable a Pipe or VC (Lines cannot be disabled).

The Enforcement Policy Editor displays a tree-table of the Line, Pipes and Virtual Channels currently defined in your NetXplorer. Each condition fragment in the line in the table represents a single Condition. A Pipe can be defined by one of more Conditions and can include one or more Virtual Channels. A Virtual Channel can be defined by one or more Conditions.

There is always one default Line, called **Fallback Line**, in the Enforcement Policy Editor. In addition, there is always one default Pipe, called **Fallback Pipe**. The Conditions of the default Line and Pipe cannot be modified or deleted.

Every Pipe has a default Virtual Channel called **Fallback**. The conditions or Condition of this default Virtual Channel cannot be modified or deleted, but you can delete the Pipe entirely.

You can expand/collapse a NetEnforcer, Line, Pipes or Virtual Channels in the Enforcement Policy Editor by clicking the  or  on the left of a Pipe or Virtual Channel, or by pressing <Shift + right arrow> or <Shift + left arrow> on your keyboard.

Pipes or Virtual Channels may be moved up or down in the Enforcement Policy Editor by right clicking on the entity you wish moved and selecting **Move Up** or **Move Down** from the menu.

Relevant buttons to the object you have selected in the Enforcement Policy Editor appear in the Quick Access Toolbar in the upper right hand corner of the GUI.

View Options

You can modify the Enforcement Policy Editor view by opting to hide or display the available columns.

To customize the Enforcement Policy Editor view:

1. From the Actions menu, select **Table Column Configuration**. The Enforcement Policy Columns Visibility dialog is now displayed.

The dialog box is titled "Enforcement Policy Columns Visibility" and is divided into three sections:

- Identification:**
 - Name
 - Description
- Conditions:**
 - Alarms Assignment
 - In Use
 - Internal
 - Direction
 - External
 - Service
 - Time
 - ToS
 - Encapsulation
 - Interface
 - Tethering
- Actions:**
 - Access
 - Quality of Service
 - Service Activation
 - ToS Remarking
 - DoS
 - Quota

At the bottom of the dialog are two buttons: "Save" (highlighted in blue) and "Cancel".

Figure 5-3: Enforcement Policy Columns Visibility dialog

2. Select the checkboxes to the left of the columns you want to display in the Enforcement Policy Editor.
3. Click **Save**.

Defining Enforcement Policy

The typical workflow for configuring your QoS Enforcement Policy is shown in the following diagram:

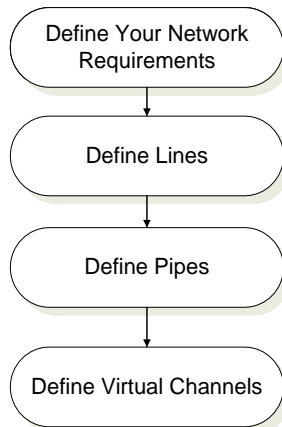


Figure 5-4: Defining Enforcement Policy Workflow

Each step of the workflow is described in the following sections. You can also define Pipes and Virtual Channels using templates.

Defining Your Network Requirements

Before defining Lines, Pipes or Virtual Channels, you must determine the type of traffic flowing through your network. Using NetXplorer’s Monitoring functions (described in *Chapter 7, Monitoring Reports*) you can determine your current network application patterns, and define the necessary QoS classification and actions.

The following are examples of traffic patterns and required QoS Enforcement Policy:

- Applications on your network that you consider “mission-critical” applications. These may be special applications that are time and/or resource sensitive. You may want to provide increased bandwidth or server resources.
- Items on your network that you consider low priority. These may include traffic that you consider non-time and/or response sensitive, or applications that you wish to limit during busy hours, such as FTP traffic.
- Applications that you do not want used on your network during certain times, such as new file-sharing applications that enable clients in your network to function as servers, thereby drastically increasing outbound traffic volume.
- Background tasks that are important, but can be performed at a slower rate. These may include email traffic or certain file transfers.
- Time-sensitive network applications. These may include streaming applications such as real-time audio or video.
- Customers or groups of customers categorized into various “tiered” levels. For example, you may wish to have Gold-level customers.

Once you have classified your network traffic, you can define your QoS Enforcement Policy.

Defining Lines

Each Line is defined by at least one Condition, and any traffic meeting those conditions is channeled to that Line. The actions defined for the Line are then applied to the traffic.

NOTE Multiple lines are not supported by AC-1000 Series and AC-2500 Series models.

To add a Line:

1. Select a Line in the Enforcement Policy table and select **Insert Line** from the Actions menu

OR

Select a Line in the Enforcement Policy table and click the **Insert Line** icon on the Quick Access Toolbar.

OR

Right-click a Line in the Enforcement Policy table and select **Insert Line** from the popup menu.

The **Enforcement Policy** tab of the Insert Line dialog is displayed.

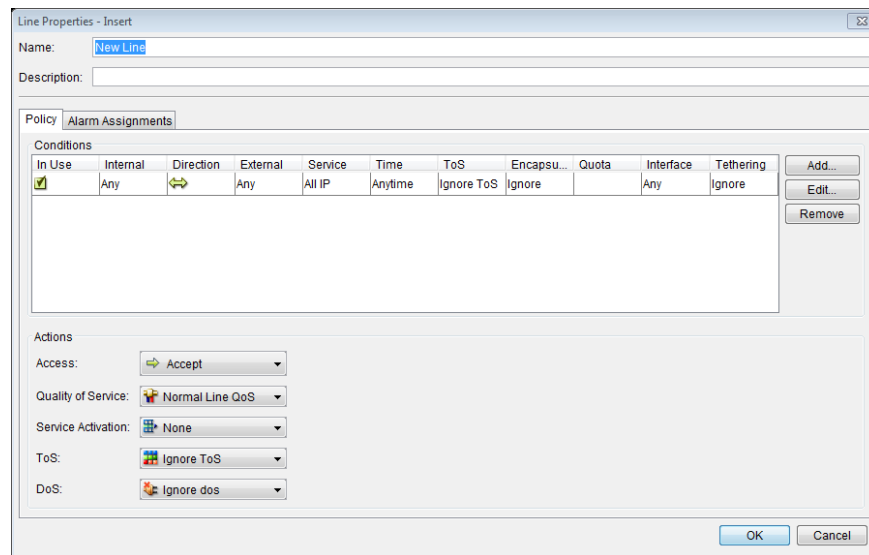


Figure 5-5: Insert Line Dialog – Enforcement Policy Tab

A new Line is added above the selected Line. The new Line contains a default Pipe (Fallback), and has default values for its Conditions (conditions) and actions.

2. Enter a new name for the Line, if required. Assigning a logical name to the Line helps you to classify your traffic.
3. Modify the **Conditions** of the Line by double-clicking the cell in the relevant column and selecting the required condition from the dropdown list that is displayed.

NOTES

You can view and edit all of the parameters of a Condition by clicking Edit to display the Condition Properties dialog (

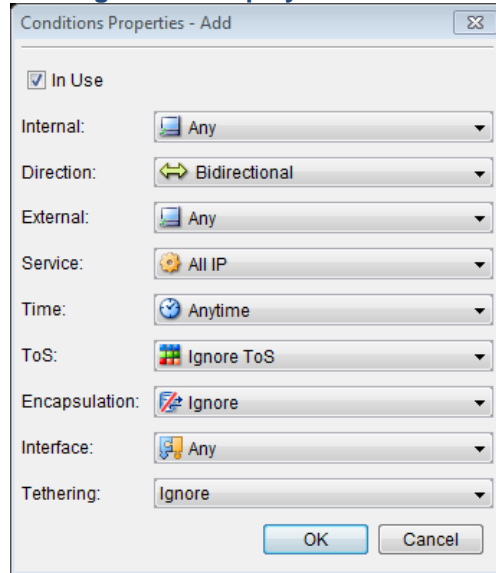



Figure 5-12).

To remove a Condition from a rule, select the Condition in the Conditions list and click Remove.

4. Modify the actions of the Line by selecting the required action from the dropdown list for each of the actions as follows:

Access	The access given to traffic. The default value is Accept
Quality of Service	The quality of service applied to traffic given access. The QoS determines priority, minimum and maximum bandwidth and traffic-shaping techniques (CBT or Burst). The default value is Normal Priority.
Service Activation	Sets if the connection should be passed as is, or steered to a pre-defined integrated service, Port or URL, when possible. The default is Pass As Is .
ToS	Sets the ToS Priority for the Line . The default is Any .
DoS	Sets the Denial of Service attack Enforcement Policy for the Line . The default is Ignore DoS .

5. Click **OK** to return to the Enforcement Policy Table.
6. Click  or select **Save** from the File menu to save the new Line.

TIP You can also add a new Line by copying and pasting an existing Line and modifying its definition.

Defining Pipes

Each Pipe is defined by at least one Condition, and any traffic meeting those conditions is channeled to that Pipe. The actions defined for the Pipe are then applied to the traffic.

To add a Pipe:

1. Select a Pipe in the Enforcement Policy table and select **Insert Pipe** from the Actions menu

OR

Select a Pipe in the Enforcement Policy table and click the **Insert Pipe** icon on the Quick Access Toolbar.

OR

Right-click a Pipe in the Enforcement Policy table and select **Insert Pipe** from the popup menu.

The **Enforcement Policy** tab of the Insert Pipe dialog is displayed.

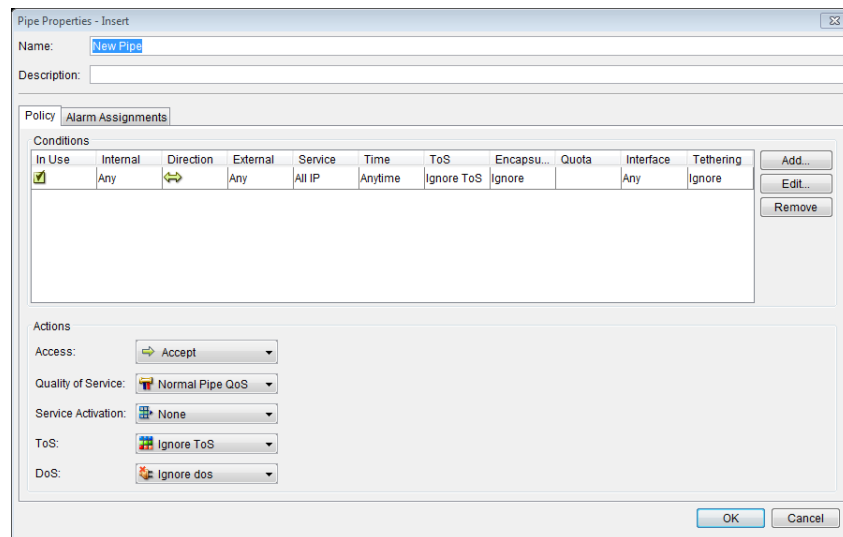


Figure 5-6: Insert Pipe Dialog – Enforcement Policy Tab

A new Pipe is added above the selected Pipe. The new Pipe contains a default Virtual Channel (Fallback), and has default values for its Conditions (conditions) and actions.

2. Enter a new name for the Pipe, if required. Assigning a logical name to the Pipe helps you to classify your traffic.
3. Modify the **Conditions** of the Pipe by double-clicking the cell in the relevant column and selecting the required condition from the dropdown list that is displayed.

NOTES

You can view and edit all of the parameters of a Condition by clicking Edit to display the Condition Properties dialog (

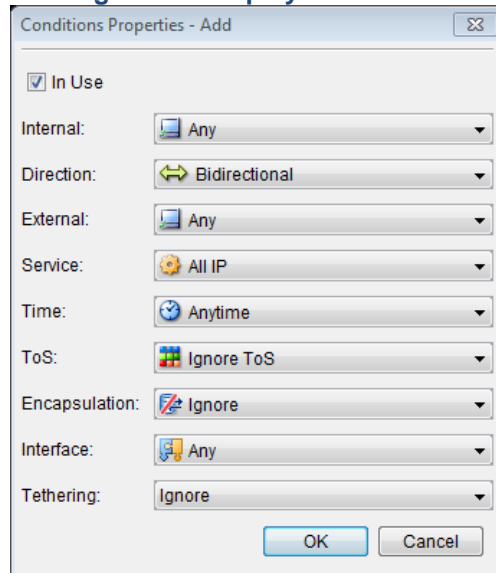



Figure 5-12).

To remove a Condition from a Pipe, select the Condition in the Conditions list and click Remove.

4. Modify the actions of the Pipe by selecting the required action from the dropdown list for each of the actions as follows:

Access	The access given to traffic. The default value is Accept
Quality of Service	The quality of service applied to traffic given access. The QoS determines priority, minimum and maximum bandwidth and traffic-shaping techniques (CBT or Burst). The default value is Normal Priority.
Service Activation	Sets if the connection should be passed as is, or steered to a pre-defined integrated service, Port or URL, when possible. The default is Pass As Is .
ToS	Sets the ToS Priority for the Pipe. The default is Any .
DoS	Sets the Denial of Service attack Enforcement Policy for the Pipe. The default is Ignore DoS .

5. Click **OK** to return to the Enforcement Policy Table.
6. Click  or select **Save** from the File menu to save the new Pipe.

TIP You can also add a new Pipe by copying and pasting an existing Pipe and modifying its definition.

Adding Pipe Templates

Pipe templates enable you to automatically add instances of the same Pipe for each host in a selected Host Catalog entry. This eliminates the need to define individual Pipes when the only difference between them is the IP address in the source or destination. Pipe templates are added at the same hierarchy level as Pipes.

To add a Pipe Template:

1. Select a Pipe in the Enforcement Policy table and select **Insert Pipe Template** from the Actions menu

OR

Select a Pipe in the Enforcement Policy table and click the **Insert Pipe Template** icon on the Quick Access Toolbar.

OR

Right-click a Pipe in the Enforcement Policy table and select **Insert Pipe Template** from the popup menu.

The **Enforcement Policy** tab of the Insert Pipe Template dialog is displayed.

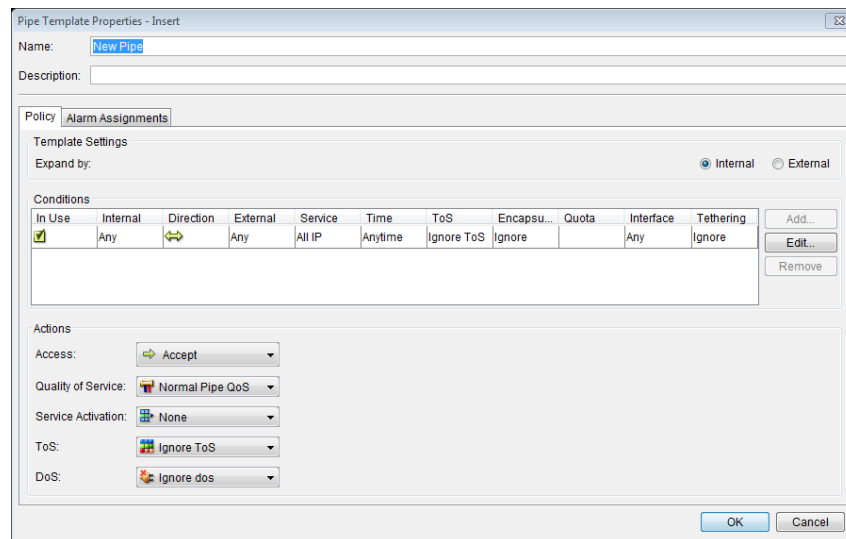


Figure 5-7: Insert Pipe Template Dialog – Enforcement Policy Tab

A new Pipe Template is added above the selected Pipe. The new Pipe Template contains a default Virtual Channel (Fallback), and has default values for its Conditions (conditions) and actions.

2. Enter a new name for the Pipe Template, if required. Assigning a logical name to the Pipe Template helps you to classify your traffic.
3. In the Template Settings area, you may decide if the Template instances will expand as Internally or Externally.
 Select **Internal** if you wish a new instance to be generated for each new Internal connection (default).
 Select **External** if you wish a new instance to be generated for each External connection.
4. Modify the **Conditions** of the Pipe Template by double-clicking the cell in the relevant column and selecting the required condition from the dropdown list that is displayed.

NOTE

You can view and edit all of the parameters of a Condition by clicking Edit to display the Condition Properties dialog (

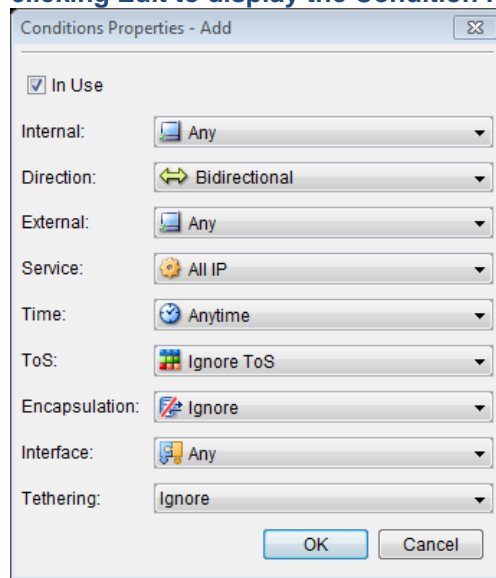


Figure 5-12).


There is one and only one rule in a template. The user cannot add additional ones.


5. Modify the actions of the Pipe Template by selecting the required action from the dropdown list for each of the actions as follows:

Access The access given to traffic. The default value is Accept

Quality of Service	The quality of service applied to traffic given access. The QoS determines priority, minimum and maximum bandwidth and traffic-shaping techniques (CBT or Burst). The default value is Normal Priority.
Service Activation	Sets if the connection should be passed as is, or steered to a pre-defined integrated service, Port or URL, when possible. The default is Pass As Is .
ToS	Sets the ToS Priority for the traffic. The default is Any .
DoS	Sets the Denial of Service attack Enforcement Policy. The default is Ignore DoS .

6. Click **OK** to return to the Enforcement Policy Table.

7. Click  or select **Save** from the File menu to save the new Pipe.

NOTE When adding a Pipe Template, Pipes identical to the Pipe Template but with a different Connection Source or Connection Destination are created for every member of the selected Host Catalog entry upon saving the Enforcement Policy Editor. These Pipes are not displayed in the Enforcement Policy table. A Pipe Template is represented by the  icon.

Adding Pipe Service Plan Templates

NOTE Service Plans are only available to those users with the Subscriber Management Platform (SMP) installed and the appropriate license key entered to enable the feature.

Pipe service plan templates enable you to automatically add the same Service Plan to instances of the same Pipe for each host in a selected Host Catalog entry.

To add a Pipe Service Plan Template:

1. Select a Pipe in the Enforcement Policy table and select **Insert Pipe Service Plan Template** from the Actions menu

OR

Select a Pipe in the Enforcement Policy table and click the **Insert Pipe Service Plan Template** icon on the Quick Access Toolbar.


OR

Right-click a Pipe in the Enforcement Policy table and select **Insert Pipe Service Plan Template** from the popup menu.

The Pipe Service Plan Properties - Insert dialog is displayed.



Figure 5-8: Pipe Service Plan Properties – Insert Dialog

2. Select the pre-existing Service Plan to be used for the template from the drop down menu. Service plans may be created in the Service Plan catalog.
3. Enter a description of the template, if relevant.
4. Click **OK** to return to the Enforcement Policy Table.
5. Click  or select **Save** from the File menu to save the new Pipe.

Defining Virtual Channels

A Virtual Channel is added to a Pipe. A Virtual Channel is defined by at least one Condition and any traffic meeting those conditions is channeled to that Virtual Channel. The actions defined for the Virtual Channel are then applied to the traffic.

In addition, Virtual Channel templates enable you to automatically add instances of the same Virtual Channel for each host in a selected Host Catalog entry. This eliminates the need to define individual Virtual Channels when the only difference between them is the IP address in the source or destination. Virtual Channel templates are added at the same hierarchy level as Virtual Channels.

NOTE **The actions of the Pipe influence all the Virtual Channels under that Pipe and are enforced together with the Virtual Channel's actions on every connection that is matched to the Pipe.**

To add a Virtual Channel:

1. Select a Virtual Channel in the Enforcement Policy table and select **Insert Virtual Channel** from the Actions menu
OR
Select a Virtual Channel in the Enforcement Policy table and click the **Insert Virtual Channel** icon on the Quick Access Toolbar.
OR

Right-click a Virtual Channel in the Enforcement Policy table and select **Insert Virtual Channel** from the popup menu.

The Enforcement Policy tab of the Virtual Channels Properties dialog is displayed.

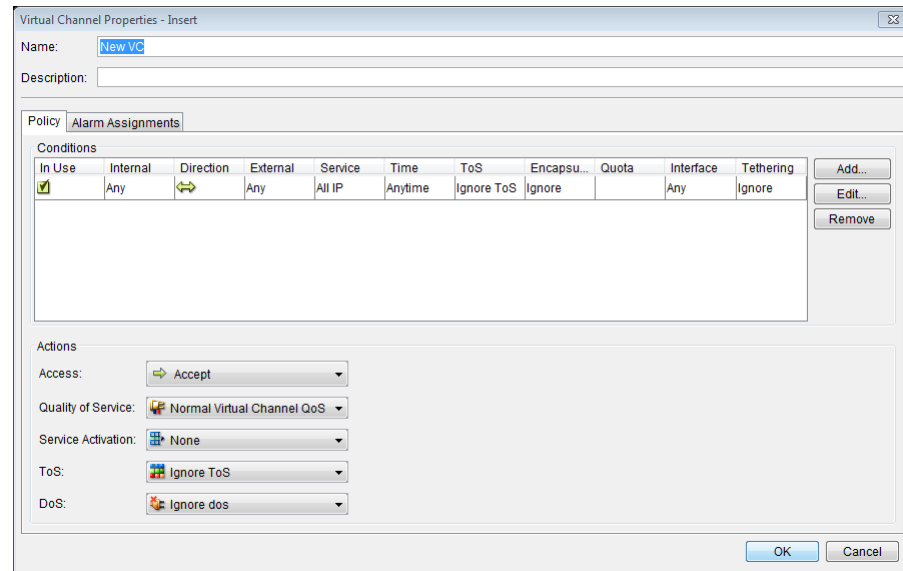




Figure 5-9: Virtual Channel Properties Dialog

A new Virtual Channel is added to the selected Pipe, or to the Pipe to which the selected Virtual Channel belongs. The new Virtual Channel has default values for its Conditions and actions.

2. Enter a new name for the Virtual Channel, if required. Assigning a logical name to the Virtual Channel helps you to classify your traffic.
3. Modify the Condition of the Virtual Channel in the same way as for a Pipe, as described on page 5-14.
4. Modify the actions of the Virtual Channel in the same way as for a Pipe, as described on page 5-14.
5. Configure the template settings for the Virtual Channel in the same way as for a Pipe.
6. Click  to save the new Virtual Channel.

NOTE If you add a Virtual Channel template, Virtual Channels identical to the Virtual Channel template but with a different Connection Source or Connection Destination are created for every member of the selected Host Catalog entry upon saving the Enforcement Policy Editor. These Virtual Channels are not displayed in the Enforcement Policy table. A Virtual Channel template is represented by the  icon.

TIP You can also add a new Virtual Channel by copying and pasting an existing Virtual Channel and modifying its definition.

Adding Virtual Channel Templates

Virtual Channel templates enable you to automatically add instances of the same Virtual Channel for each host in a selected Host Catalog entry. This eliminates the need to define individual Virtual Channels when the only difference between them is the IP address in the source or destination. Virtual Channel templates are added at the same hierarchy level as Virtual Channels.

To add a Virtual Channel Template:

1. Select a Virtual Channel in the Enforcement Policy table and select **Insert Virtual Channel Template** from the Actions menu

OR

Select a Virtual Channel in the Enforcement Policy table and click the **Insert Virtual Channel Template** icon on the Quick Access Toolbar.

OR

Right-click a Virtual Channel in the Enforcement Policy table and select **Insert Virtual Channel Template** from the popup menu.

The Enforcement Policy tab of the Virtual Channels Template Properties dialog is displayed.

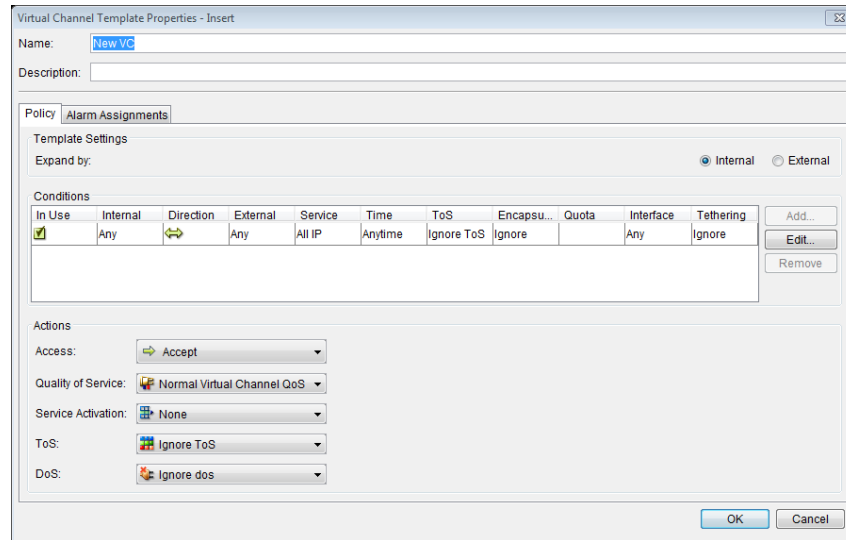



Figure 5-10: Virtual Channel Template Properties Dialog

A new Virtual Channel is added to the selected Pipe, or to the Pipe to which the selected Virtual Channel belongs. The new Virtual Channel has default values for its Conditions and actions.

2. Enter a new name for the Virtual Channel, if required. Assigning a logical name to the Virtual Channel helps you to classify your traffic.
3. In the Template Settings area, you may decide if the Template instances will expand as Internally or Externally.

Select **Internal** if you wish a new instance to be generated for each new Internal connection (default).

Select **External** if you wish a new instance to be generated for each External connection.
4. Modify the Condition of the Virtual Channel Template in the same way as for a Pipe, as described on page 5-15.
5. Modify the actions of the Virtual Channel in the same way as for a Pipe, as described on page 5-14.
6. Configure the template settings for the Virtual Channel in the same way as for a pipe, as described on page 5-15.
7. Click  to save the new Virtual Channel.

NOTE When adding a Virtual Channel template, Virtual Channels identical to the Virtual Channel template but with a different Connection Source or Connection Destination are created for every member of the selected Host Catalog entry upon saving the Enforcement Policy Editor. These Virtual Channels are not displayed in the Enforcement Policy table. A Virtual Channel template is represented by the icon.

Adding Virtual Channel Service Plan Templates

NOTE Service Plans are only available to those users with the Subscriber Management Platform (SMP) installed and the appropriate license key entered to enable the feature.

Virtual Channel service plan templates enable you to automatically add the same Service Plan to instances of the same VC for each host in a selected Host Catalog entry.

To add a VC Service Plan Template:

1. Select a VC in the Enforcement Policy table and select **Insert Virtual Channel Service Plan Template** from the Actions menu

OR

Select a Pipe in the Enforcement Policy table and click the **Insert Virtual Channel Service Plan Template** icon on the Quick Access Toolbar.

OR


Right-click a Pipe in the Enforcement Policy table and select **Insert Virtual Channel Service Plan Template** from the popup menu.

The Virtual Channel Service Plan Properties - Insert dialog is displayed.



Figure 5-11: Virtual Channel Service Plan Properties – Insert Dialog

2. Select the pre-existing Service Plan to be used for the template from the drop down menu. Service plans may be created in the Service Plan catalog.
3. Enter a description of the template, if relevant.
4. Click **OK** to return to the Enforcement Policy Table.

- Click  or select **Save** from the File menu to save the new Virtual Channel.

Adding Conditions

When traffic meets a Condition, it is assigned to that Condition. The actions assigned to the traffic are the actions defined for the rule — Line, Pipe or Virtual Channel — to which the Condition belongs.

To add a Condition:

- Add a Condition in one of the following ways:
 - Select a Pipe or Virtual Channel in the Enforcement Policy table and from the Actions menu, select **Properties**.
 - Right-click a Pipe, Virtual Channel or Condition in the Enforcement Policy table and select **Properties** from the popup menu.

The Conditions Properties dialog is displayed.

- To add a Condition, click **Add** in the Conditions area. The Condition Properties dialog is displayed.

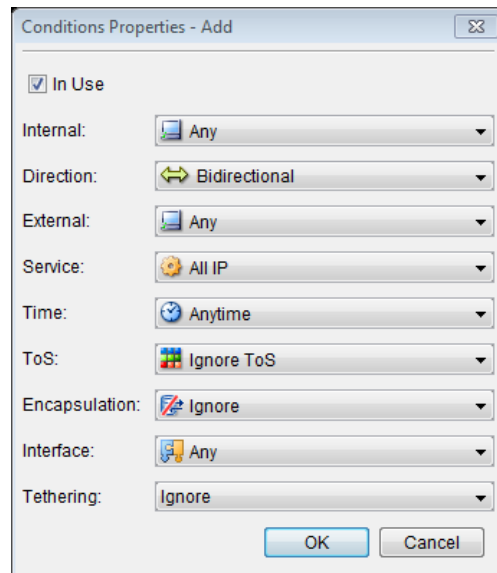



Figure 5-12: Condition Properties Dialog

- Configure the following parameters:

In Use The status of the Condition. The Condition is enabled when the checkbox is selected.

Internal	The source of the connection. The default value is Any. NOTE When creating a template based on an internal Host entry, the value of the Internal Condition cannot be set to Any.
Direction	The direction of the traffic between the selected source and destination (bidirectional or unidirectional). The default value is bidirectional,  .
External	The destination of the connection. The default value is Any. NOTE When creating a template based on an internal Host entry, the value of the External Condition cannot be set to Any.
Service	The protocol relevant to a connection. The default value is All Service.
Time	The time of the connection The default value is Anytime.
ToS	The ToS marking of the connection. The default value is Any.
Encapsulation	The VLAN or GRE encapsulation value used. The default value is Ignore.
Interface	The physical interface via which the connection enters/leaves the in-line platform
Tethering	Whether or not the connection originates from a tethered mobile device

4. Click **OK**. A new Condition is added to the selected Pipe or Virtual Channel, or to the Pipe or Virtual Channel to which the selected Condition belongs.
5. Specify the conditions for the Condition in the same way as for a Pipe, as described on page 5-14.

Enforcement Policy Table Order

You should define Lines, Pipes and Virtual Channels so that those that are more specific are defined before those that are more general. Similarly, the Conditions defined for a Line, Pipe or Virtual Channel should follow this order. This is because NetXplorer searches the Enforcement Policy table from the top down. Thus as soon as a Pipe Condition is found to match the connection, NetXplorer looks at no more Pipes. Similarly, within the matched Pipe, as soon a Virtual Channel Condition is found to match the connection, NetXplorer looks no further.

Using cut and paste or by using the up/down buttons, you can change the order of the Enforcement Policy table, as follows:

- Change the order of Pipes within the Enforcement Policy table
- Change the order of Virtual Channels within Pipes
- Change the order of Conditions within Pipes or Virtual Channels


You cannot change the position of **Lines**, **Fallback Lines**, **Fallback Pipes** or **Fallback Virtual Channels**. The **Fallback Pipe** is always at the bottom of the Enforcement Policy table and the **Fallback Virtual Channel** is always the last Virtual Channel in a Pipe.

Copying a Enforcement Policy Element

You can apply the same Enforcement Policy element to more than one NetEnforcer by copying and pasting the Enforcement Policy from one NetEnforcer to another. Similarly, you can copy Virtual Channel policies from one pipe to another, in the same NetEnforcer or across NetEnforcers.

Copying a Enforcement Policy entity copies item all of its subtentities as well. For example, if you copy a Pipe, the Pipe is copied together with any associated Virtual Channels.

To copy a Enforcement Policy:

1. In the Enforcement Policy Editor, right-click the Enforcement Policy (Pipe, or Virtual Channel) to be duplicated and select **Copy** from the popup menu,
OR
Select the Enforcement Policy in the Enforcement Policy Editor and select **Copy** from the Edit menu.
2. Select the NetEnforcer, Line or Pipe to which you want to copy the Enforcement Policy and select **Enforcement Policy Editor** from the View menu or click on  the toolbar.
3. Right-click the component in the tree in the Enforcement Policy Editor and select **Paste** from the popup menu or select **Paste** from the Edit menu. The Properties dialog for the selected Enforcement Policy is displayed.
4. Click **OK** to save the Enforcement Policy with the identical parameters,
OR
Edit the Enforcement Policy parameters, as required, and then click **OK** to save the Enforcement Policy.

NOTE **The name of the Enforcement Policy must be unique within any given branch of the Network tree.**

Enforcement Policy Distribution

Using the Enforcement Policy Distribution feature it is possible to update the policies of one unit and then distribute the new policies to other NetEnforcer or Service Gateway units on the Network. All NetEnforcers must be of the same Series and running the same major software version.

To distribute policies

1. In the Navigation pane, right-click a NetEnforcer or Service Gateway in the Navigation tree and select **Enforcement Policy Distribution** from the popup menu.

OR

Select a NetEnforcer in the Navigation tree and then select **Enforcement Policy Distribution** from the View menu.

NOTE The NetEnforcer selected in the Navigation Pane will serve as the source NetEnforcer. Its Enforcement Policy table will be distributed to other NetEnforcers.

The Enforcement Policy Distribution dialog is displayed.

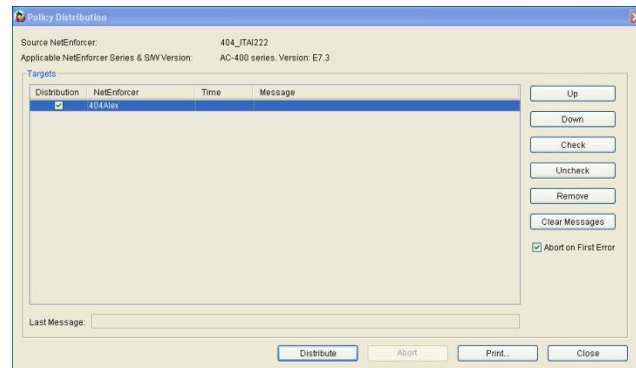


Figure 5-13: Enforcement Policy Distribution Dialog

2. The **Targets** list will populate with all NetEnforcers on the network that policies can be distributed to. Each relevant NetEnforcer is listed by name, with the time it received the new policies and any system messages.

NOTE Policies can only be distributed to NetEnforcers from the same series, running the same software version.

3. Click the **Distribute** checkbox to include that NetEnforcer in the distribution or select a NetEnforcer and use the **Check** and **Uncheck** buttons.
4. Select a NetEnforcer and click **Up** or **Down** to change its location in the distribution order.

5. Select a NetEnforcer and click **Remove** to delete the NetEnforcer from the targets list or **Clear Messages** to delete any system messages.
6. Select the **Abort on First Error** checkbox to instruct NetXplorer to cancel the entire Enforcement Policy Distribution operation on the first error.
7. Click **Distribute** to distribute the Enforcement Policy Table of the source NetEnforcer to all selected NetEnforcers. The Enforcement Policy Tables of the NetEnforcers selected will be overwritten in order, starting at the top of the list.
8. Click **Abort** at any time to stop the process or **Print** to print the **Results** list.

NOTE **Aborting the distribution will not roll back the Enforcement Policy Catalogs of any NetEnforcers already overwritten.**

9. Click **Close** to close the Enforcement Policy Distribution dialog box.

Restore Enforcement Policy and Catalogs

Using the Restore Enforcement Policy and Catalog feature it is possible to restore the saved image of the Enforcement Policy Table and catalogs which is stored on each NetEnforcer or Service Gateway and updated periodically. This feature should be used if a NetEnforcer or Service Gateway becomes corrupted or its policies and catalogs become damaged, requiring a roll back to a previous, working configuration.

To restore policies and catalogs:

1. Select Restore Enforcement Policy and Catalogs from the Tools menu.

The Restore Enforcement Policy and Catalogs dialog is displayed.

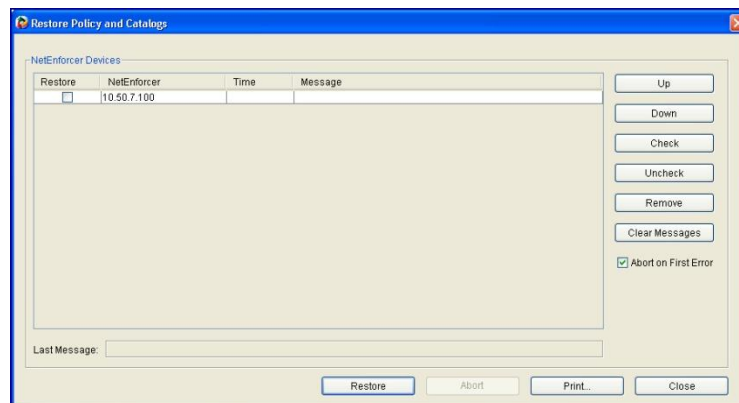


Figure 5-14: Restore Enforcement Policy and Catalogs Dialog

2. The **NetEnforcer Devices** list will populate with all NetEnforcers and Service Gateways on the network. Each relevant NetEnforcer or Service Gateway is listed by name, with the time it received the new policies and any system messages.
3. Click the **Restore** checkbox to include that NetEnforcer or Service Gateway in the restoration or select a NetEnforcer or Service Gateway and use the **Check** and **Uncheck** buttons.
4. Select a NetEnforcer or Service Gateway and click **Up** or **Down** to change its location in the distribution order.
5. Select a NetEnforcer or Service Gateway and click **Remove** to delete the NetEnforcer or Service Gateway from the list or **Clear Messages** to delete any system messages.
6. Select the **Abort on First Error** checkbox to instruct NetXplorer to cancel the entire Enforcement Policy Distribution operation on the first error.
7. Click **Restore** to restore the saved Enforcement Policy table and catalogs to each device. The NetEnforcers or Service Gateways selected will be restored in order, starting at the top of the list.
8. Click **Abort** at any time to stop the process or **Print** to print the **Results** list.

NOTE **Aborting the restoration will not roll back the Enforcement Policy Tables or Catalogs of any devices already overwritten.**

9. Click **Close** to close the Restore Enforcement Policy and Catalogs dialog box.

NetXplorer Charging Policy

Overview

NOTE **All Charging Policies require the Subscriber Management Platform and a specific ChargeSmart license. For further information, please contact Allot Customer Support at support@allot.com.**

NetXplorer enables you to classify two different sorts of Charging Policies: Online and Offline.

- An **Online Charging Policy** provides online (or real-time) credit control and quota management for subscriber data sessions. Quota management in this situation may include multiple data sessions where the subscriber's usage and remaining quota balance is monitored. Online Charging Policies may be used to support Enforcement Policies for both pre-paid and post-paid subscribers.
- An **Offline Charging Policy** uses charging data in the form of Charging Data Records (CDRs) and diameter accounting messages about services the subscriber has already used. An Offline Charging Policy does not have an active, real-time role in the processing of charges.

Each Online or Offline Charging Policy is made up of Rules. Each Rule is connected to a Service Plan and includes a Charging Plan.

Charging Policies are defined using the Online and Offline Charging Policy Editors.

For more information about defining Charging Policies in NetXplorer, see the **SMP User Guide**.

Identification		Conditions	Actions
Name	Description	Service Plan	Charging Plan
Rule1		gold	plan2
Fallback	Fallback rule	Any	No-Plan

Figure 5-15: Online Charging Policy Editor



NetXplorer Charging Policy Editors

You set your Charging Policy by using either the Online Charging Policy Editor or the Offline Charging Policy Editor.

To access the Online/Offline Charging Policy Editors:

1. From the View menu, select **Online Charging Policy** or **Offline Charging Policy**.

OR

Click  on the toolbar to open the Online Charging Policy Editor or  to open the Offline Charging Policy Editor.

OR

Select and right-click a network element in the Network Tree and select **Online Charging Policy** or **Offline Charging Policy** from the popup menu.

The Online or Offline Charging Policy Editor is displayed:

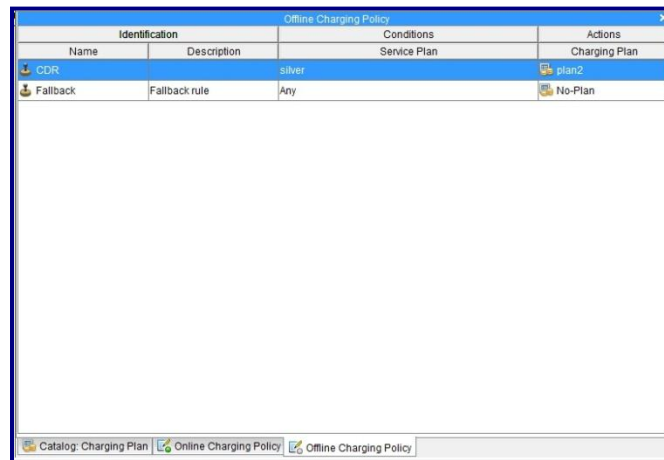


Figure 5-16: Offline Charging Policy Editor

- Each Charging Policy is made up of a series of Rules. Each Rule connects a Charging Plan to a Service Plan and they are triggered in order starting from the top of the table.
- There is always one default Rule, called **Fallback**, in a Charging Policy Editor. The Fallback rule is configured by default with **Any** Service Plan and **No-Plan** Charging Plan. The Charging Plan may be changed, but not the Service Plan so as to ensure that all subscribers fall into a Rule in the Charging Policy.
- When a Charging Policy Editor is open a set of Quick Access icons appear on the menu bar which allow you to insert Rules and moves Rules up and down.

To add a Rule to a Charging Policy:

- Select a Rule in the Charging Policy Editor and select **Insert Rule** from the Actions menu

OR

Select a Rule in the Charging Policy Editor and click the **Insert Rule** icon on the Quick Access Toolbar.

OR

Right-click a Rule in the Charging Policy table and select **Insert Rule** from the popup menu.

The **New Charging Policy Rule** dialog is displayed.

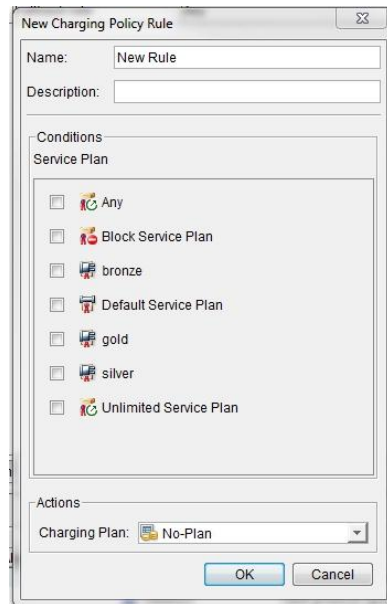


Figure 5-17: New Charging Policy Rule Dialog

2. Enter a name and description (if required) for the Rule.
3. Select a pre-defined Service Plan for the Rule in the Conditions area. Service Plans are defined in the Service Plan catalog.
4. Select a pre-defined Charging Plan for the Rule in the Actions area. Charging Plans are defined in the Charging Plan catalog.
5. Click **Save**.

Chapter 6: NetXplorer Alarms

Overview


NetXplorer enables you to not only monitor the state of the system, but also to receive alarms when certain thresholds and conditions are met.


NetXplorer includes a pre-defined list of events that are recorded in the Events Log and can be used to monitor the occurrence of system events in the Network. You can view the events for specific devices in the Events Log or you can configure specific events to generate alarms that are displayed in the Alarms Log,


In addition, user-defined alarms can be configured so that an alarm is sent to help you identify excessive connections or abnormal behavior on a Line, Pipe or Virtual Channel. For example, you can set an alarm to identify when the bandwidth for a particular link/customer is close to reaching its maximum. In order for a user defined alarm definition to generate an alarm, it must first be assigned to a specific NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel in the Network. User-defined alarms are displayed in the Alarms Log. For details on configuring alarms, refer to *Configuring User-defined Alarms* on page 6-8.

The Alarms Log is displayed in the Logs Pane and provides a list of all open alarms generated by the system (user-defined and event-based). An alarm remains open until the condition that generated it is no longer valid or until it is manually removed by an operator. For details on managing alarms, refer to *Managing Alarms* on page 6-22.

Alarm Object Indicators

In the Network tab of the Navigation Pane, the severity of the most serious alarm for a system component) is indicated on a network object by the addition of a color-coded alarm icon on the lower right portion of the device icon (Warning: gray; Minor: blue; Major: yellow; Critical: red). For example,  , indicates that a major alarm has occurred on the NetEnforcer or Service Gateway.

Accessibility problems are indicated by the addition of an icon in the upper right portion of the device icon. For example,  , indicates that the NetEnforcer or Service Gateway is not accessible.

The populated severity of alarms for a system component or one of its sub elements is indicated by the addition of a color-coded alarm icon on the upper left portion of the device icon (Warning: gray; Minor: blue; Major: yellow; Critical: red). For example,  , indicates a critical alarm is open for one at least one of the subelements in the network.

Navigation Pane

It is easy to review current Alarm settings by opening the Alarms/Events pane in the Navigation Pane.

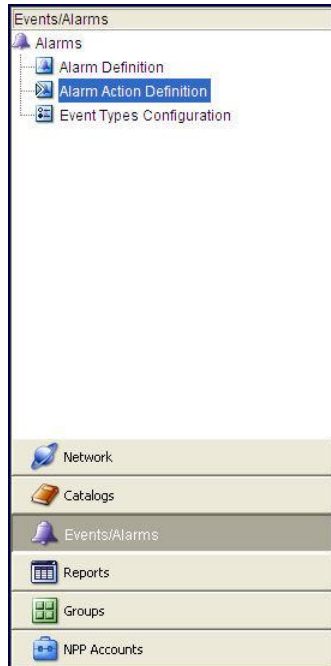


Figure 6-1: Events/Alarms Pane

From the Events/Alarms pane it is possible to review, configure and add and delete Alarm Definitions, Alarm Action Definitions and Event Types.

Configuring Alarms, Traps and Actions on Events

Events are specific occurrences that are recorded for network elements. NetXplorer is provided with a set of pre-defined events. All events are automatically logged by the system and can be viewed in the Events Log. In addition, if an event is configured to trigger an alarm, the event alarm is displayed in the Alarms Log.

NetXplorer is provided with predefined Event Types. You can configure the event to trigger an alarm and set the severity of the alarm that is generated. The resulting alarms are displayed in Alarms Log.

To configure an event alarm, trap or action:

1. Select **Events/Alarms** in the Navigation pane, and then select **Event Types Configuration** in the navigation tree,

OR

From the View menu, select **Alarms| Event Types Configuration**,

OR

On the toolbar, click the **Alarms** icon and select **Event Types Configuration** from the popup menu.

The Event Types Configuration application is displayed.

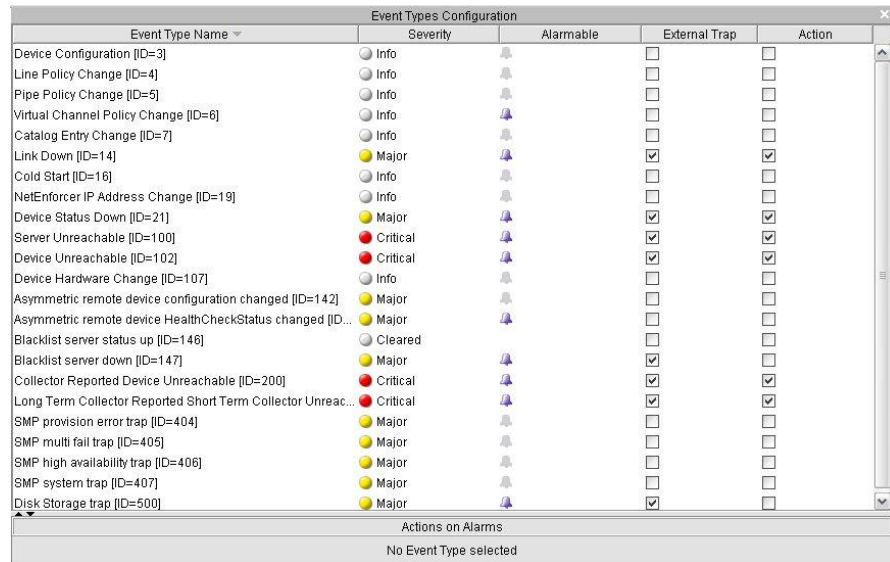


Figure 6-2: Event Types Configuration

- Set the severity of a specific alarm type by selecting the required level from the **Severity** dropdown list.
- Configure an event to generate or not generate an alarm by selecting or clearing the **Alarmable** dropdown list as required.
- Select the **External Trap** checkbox for any event you wish to send a trap to an external NMS Server (see page 3-12).
- Select the **Action** checkbox for any event you wish to trigger a script action. Configure the script action by right clicking the event and selecting **New Alarm Action Definition** from the drop down menu.

The Action Alarm Definition Entry Properties dialog opens.

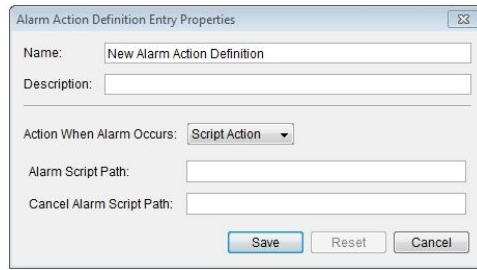



Figure 6-3: Action Alarm Definition Entry Properties

6. Edit the name and description of the entry in the relevant fields, if required.
7. In the **Action When Alarm Occurs** dropdown list, the only option available here is **Script Action** which runs a predefined Script when the Alarm triggers.

NOTE To configure an alarm to send an email as its action, see [Defining an Alarm Action Definition on page 6-14](#).

8. Enter an Event Script Path which points to the alarm script in the relevant fields.
9. Click **Save** to save the alarm action entry.

Once assigned, the action will appear in the Action on Alarm field at the bottom of the Event Type Configuration window when the relevant event is selected. An alarm action can be deleted, edited and copy/pasted to another event.

10. From the File menu, select **Save** or click **Save**  on the toolbar to save the new configuration.

NOTE: The NetXplorer sends device ID, line ID, pipe ID, VC ID and Mediator Device (SMP/STC) ID for use in the script. The parameters are sent in the order and format shown below:

DEV_ID:<id> LINE_ID:<id> PIPE_ID:<id> VC_ID:<id> MD_ID:<id>

In case a particular parameter is not defined, a value of “none” will be returned. So an example of the parameters sent might be:

DEV_ID:16 LINE_ID:1 PIPE_ID:6 VC_ID:0 MD_ID:none

Viewing Events

You can view the events log entries for a specific network component.


To view event log entries:

1. In the Navigation pane, right-click the network component in the Navigation tree and select **Events** from the popup menu.

OR

Select the network component in the Navigation tree and then select **Events** from the View menu.

OR

Select the network component in the Navigation tree and then click the **Events** icon  on the toolbar.

The Events Date Coverage dialog is displayed.

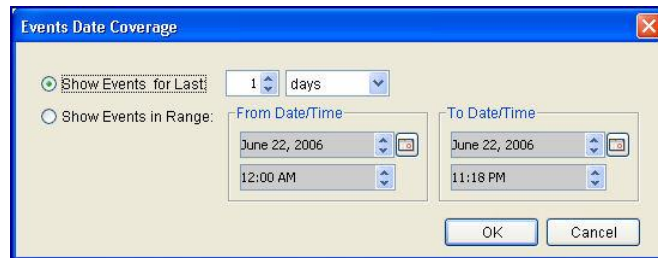


Figure 6-4: Events Date Coverage

2. To view events from the current time and earlier, select the **Show Events for Last** radio button. Then enter the relevant quantity of time and select the unit of time (weeks, days, hours, minutes) in the designated fields.

OR

To set a definite starting and end point for events, select the **Show Events in Range** radio button. Then enter the relevant dates and times in the From Date/Time and To Date/Time areas.








3. Click **OK**. The events for the designated time period are displayed in the Application Details pane.

ID	Date	Time	Severity	Type	Category	Description
3401	Jun 12, 2...	3:04:05 PM	Cleared	Device Reachabl...	Application se...	AllotAlpha199.203.223.2 is reacha...
3399	Jun 12, 2...	3:03:39 PM	Info	NetEnforcer Conf...	Application se...	NetEnforcer configuration imported fr...
3397	Jun 12, 2...	3:03:38 PM	Info	Cold Start [ID=16]	Device configu...	Cold Start
3396	Jun 12, 2...	3:02:20 PM	Critical	Device Unreacha...	Application se...	AllotAlpha199.203.223.2 is unreac...
3275	Jun 11, 2...	4:15:20 PM	Cleared	Link Up [ID=15]	Device configu...	Link EXTERNAL is up: admin status i...
3273	Jun 11, 2...	4:15:18 PM	Info	NetEnforcer Conf...	Application se...	NetEnforcer configuration imported fr...
3274	Jun 11, 2...	4:15:18 PM	Cleared	Link Up [ID=15]	Device configu...	Link INTERNAL is up: admin status i...
3269	Jun 11, 2...	4:15:17 PM	Info	Cold Start [ID=16]	Device configu...	Cold Start
3270	Jun 11, 2...	4:15:17 PM	Cleared	Automatic Alarm ...	Application se...	Automatic Alarm purge performed by ...
3271	Jun 11, 2...	4:15:14 PM	Major	Link Down [ID=14]	Device configu...	Link INTERNAL is down: admin statu...
3272	Jun 11, 2...	4:15:14 PM	Major	Link Down [ID=14]	Device configu...	Link EXTERNAL is down: admin stat...
3244	Jun 11, 2...	4:06:07 PM	Info	NetEnforcer Conf...	Application se...	NetEnforcer configuration imported fr...
3243	Jun 11, 2...	3:54:07 PM	Major	External Data So...	Security	Data Source in 199.203.223.2 is d...

Figure 6-5: Sample Events Log

Events Log Toolbar Options


The following icons are added to the NetXplorer toolbar when you click in the Events Log.

Button	Description
 Start of Events	Navigates to the first page of the Events Log.
 Page Events Backward	Navigates to the previous page.
 Page Events Forward	Navigates to the next page.
 End of Events	Navigates to last page of the Events Log
 Find	Enables you to search for events according to the content included in a specific parameter. Refer to Searching for Alarms, page 6-21.
 Sort	Enables you to sort the alarms in the Alarms Log according to the headers in the log. Refer to Sorting Alarms, page 6-18.
 Events Date Coverage	Enables you to redefine the range of time for the events displayed.

Sorting Events

You can sort the events in the Events Log according to the headers in the log (date, time, type category, description, and so on).


To sort the events in the Events Log:

1. Click the header according to which you want to sort the events.
OR
Right-click in the Events Log and select **Sort** from the popup menu.
OR
Click  on the toolbar. Then select the header from the submenu.
2. The events are sorted according to the selected header.

Searching for Events

You can search for events in the Events Log according to the headers in the log (ID, Date, Time, Severity, Type, Category, and Description).

To find an event:

1. From the Edit menu, select **Find**,
OR
Right-click and select **Find** from the popup menu,
OR
Click  in the toolbar.
The Find dialog is displayed.

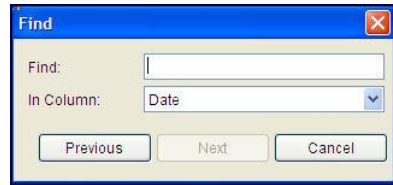


Figure 6-6: Find Dialog

2. Enter the text string (full or partial) that you want to search for in the **Find** field.
3. Select the parameter in which the text should appear from the **In Column** dropdown list.
4. Click **Previous** to go back to the last found match.
5. Click **Next** to begin the search from the currently selected row. If a match is found, the first match is highlighted in the Events log.
6. Click **Next** again to search for an additional match. (Repeat as required to view subsequent matches.)

Configuring User-defined Alarms

User-defined alarms can be triggered according to conditions existing in a NetEnforcer or Service Gateway, or in a selected Line, Pipe or Virtual Channel. When an alarm is triggered, it is displayed in the Alarms Log. You can also send notification of alarms by email.

The Alarms Editor enables you to define the conditions that trigger alarms (Alarm Definitions) as well as the action to be taken when an alarm is generated.

Configuring Alarm Definitions

Defining an alarm entry enables you to configure threshold alarms and determine the action to be taken when an alarm is generated by the system.

An alarm action is the action to be taken when an alarm is generated. You can configure alarms to be sent to a specific email address.

Working with Alarm Definitions

You can view and edit the configured alarms in the Alarm Definition List.

To view alarm definitions:

1. Select **Alarm** in the Navigation pane, and then select **Alarm Definition** in the navigation tree,

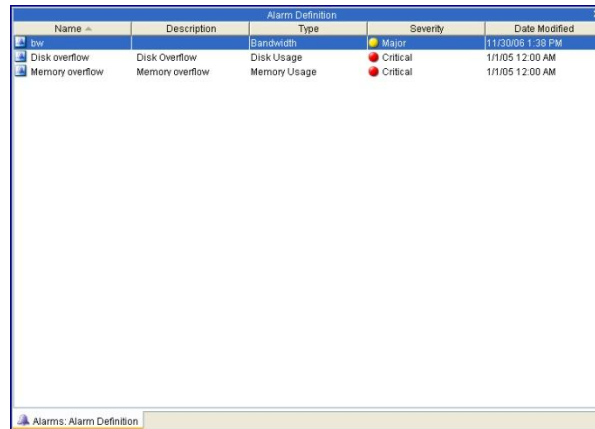
OR

From the View menu, select **Alarms | Alarm Definition**,

OR

On the toolbar, click the **Alarms** icon and select **Alarm Definition** from the popup menu.

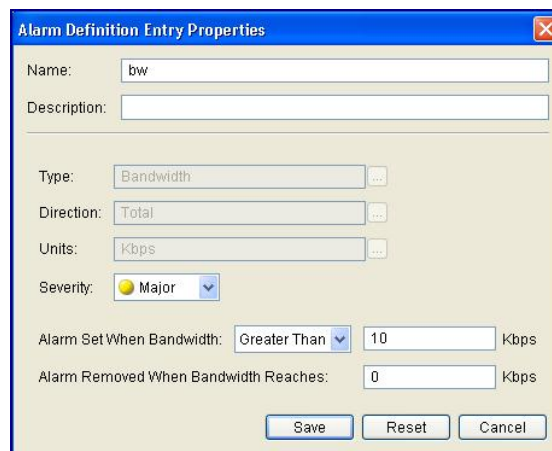
The Alarm Definition tab displays a list of the currently configured alarms.



Name	Description	Type	Severity	Date Modified
bw		Bandwidth	Major	11/30/06 1:38 PM
Disk overflow	Disk Overflow	Disk Usage	Critical	1/1/05 12:00 AM
Memory overflow	Memory overflow	Memory Usage	Critical	1/1/05 12:00 AM

Figure 6-7: Alarm Definition

- To view the properties of a specific alarm, right-click the alarm in the entries list and select **Properties** from the popup menu or double-click the alarm entry.



Alarm Definition Entry Properties

Name:

Description:

Type: ...

Direction: ...

Units: ...

Severity: ▼

Alarm Set When Bandwidth: Kbps

Alarm Removed When Bandwidth Reaches: Kbps

Figure 6-8: Alarm Definition Entry Properties Dialog

To edit alarm definitions:

- Select and right-click the alarm entry in the Alarm Entries List and select **Properties** from the popup menu or double-click the alarm entry. The Alarm Entry Properties dialog is displayed.

2. Edit the alarm parameters, as required. It is possible to edit the alarm name, severity, relation and threshold values.
3. Click **Save** to save the changes to the alarm entry.

Adding Alarm Entries

You can configure alarm entries for the following alarm types:

- Bandwidth
- Disk Usage (device only)
- Memory Usage (device only)
- Number of Active Pipes (device only)
- Number of Active Virtual Channels (device only)
- Number of Dropped Connections
- Number of Live Connections
- Number of New Connections
- Number of Active Lines (AC-400/AC-800 only)

The procedure for defining an alarm entry and the specific parameters defined vary according to the alarm type selected as indicated in the **Type** field.

Alarm Entry Type	Direction	Units	Severity	Threshold Values
Bandwidth (not device)	✓	✓	✓	✓
Disk Usage (device only)			✓	✓
Memory Usage (device only)			✓	✓
Number of Active Pipes (device only)			✓	✓
Number of Active Virtual Channels (device only)			✓	✓
Number of Dropped Connections (not device)			✓	✓
Number of Live Connections (not device)			✓	✓

Alarm Entry Type	Direction	Units	Severity	Threshold Values
Number of New Connections (not device)			✓	✓
Number of Active Lines			✓	✓

In the example given here, a Bandwidth type alarm entry is defined.

To add an alarm definition:

1. Right-click in the Alarms Definition List and select **New Alarm Definition** from the popup menu.

The Alarm Definition Entry Properties dialog is displayed.

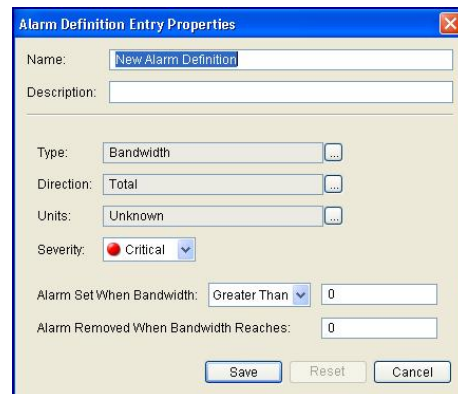


Figure 6-9: New Alarm Definition Entry Properties

2. Edit the name of the entry in the **Name** field, if required.
3. Click the browse button adjacent to the **Type** field. The Alarm Wizard - Select Alarm Type dialog is displayed.

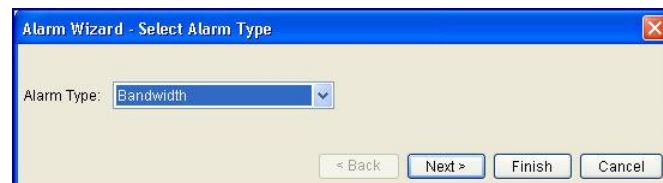


Figure 6-10: Select Alarm Type

4. Select the type of alarm from the **Alarm Type** dropdown list.
5. Click **Finish** to return to the Alarm Definition Entry Properties dialog box

OR

Click **Next** to open the Alarm Wizard -Select Direction dialog box.



Figure 6-11: Select Direction

6. Select the required direction from the **Direction** dropdown list (**Total, Inbound or Outbound**).

Click **Finish** to return to the Alarm Entries Entry Properties dialog box

OR

Click **Next** to open the Alarm Wizard - Select Units dialog box.

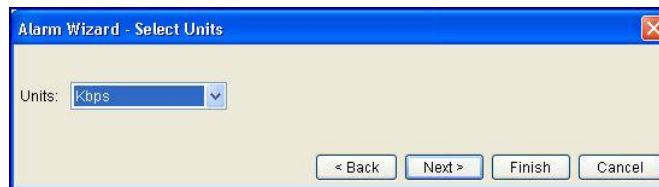


Figure 6-12: Select Units

7. Select the unit of measurement for monitoring from the **Units** dropdown list (**Kbps or Number of Packets**).
8. Click **Finish** to return to the Alarm Entries Entry Properties dialog box

OR

Click **Next** to open the Alarm Wizard -Select Severity dialog box.



Figure 6-13: Select Severity

9. Select the required level of severity from the Severity dropdown list (Critical, Major, Minor or Warning).
10. Click **Finish** to return to the Alarm Entries Entry Properties dialog box

OR

Click **Next** to open the Alarm Wizard -Select Values dialog box.



Figure 6-14: Select Values

NOTE The parameters configured in the **Alarm Wizard - Select Values** dialog are determined by the selected **Alarm type**.

11. In the **Alarm Set When....** field, define the condition that must exist before an alarm is generated by selecting **Greater than, Less than, Equal to** or **Not Equal to** from the dropdown list and entering the relevant quantity in textbox.
12. In the **Alarm Cleared When...reaches** field, define the condition that must exist before an alarm is cleared.
13. Click **Finish**. The Alarm Definition Entry Properties dialog for the selected type of entry is displayed. For example, Figure 6-9 shows the Alarm Definition Entry Properties dialog for the Bandwidth alarm type.
14. Click **Save** to save the Alarm Definition Entry definition.

Configuring Alarm Actions

Viewing and Editing Alarm Action Definitions

You can view the configured alarm action definitions in the Alarm Action Definition List

To view alarm action definitions:

1. Select **Events/Alarms** in the Navigation pane, and then select **Alarm Action Definition** in the navigation tree.

OR

From the View menu, select **Alarms | Alarm Action Definition**,

OR

On the toolbar, click the **Alarms** icon and select **Alarm Action Definition** from the popup menu.

The Alarm Action Definition List is displayed.

Defining an Alarm Action Definition

You can define an alarm action definition. When an alarm that is configured to take this action is triggered, an email notification may be sent to the address defined in the alarm action definition, or a pre-defined script may be run.

To define an alarm action:

1. Right-click **Alarms Action Definition** in the Navigation tree and select **New Alarm Action Definition** from the popup menu.

The Alarm Action Definition Entry Properties dialog is displayed.

2. Edit the name of the entry in the **Name** field, if required.
3. Select the action to be taken in response to the alarm from the **Action When Alarm Occurs** dropdown list, as follows:
 - **Send Email to:** Sends notification of an alarm to a configured email address.

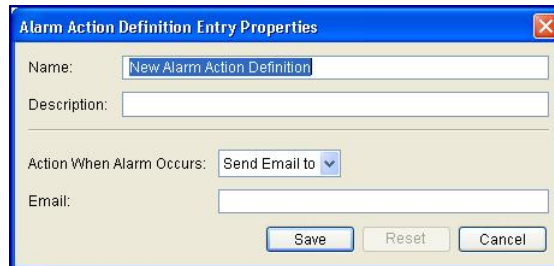


Figure 6-15: Alarm Action Definition Entry Properties – Send Email to

- **Script Action:** Runs a predefined Script when the Alarm triggers.

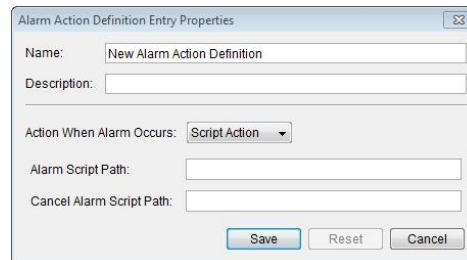


Figure 6-16: Alarm Action Definition Entry Properties – Script Action

4. Configure the alarm action parameters as follows:
 - If **Send Email to** was selected, enter the email address to which the alarm is to be sent in the Email field.
 - If **Script Action** was selected, enter the paths to the alarm script and the cancel alarm script in the relevant fields.
5. Click **Save** to save the alarm action entry.

NOTE The NetXplorer sends device ID, line ID, pipe ID, VC ID and Mediator Device (SMP/STC) ID for use in the script. The parameters are sent in the order and format shown below:

DEV_ID:<id> LINE_ID:<id> PIPE_ID:<id> VC_ID:<id> MD_ID:<id>

In case a particular parameter is not defined, a value of “none” will be returned. So an example of the parameters sent might be:

DEV_ID:16 LINE_ID:1 PIPE_ID:6 VC_ID:0 MD_ID:none

To edit an alarm action entry:

1. Select and right-click the alarm action entry in the Alarm Action Definition List and select **Properties** from the popup menu or double-click the action alarm entry. The Alarm Action Definition Entry Properties dialog is displayed.
2. Edit the alarm action parameters, as required.
3. Click **Save** to save the changes to the alarm action entry.

Assigning Alarms

In order for an alarm entry to generate an alarm, it must first be assigned to a specific NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel in the Enterprise.

Viewing Alarm Assignments

You can view a list of the alarm entries assigned to a specific NetEnforcer or Service Gateway, Line, Pipe or Virtual Channel.

To view alarm assignments:

1. In the Navigation pane, right-click the NetEnforcer or Service Gateway in the Network tree and select **Alarm Definition Assignments | Alarm Definition Assignment List**.

OR

In the Enforcement Policy Editor, right-click the Line, Pipe or Virtual Channel and select **Alarm Assignment**.

OR

In the Enforcement Policy Editor, double-click in the **Alarms Assignment** column.

The Alarm Assignments tab is displayed for the selected entity.

Assigning Alarms

To assign an alarm:

1. In the Navigation pane, right-click the NetEnforcer or Service Gateway in the Network tree and select **Alarm Definition Assignment | New Alarm Definition Assignment**.

OR

In the Enforcement Policy Editor, right-click the Line, Pipe or Virtual Channel, and select **Alarm Assignments | Add Alarm Assignment**.

OR

In the Enforcement Policy Editor, double-click in the **Alarms Assignment** column.

The Alarm Definition Assignment Editor dialog is displayed.

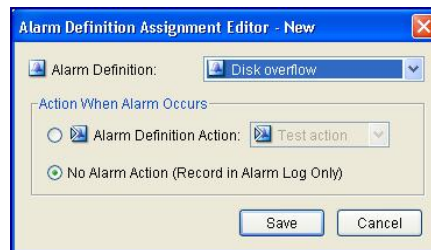


Figure 6-17: New Alarm Definition Assignment Editor

2. Select the required alarm from the **Alarm Definition** dropdown list.
3. Set the action to occur when alarm is generated by selecting the **Alarm Definition Action** or **No Alarm Action** radio button. If you select **Alarm Action**, select the type of action from the dropdown list.
4. Click **Save**. The alarm is added to the Alarm Definition Assignment list for the selected NetEnforcer or Service Gateway.

Viewing the Alarms Log

Located in the Logs Pane in the lower portion of the NetXplorer window, the Alarms Log displays a list of the alarms triggered by either assigned alarm entries or alarmed event types.

Ack	Date	Time	Severity	Alarm Definition	Source	Description
	Aug 11, 2010	2:48:17 PM	Major	-	aa	Data Source in 10.50.37.11 is down
	Aug 11, 2010	10:37:48 AM	Major	-	10.50.8.35	License Warning: attribute type: vc number, limiting type: number o...
	Aug 11, 2010	10:26:19 AM	Major	-	10.50.8.35	License Warning: attribute type: vc number, limiting type: number o...
	Aug 11, 2010	10:16:19 AM	Major	-	10.50.8.35	License Warning: attribute type: vc number, limiting type: number o...
	Aug 11, 2010	10:06:19 AM	Major	-	10.50.8.35	License Warning: attribute type: vc number, limiting type: number o...

Figure 6-18: Alarms Log

The Alarms Log is automatically refreshed every 30 seconds and provides the following information for each alarm:

Ack A checkmark in this column indicates that the alarm has been acknowledged. Acknowledging an alarm re-arms the alarm definition so that NetEnforcer again checks to see if the alarm condition exists. Acknowledged alarms are ignored when establishing severity indicators in the Network Tree.

Date The date on which the event triggering the alarm occurred.

Time The time when the event triggering the alarm occurred.

Severity The severity of the alarm. The color of the severity icon reflects the severity as follows:

Warning: Gray
 Minor: Blue
 Major: Yellow
 Critical: Red
 Information: White

Alarm Definition This is the name of the assigned alarm definition in the Alarm Definition list associated with the alarm. This will be blank if the alarm occurred as a result of an alarmable event type.






Source The type of object where the event triggering the alarm occurred followed by and underscore and the object's name. The possible object types are: **NE** (NetEnforcer), **Line**, **Pipe**, **VC** (Virtual Channel), **Network**, **Collectors**, **SMP**, **Long-Term Monitoring** or **Short-Term Monitoring**.

Example: **pipe_mail**

Description A summary of the event triggering the alarm.

Alarms Log Toolbar

The following buttons appear at the upper right hand corner of the Logs Pane when an Alarms Log is open:

BUTTON	DESCRIPTION
 Acknowledge	Enables you to indicate that you have seen the alarm. It does not indicate that any action has been taken in response to the alarm. Refer to <i>Acknowledging Alarms</i> , page 6-22.
 Remove	Enables you to remove an alarm, removing it from the active Alarms Log. Refer to <i>Removing Alarms</i> , page 6-23.
 Find	Enables you to search for alarms according to the content included in a specific alarm parameter. Refer to <i>Searching for Alarms</i> , page 6-21.
 Sort	Enables you to sort the alarms in the Alarms Log according to the headers in the log. Refer to <i>Sorting Alarms</i> , page 6-18.
 Filter	Enables you to apply a filter to the Alarms Log so that only alarms matching the filter are displayed. Refer to <i>Filtering Alarms</i> , page 6-19.

Sorting Alarms

You can sort the alarms in the Alarms Log according to the headers in the log (date, time, severity, source, and so on).

To sort the alarms in the Alarms Log:

1. Click the header according to which you want to sort the events.

OR

Right-click in the Events Log and select **Sort** from the popup menu.

OR


Click  on the toolbar. Then select the header from the submenu.

The listed alarms are sorted according to the selected header.

Filtering Alarms

You can apply a filter to the Alarms Log so that only alarms matching the filter are displayed. This is particularly useful because the Alarms Log may include up to 1,000 alarms.

To define a filter:

1. Right-click in the Alarms Log and select **Filter** from the popup menu or click  in the toolbar. The Alarm Log Filter Definitions dialog is displayed:

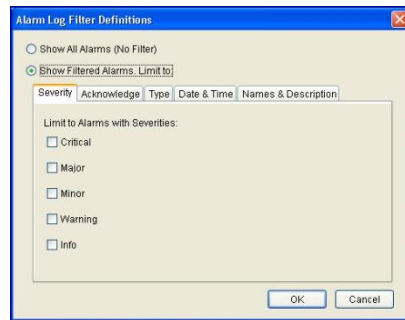


Figure 6-19: Alarm Log Filter Definitions: Severity Tab

2. Select Show Filtered Alarms.

Define the filter parameters in the different tabs as follows:

- In the Severity tab, select the Severity levels as required: Critical, Major, Minor, Info, Warning.
- In the Acknowledge tab, select Acknowledged or Unacknowledged to include acknowledged and/or unacknowledged alarms.

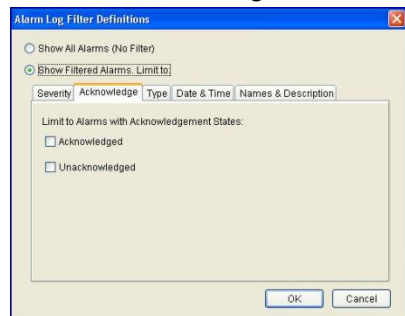


Figure 6-20: Alarm Log Filter Definitions: Acknowledge Tab

- In the Type tab, select the type of alarms to be shown, TCA (threshold alarms) or Non-TCA alarms.

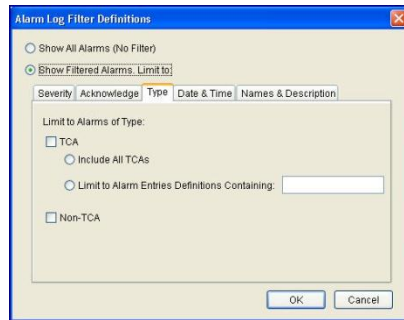


Figure 6-21: Alarm Log Filter Definitions: Type Tab

- In the Date & Time tab, configure the dates and time for which you want to view alarms.

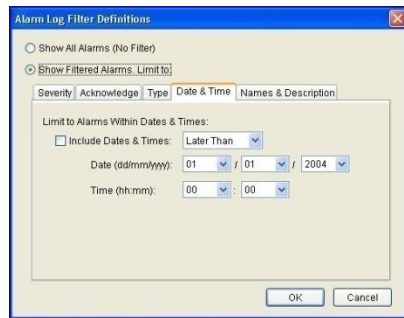


Figure 6-22: Alarm Log Filter Definitions: Date & Time Tab

- In the Names & Description tab, enter the following types of specifying key words as required: Source Names Containing and Descriptions Containing.

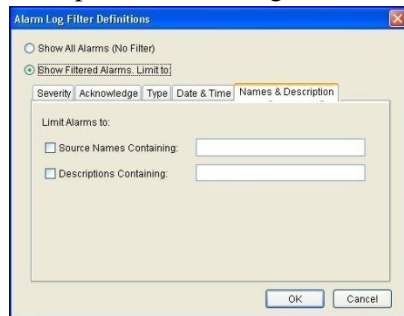


Figure 6-23: Alarm Log Filter Definitions: Names & Description Tab

3. Click **OK**. The filter is applied. Only the alarms that match the filter parameters are displayed in the Alarms Log and **Filtered** is displayed in the status bar.

NOTES To clear any filters, the user should reenter the Filters dialog box and select “Show All Alarms (No Filter)” radio button, then click OK. The log then refreshes without any filter.

If two or more filter parameters are selected, the results will include all alarms that answer at least one of the parameters.

Viewing Alarm Properties

You can view the configured properties of an alarm in the Alarms Log.

To view alarm properties:

Right-click an alarm in the Alarms Log and select Properties from the popup menu or double click the alarm. The Alarm Properties dialog is displayed.

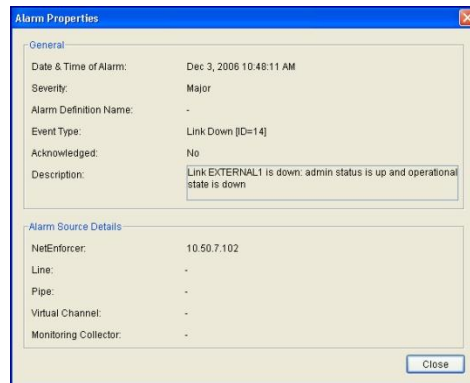



Figure 6-24: Alarm Properties Dialog

Searching for Alarms

You can search for alarms according to the content included in a specific alarm parameter.

To search for an alarm:

1. From the Edit menu, select **Find**,
OR
Right-click and select **Find** from the popup menu,
OR
Click  in the toolbar.
The Find dialog is displayed.

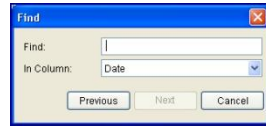


Figure 6-25: Find Dialog

2. Enter the text string (full or partial) that you want to search for in the **Find** field.
3. Select the parameter in which the text should appear from the **In Column** dropdown list.
4. Click **Next** to begin the search. If a match is found, the first match is highlighted in the Alarms Log.
5. Click **Next** again to search for an additional match. (Repeat as required to view subsequent matches.)
6. Following your first match, the **Previous** button appears. Click it to go back to the last match.

Managing Alarms


As part of the system monitoring process, you can view, acknowledge and remove alarms in NetXplorer.

Acknowledging Alarms

Acknowledging an alarm indicates only that you have seen the alarm. It does not indicate that any action has been taken in response to the alarm.

NOTE **Once an alarm has been acknowledged, its severity is no longer reflected in the Object icon in the Network tree.**

To acknowledge specific alarm(s):

1. Select the alarm(s) in the Alarms Log.
2. Right-click and select **Acknowledge Selected Alarms** from the popup menu or click  in the toolbar.
3. The alarm is acknowledged and a checkmark is displayed in the **Ack** column for the alarm in the Alarms Log.


To acknowledge all alarms:

Right-click an alarm in the Alarms Log and select **Acknowledge All Alarms** from the popup menu. All alarms are acknowledged and a checkmark is displayed in the **Ack** column for each alarm in the Alarms Log.

Removing Alarms

Removing an alarm removes the alarm from the system and from the Alarms Log. You remove an alarm that is insignificant or that resulted from a problem that has since been resolved.

To remove specific alarm(s):

1. Select the alarm(s) in the Alarms Log.
2. Right-click and select **Remove Selected Alarms** from the popup menu or click  on the toolbar. A system message is displayed.
3. Click **Yes** to confirm. The removed alarm is removed from the Alarms Log.

To remove all alarms:

1. Right-click an alarm in the Alarms Log and select **Remove All Alarms** from the popup menu. A system message is displayed.
2. Click **Yes** to confirm.

Monitoring & Reports

The Alarms Log provides direct access to relevant real-time monitoring and long-term reporting graphs. This enables you to quickly access a monitoring graph for closer inspection of a problematic situation. For example, if an alarm is triggered on a particular Pipe because the number of live connections in the Pipe has exceeded a specified amount, you can access the real-time monitoring graphs for the Pipe to understand more clearly if there is a problem or if your QoS Enforcement Policy requires modification.

To access monitoring graphs from the Alarms Log, right-click an alarm and select from the options displayed. The monitoring graphs available vary according to the object type selected.

For further information on monitoring and reports, refer to *Chapter 7, Monitoring Reports*.

Chapter 7: Monitoring Reports

Monitoring Reports Options

NetXplorer's monitoring and reporting options enable you to monitor applications, protocols, policies, hosts and subscribers in real time and to verify enforcement of the most suitable QoS Enforcement Policy.

Different applications, such as e-Business, ERP and real-time applications require performance guarantees. Other mission-critical applications may suffer from a shortage of bandwidth, while non-critical Web browsing and batch traffic, such as mail and FTP, may use up network resources. In other network setups, some users require a higher level of service than others. For example, internationally dispersed branch offices have expensive narrow WAN links to headquarters and many different users share the same bandwidth. On campuses, students overload network resources (WAN connection, caches, servers) with excessive requests for service (audio traffic), while the administration suffers from reduced available bandwidth and longer response time. Therefore, your ability to monitor network performance determines your success in fine-tuning network performance based on your business requirements. The monitoring tools are designed to help you fine-tune your network performance.

When and where your network has peaks, bursts and bottlenecks is hard to predict. NetXplorer enables you to see these peaks in both real time and historically, which is crucial to managing these unwanted phenomena.

Monitoring Reports in NetXplorer are generated from the GUI by using the following tools:

Real-Time Monitoring

NetXplorer's real-time monitoring tool provides real-time data, enabling you to monitor applications, protocols, users and servers and to enforce the most suitable QoS Enforcement Policy. Real-time monitoring enables you to identify possible problems and traffic peaks as they occur so that corrective actions can be taken in a timely manner.

In Real-Time Monitoring, data is available for four hours at 30 second resolution and for two days at five minutes resolution. When a 30 second resolution graph is chosen, the graph will auto-refresh once the “restart” short cut button in the short-cut tool bar has been clicked.

The Real-Time Monitoring application is an optional component of NetXplorer. You can opt to use Real-Time Monitoring with one, some or all of the NetEnforcers or Service Gateways in your network. The Real-Time Monitoring application is licensed separately per NetEnforcer, or per Core Controller on a Service Gateway, and is enabled by entering an appropriate key on each device.

NOTE Real-Time Monitoring graphs are licensed per core controller blade on the Service Gateway. The license is required for all CC blades in the SG-Sigma platform in order to enable real time monitoring.

NOTE Real-Time Monitoring graphs in a 30 seconds resolution are not available when a Service Gateway has been configured to work with the “subscriber” reduction profile. For more details, see the NetXplorer Installation and Admin Guide, Chapter 5.

Long-Term Reporting

The ability to monitor applications and users over a long period of time is crucial in order to employ traffic priorities based on business requirements. NetXplorer's Long-Term Reporting application enables you to monitor your network's activity and identify trends over an extended period of time by storing monitoring data and sending the graphs to the designated recipient by email.

In Long-Term Reporting, data is available for three months at one hour resolution and for one year at daily resolution.

NOTE When you select a NetEnforcer (or one of its subcomponents) in the Navigation tree, the Monitoring and Reporting options are enabled or disabled according to whether or not the selected NetEnforcer has been licensed for the proper option.

Mobile Analytics

A special set of reports available on the Network level, specifically designed for Mobile Operators. Mobile Analytics reports provide information concerning mobile data use with the ability to generate graphs concerning mobile subscribers, devices and signaling information.

Mobile Analytics is only available when the following requirements are met:

- Allot's Subscriber Manager Platform is deployed in PCC Mode
- At least one STC is installed
- A special license key for Mobile Analytics has been purchased for the in-line platforms. Contact Allot Customer Support for details.

Ad-hoc generation of each of Mobile Analytics graphs can take a significant amount of time, depending on the size of your network and the amount of mobile traffic, therefore Allot recommends that they be generated as pre-scheduled User Defined Reports.

For instructions regarding configuring and enabling Mobile Analytics, consult the SMP Installation and Administration Guide Chapter concerning Mobile Analytics.

NOTE By default, the entirety of the data for Mobile Analytics only becomes available after 25 hours. Any report which is created which displays information for the last 25 hours will contain partial data (open sessions are not shown). In some cases, depending on the specific deployment parameters, this time period can be lessened by configuration. Contact support@allot.com if this is necessary.

Monitoring Interface

The maximum number of graphs that may be open in the GUI at any one time is 15.

Different graphs are available at each level in the Network, consequently the submenu options available for **Real-Time Monitoring** and **Long Term Reporting** vary according to the item selected.




Mobile Analytics graphs are only available on the Network level.












Quick Access Toolbar



Figure 7-1: Quick Access Toolbar – Monitoring Reports

The following icons are displayed in the NetXplorer Quick Access Toolbar when a monitoring graph is open:

BUTTON	DESCRIPTION
 Show Data by	Displays monitoring data according to total, incoming or outgoing bandwidth, incoming or outgoing packets, or live, new or dropped connections. Refer to Data Display Options, page 7-97.
 Chart Style	Displays the graph in Chart View. Refer to Graph Views, page 7-10.
 Display	<p>Enables you to hide/show the grid, configure the legend convention, hide/show All Others data, switch between bandwidth units, show the values in the actual graph (pie graphs only), show the values in the legend or show the full name in the X-Axis.</p> <p>NOTE Arrows buttons appear in the upper border between the graph and legend which may also be used to show and hide the legend information.</p>

BUTTON	DESCRIPTION
 Table View	Displays the graph in Table View. Refer to Graph Views, page 7-10.
 Errors Log	Displays a log file of any errors connected to the selected report.
 Backward	Displays the graph data for the previous graph period, and continues from that point onward.
 Forward	Redisplays the graph data to reflect the real-time data. (This option is enabled if a previous sample period has been displayed in a graph.)
 Restart Automatic Update	Starts the visual update of the graph (which is off by default). Once the graph is being automatically updated, this button is replaced by the Stop Automatic Update button. While a graph is being automatically updated, this icon appears by the title of the graph. (This option is enabled for real-time monitoring graphs only.)
 Stop Automatic Update	Suspends the visual update of the graph. (This option is enabled for real-time monitoring graphs only.)
 Add to Favorites View	Adds the current Monitoring graph to Favorite View.
 Add to Reports	Adds the current Monitoring graph to Reports.
 Graphs List	Displays a list of the currently open graphs in the Monitoring system, enabling you to easily navigate between the open graphs.
 Tile	Tiles all open graphs
 Cascade	Displays all open graphs as a Cascade

Menu Options

The following options are available when you select a graph in the Application Details area and open the Action menu from the Menu Bar, or Right-click on an open graph:

BUTTON	DESCRIPTION	RIGHT CLICK MENU	ACTION MENU
Show Data by	Displays monitoring data according to incoming or outgoing bandwidth, incoming or outgoing packets, or live, new or dropped connections. Refer to Data Display Options, page 7-97.	√	√
Chart Style	Displays the graph in the selected type of Chart View. Refer to Graph Views, page 7-10.	√	√
Display	Enables you to hide/show the grid, configure the legend convention, hide/show All Others data, switch between bandwidth units, show the values in the actual graph (pie graphs only), show the values in the legend or show the full name in the X-Axis. NOTE Arrows buttons appear in the upper border between the graph and legend which may also be used to show and hide the legend information.	√	√
Table View	Displays the graph in Table View. Refer to Graph Views, page 7-10.	√	√
Errors Log	Displays a log file of any errors connected to the selected report.	√	√
Backward	Displays the graph data for the previous graph, and continues from that point onward.	√	√
Forward	Displays the next sample.	√	√
Stop Update	Suspends the visual update of the graph. Click Stop Update again to restore the visual update. (This option is enabled for real-time monitoring graphs only.)	√	√

BUTTON	DESCRIPTION	RIGHT CLICK MENU	ACTION MENU
Drill Down	Drills down within any displayed graph to view a cross-section of data for a specific entity represented in the graph. For example, upon examining a Pipes Distribution graph for a specific NetEnforcer, you may want to view the breakdown of utilization for a specific pipe.	√	X
Edit	Opens the Enforcement Policy Editor to edit the selected NetEnforcer or Service Gateway, Line, Pipe or VC in the graph.	√	X
Add to Favorite View	Adds the current graph to the Favorite View setup.	√	√
Add to Reports	Adds the selected Monitoring graph to Reports.	√	√
Export	Allows you to export the current graph as a .csv, .xml, .png, .pdf, .jpg or .html file. NOTE If the graph has a sliding horizontal axis, the exported .jpg will be scaled to show the entire graph.	√	√
Export to CLI	Allows you to export a text file which contains the Monitoring CLI command for generating the current graph. This command may then be edited to change the properties of the graph.	√	√
Print	Prints the current graph.	√	√
Close	Closes the selected graph.	√	√
Full Screen	Enlarges the graph to full size of your screen. Double click the full screen graph to return to its previous dimensions.	√	√
Properties	Displays the report/graph definition properties for the specific graph, enabling you to modify the definition, as required.	√	√

Navigation Pane

It is easy to review and generate predefined reports by opening the Reports pane in the Navigation Pane.

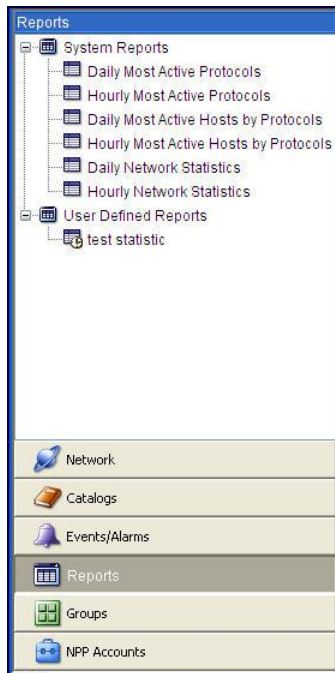


Figure 7-2: Reports Navigation Pane

From the Reports navigation pane, it is possible to access three specific forms of reports.

- **System Reports** – Key indices that are automatically defined by the NetXplorer. The following System Reports are available by default:
 - Daily Most Active Protocols on the Network level
 - Hourly Most Active Protocols on the Network level
 - Daily Most Active Hosts stacked by protocol on the Network level
 - Hourly Most Active Hosts stacked by protocol on the Network level
 - Daily Network Statistics
 - Hourly Network Statistics
- **User Defined Reports** – Customized reports that are defined and stored by the user for quick access. For more information see Scheduling a Report on page 7-88.

- **Compound Reports** – Reports that include more than one User Defined Report, designed to be generated automatically at the same time. Compound Reports are indicated by an orange Report icon. For more information see **Compound Reports** on page 7-95.

Report Folders

Folders can be defined in the Reports Navigation pane in order to make User-Defined reports easier to categorize. The folders allow the user to categorize the reports by any criteria they wish.

To create a Report Folder:

1. Open the Reports Navigation pane.
2. Select **Actions > New > Report Folder**
3. The Report Folder Properties dialog box opens, allowing you to enter a name for the folder.

Click **Save** to add the folder to the Reports navigation pane.

4. The new folder appears in the Reports navigation pane.
5. To delete a folder, right click on the folder and select **Delete**. This will also delete any reports stored in the folder.

Graph Views

By default, Monitoring Reports are displayed in a chart or graph. However, you can also display the values in table format. These different views are called Chart View and Table View.

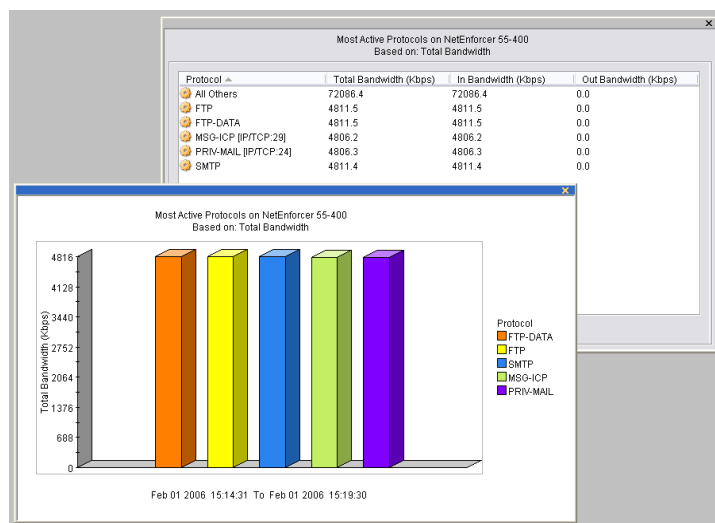


Figure 7-3: Graph Views

When in Chart View, you can alternate the layout style of the graph between a Bar chart and a Pie chart, or between a Line chart and a Stack Area chart. Different graphs have different styles. For example, a Pipes Distribution graph can be displayed as a Line chart or Stack Area chart. A Most Active Hosts graph can be displayed as a Bar chart or Pie chart. These different graph styles are reflected by icons in the upper right hand corner of the Reporting dialog box.

NOTE Graph appearance may vary slightly depending upon the graphics settings of the client computer.

Following are examples of different graph styles.

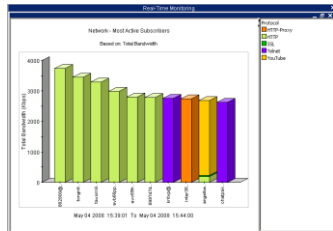


Figure 7-4: Bar Chart

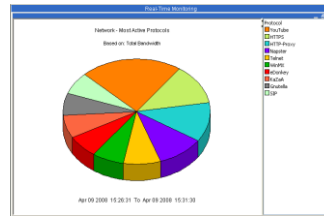


Figure 7-5: Pie Chart

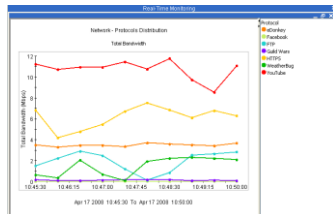


Figure 7-6: Line Chart

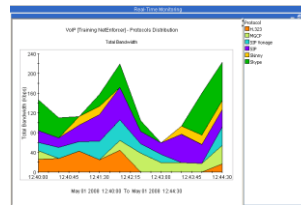


Figure 7-7: Stack Area Chart

Monitoring Reports Graphs

This section describes the graph functionality that is available in Real-time monitoring and Long-Term Reporting in NetXplorer. The following Monitoring Report subjects are available.

Core Graphs

Using one or more graphs from the core graphs category will give you a full picture of your network statistics and its behavior. Those graph display the bandwidth so you can see it as if you are inside the physical line. This category contains the following graphs:

- **Statistics Reports:** Displays traffic statistics.
- **Protocols Reports:** Displays data concerning specific protocols or groups of protocols on the Network.
- **Policy Entities Reports:** Displays data concerning a specific Policy Entity or type of Entity on the Network. These include NetEnforcers/Service Gateways, Lines, Pipes and Virtual Channels.
- **Hosts/Conversations Reports:** Display the most active host objects over the period defined or the distribution of selected hosts over the period defined.

Additional Graphs

Using the additional graphs allows you to go in depth when investigating your network, and to adjust your view to see specific details in your network. This category contains the following graphs:

- **Utilization Reports:** Displays how much of an object's available bandwidth is being used.
- **Typical Time Reports:** Display the average of selected parameters over a typical day or a typical week, over the selected time period. All standard Real-Time and Long-Term graphs may be generated as Typical Time reports.
- **Popularity Reports:** Displays data concerning the popularity of certain objects or a type of object on the Network.
 - **Pipe Popularity Reports:** Display the most popular Pipes on your network.
 - **VC Popularity Reports:** Displays the most popular VCs on your network.
 - **Average Protocol Popularity (Average Most Popular Protocols):** Displays the most popular Protocols, based on an average of all subscribers.
- **Services Reports:** These reports pertain to services available on the NetXplorer.

- **WebSafe Traffic:** Displays the amount of traffic being used by the WebSafe service.
- **HTTP:** Displays very detailed information on domain names access distribution by various parameters.
- **Integrated Services:** Displays detailed information on Integrated Services use.
- **Asymmetry Traffic Report:** Displays the amount of traffic being sent via Asymmetry links.
- **Percentile Reports:** These reports express usage by percentile for billing and analysis purposes.
- **95th Percentile:** The 95% value (metered bandwidth) is used for billing by most Tier-1 operators and carriers.
- **Bandwidth Usage Percentiles:** Displays the average usage for different subscriber groups according to the percentile of the used bandwidth.
- **Percentile Protocols:** Displays the protocol distribution of the average bandwidth per specific subscribers/hosts group.
- **VoIP Report:** Indicates the amount of time VoIP applications are used on your network.

Subscriber Graphs

SMP Graphs are only available when an SMP is enabled on the network.

- **SMP Reports:** These reports are only available if both SMP and Quota Management are enabled. They are available as both Real-Time and Long-Term Reports.

SMP Reports include the following:

- Subscriber Reports
- Subscriber Usage Reports
- Service Plans Usage Reports
- Service Plans Popularity Reports
- Quota Analysis Reports
- Cellwise Reports
- **Mobile Analytics Reports:** These reports are only available if both an SMP in PCC mode and Mobile Analytics are enabled. They are not available through Real-Time Monitoring or Long-Term Reporting but only via the Mobile Analytics feature.

Mobile Analytics include the following reports:

- Session Signaling

- Roaming Out Volume
- Service Plans Metrics
- Service Plans Transits
- Subscriber Volume Percentiles
- Session Bitrate
- Session Duration

Report Descriptions

Core Graphs

Statistics Reports

Statistics reports display the bandwidth consumed by the entire network or specific entities in your network (NetEnforcers, Lines, Pipes or Virtual Channels). Statistics reports can be generated as Real Time Monitoring graphs or Long-Term Reporting reports

NOTE Although default statistics reports indicate total bandwidth consumption, the graph display can be modified to display data based on inbound or outbound bandwidth consumed; live or new connections; or inbound or outbound packets transmitted.

To generate a Statistics Report

1. In the Navigation pane, right-click an entity in the Navigation tree for which you want to generate a graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select Statistics. The Real-Time Monitoring: Statistics or Long Term Reporting: Statistics Properties dialog is displayed. The Statistics Report icon is displayed in the upper right hand corner of the dialog box.

The Time tab is open by default.

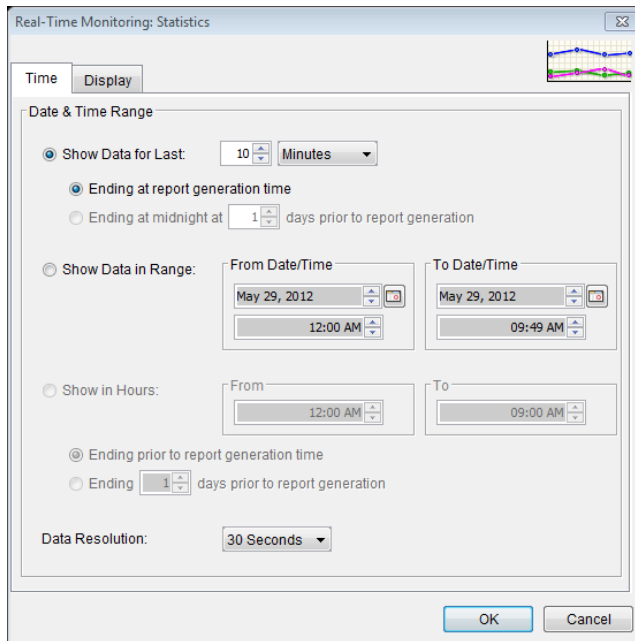


Figure 7-8: Real-Time Monitoring: Statistics dialog, Time tab

3. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

4. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.

NOTE When generating a long-term monitoring report, the available options are (1 hour, 1 day, 1 month).

5. Click the **Display** tab. The following dialog is displayed.

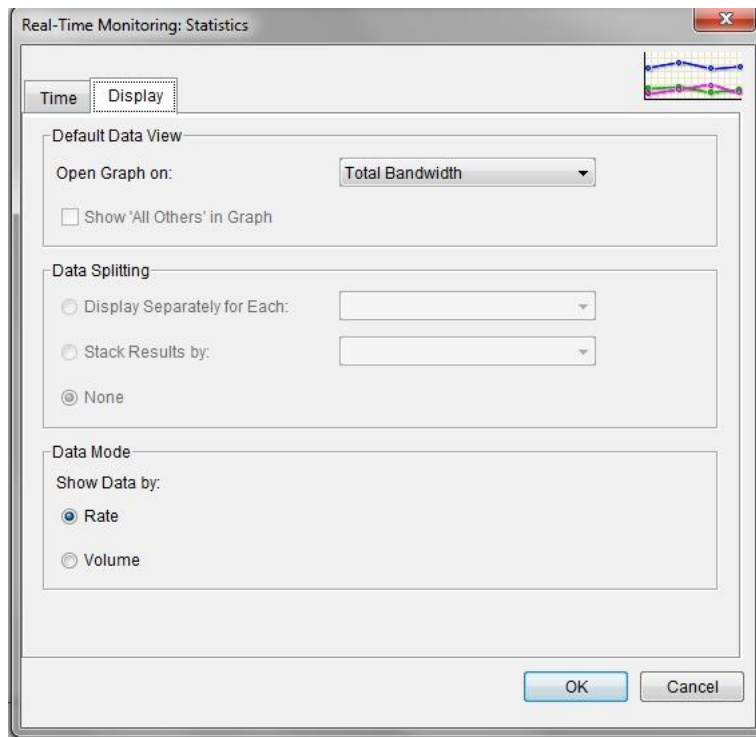


Figure 7-9: Real-Time Monitoring: Statistics dialog, Display tab

6. From the **Open Data On** dropdown list, select the parameter you wish to see Statistics about (Total Bandwidth, In Bandwidth, Out Bandwidth, Live Connections (30 Second intervals only), New Connections, Dropped Connections, In Packets or Out Packets).
7. In the **Data Splitting** area, you can opt to see the stats for specific network entities separately.
8. In the **Data Mode** area, you can opt to display data by Rate or Volume.
9. Click **OK** to generate the graph.

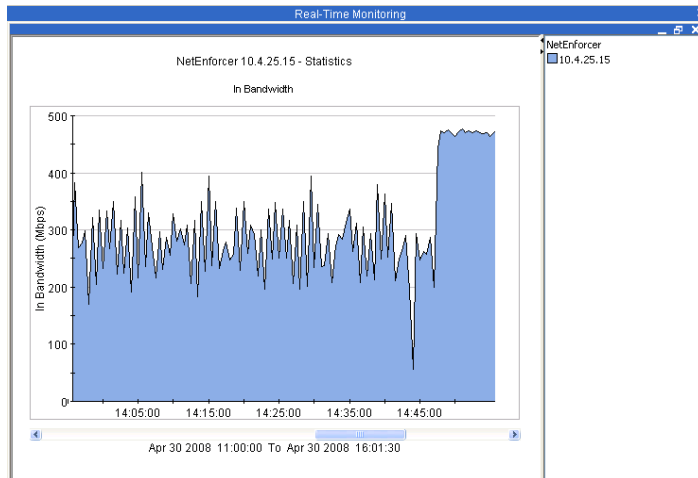


Figure 7-10: NetEnforcer Statistics

Protocol Reports

Protocol reports display information concerning specific Protocols in your network.

Protocol reports can be generated as Real Time Monitoring graphs or Long-Term Reports.

There are two types of Protocol Reports:

- A **Most Active Protocols** which indicates the most popular protocols on a Network or Object level. This report can be displayed as a bar chart, or as a line/stack area chart showing the distribution of protocols over time.

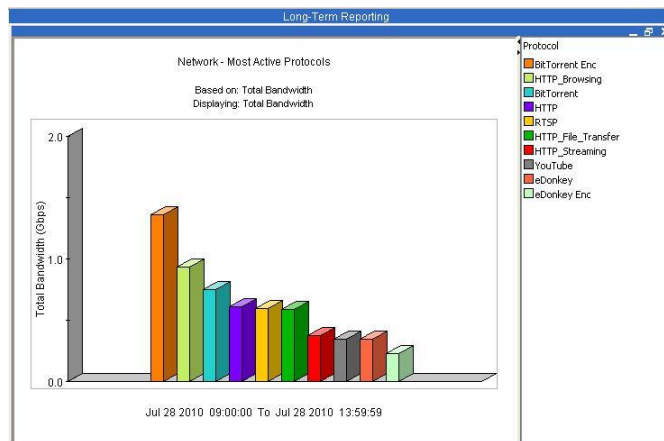


Figure 7-11: Most Active Protocols on Network – Bar Chart

- A **Distribution of Specific Protocols** report which shows the selected protocol's traffic over a set period of time. This report can be displayed as a line/stack area chart, or as a pie chart which shows the proportionate

distribution of different services or service groups, where 100% represents all of the services or service groups chosen

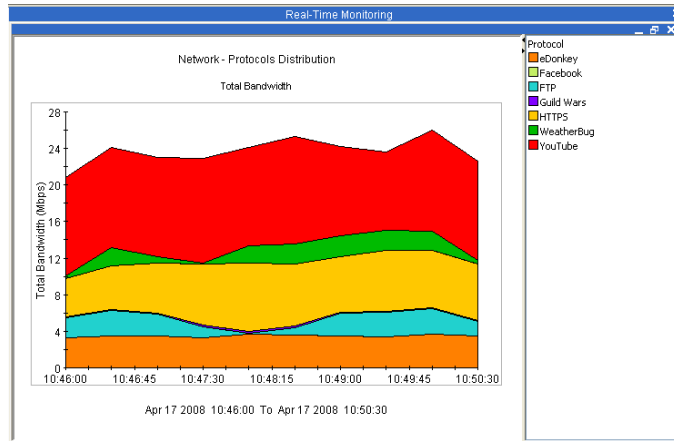


Figure 7-12: Distribution of Specific Protocols on Network – Data Displayed Over Time

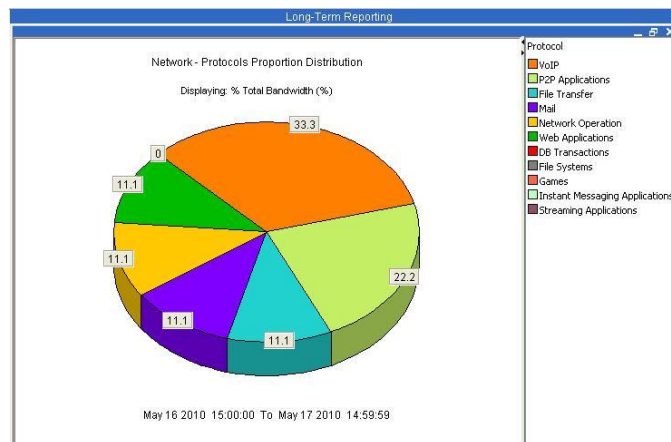


Figure 7-13: Distribution of Specific Protocols on Network – Data Displayed for Period as a Whole

To generate a Protocol Report:

1. In the Navigation pane, right-click a level in the Navigation tree for which you want to generate a graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select Protocols from the drop down menu.

The Real-Time Monitoring or Long Term Reporting dialog is displayed. The Stacked Bar Report icon is displayed in the upper right hand corner of the dialog box.

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display. Once minimum parameters have been defined, a report may be generated at any time by clicking the OK button

The Time tab is open by default.

Figure 7-14: Long-Term Reporting: Protocols dialog box, Time tab

3. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

4. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.

NOTE When generating a Long-Term Report, the available options are 1 hour, 1 day or 1 month.

5. Click the **Objects** tab. The following dialog is displayed.

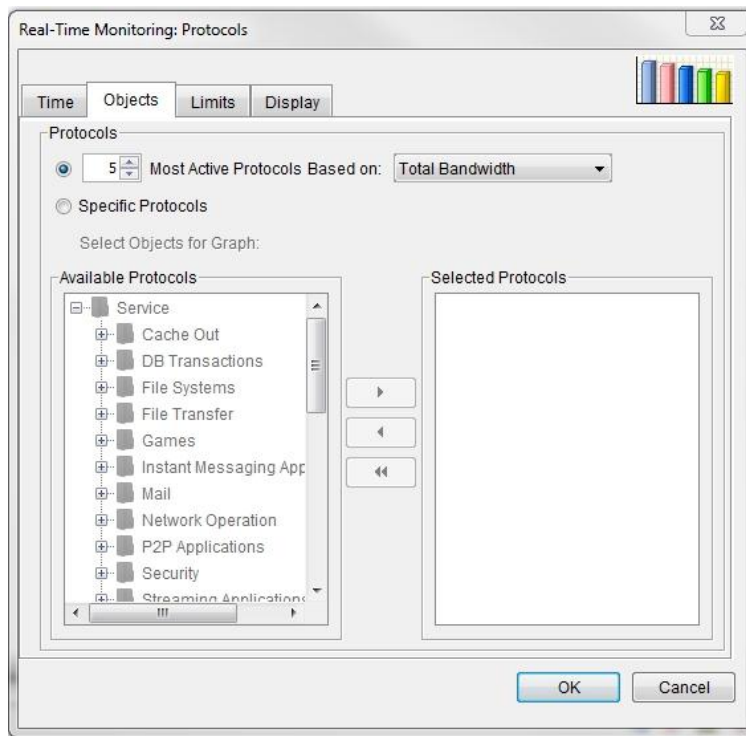


Figure 7-15: Real-Time Reporting: Protocols dialog, Objects tab

6. There are two different Protocols graphs that may be generated, based on selection on the Objects tab:
 - To generate a **Most Active Protocols** report select the upper radio button, set the number of objects you wish listed, and set the parameter you wish the report to be based on (Total Bandwidth, In Bandwidth, Out Bandwidth, Live Connections (30 Second intervals

only), New Connections, Dropped Connections, In Packets or Out Packets).

- Select the **Specific Protocol** radio button to generate a graph showing only the protocols selected in the **Select Objects for Graph** area.
7. Use the arrow keys in the **Select Objects for Graph** area to move individual services or service groups from the **Available** list to the **Selected** list. The Service Groups are all located at the top of the list. (This step is not available when defining a **Most Active Protocols** graph)

NOTE

It is not recommended to generate Protocols Distribution reports on very large Pipes or VC templates in order not to decrease performance.

8. Click the **Limits** tab. The following dialog is displayed.

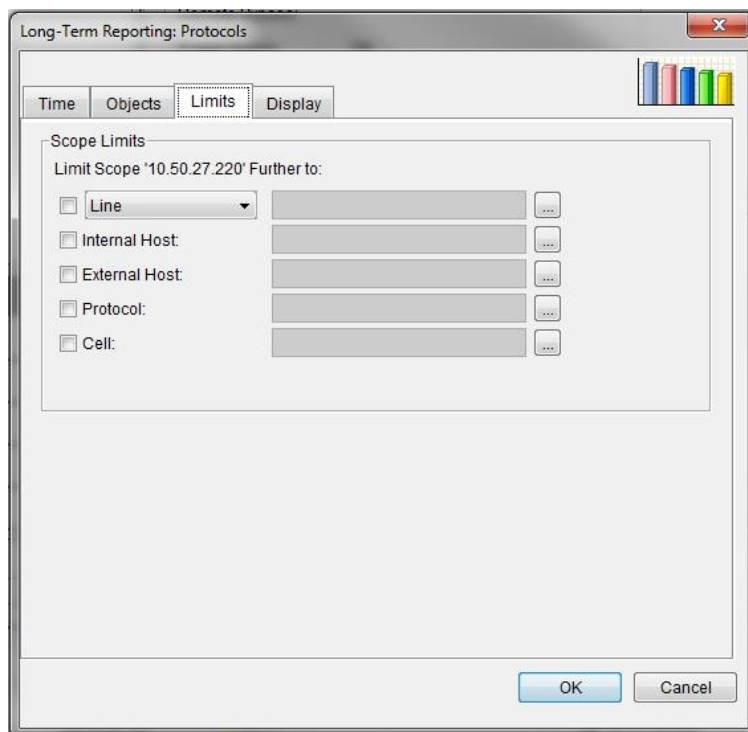


Figure 7-16: Long-Term Reporting: Protocols dialog, Limits tab

9. Use the Scope Limits parameters to refine your report to include only certain objects.

Click the appropriate check box, and click the ... button to browse the list of available objects of that type. Use the arrow keys to move objects from the **Available** list to the **Selected** list.

10. Click the **Display** tab. The following dialog is displayed.

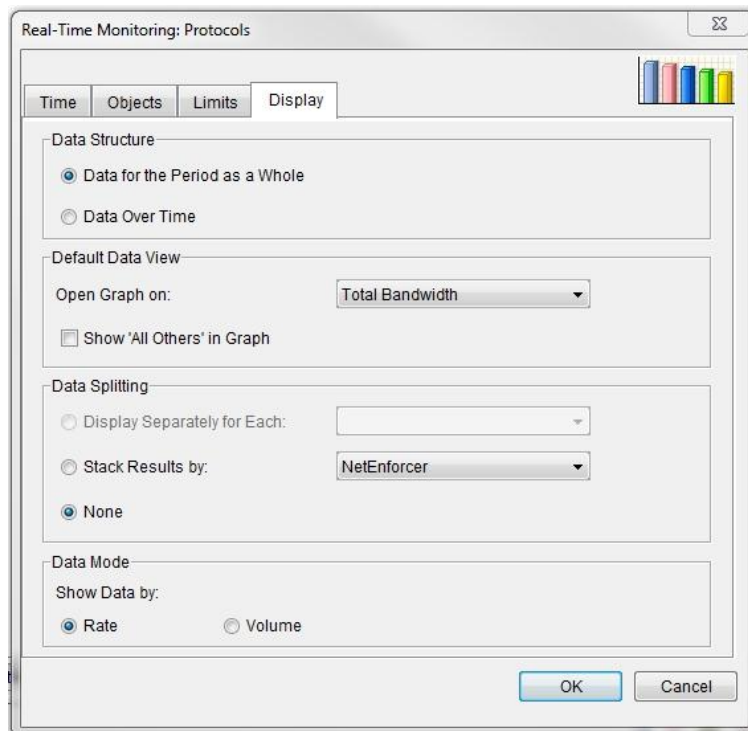


Figure 7-17: Long-Term Reporting: Pipes dialog, Display tab

11. In the Data Structure area, there are two available options:
 - **Data for the Period as a Whole:** When you have specified protocols in the Objects tab, this radio button will generate a pie chart which shows the proportionate distribution of different services or service groups, where 100% represents all of the services or service groups chosen. When you have specified most active protocols in the Objects tab, this radio button will generate a bar chart for the whole period selected.
 - **Data Over Time:** When you have specified protocols in the Objects tab, this radio button will generate a graph presents the distribution of these protocol's traffic over a set period of time. When you have specified most active protocols in the Objects tab, this radio button will present the distribution over time of the most active protocols as calculated in the specified time period.
12. From the **Default Data View** area, open the **Open Data On** dropdown list and select the parameter you wish to see Statistics about (Total Bandwidth, In Bandwidth, Out Bandwidth, New Connections, Dropped Connections, In Packets or Out Packets).
13. Select the **Show "All Others" in Graph** radio button to display all elements not selected in a single "All Others" category.

14. In the **Data Splitting** area, you can opt to see the stats for specific network entities separately.
15. In the **Data Mode** area, you can opt to display data by Rate or Volume.
16. Click **OK** to generate the selected graph.

Policy Entity Reports

Policy Entity reports display information concerning specific entities in your network (NetEnforcers/Service Gateways, Lines, Pipes or Virtual Channels). In addition, Policy Entity reports can show information concerning anything below the selected entity in the network hierarchy. For example, if you select a NetEnforcer or Service Gateway, you can also create reports that deal with its Lines, Pipes and VCs.

Policy Entity reports can be generated as Real Time Monitoring graphs or Long-Term Reports.

To generate an Policy Entity Report

1. In the Navigation pane, right-click a level in the Navigation tree for which you want to generate a graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select the entity type you wish to generate a report concerning. For example, right clicking a Line and selecting Protocols from the drop down menu will generate reports about Protocols on that Line.

The Real-Time Monitoring or Long Term Reporting dialog is displayed. The Stacked Bar Report icon is displayed in the upper right hand corner of the dialog box.

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display. Once minimum parameters have been defined, a report may be generated at any time by clicking the OK button

The Time tab is open by default.

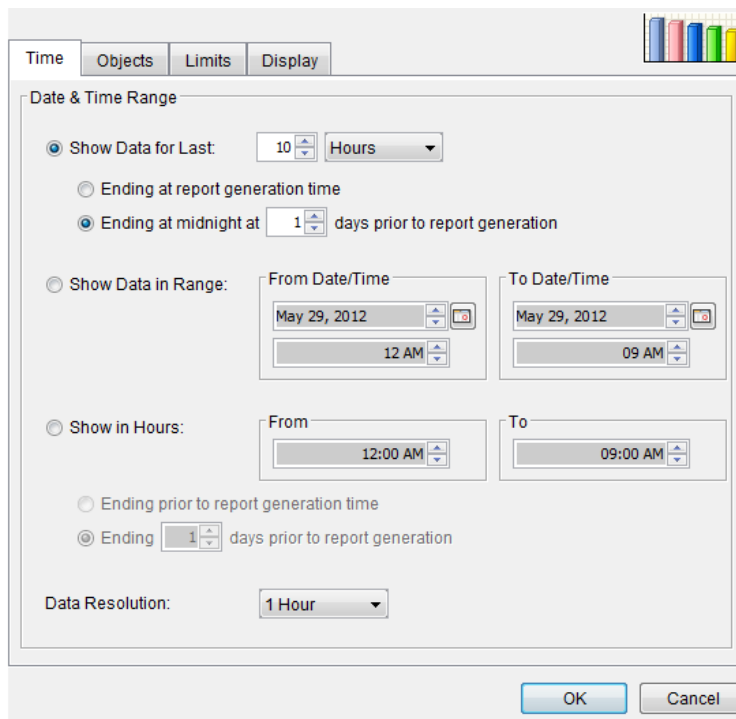


Figure 7-18: Long-Term Reporting: Pipes dialog box, Time tab

3. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

4. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
5. Click the **Objects** tab. The following dialog is displayed.

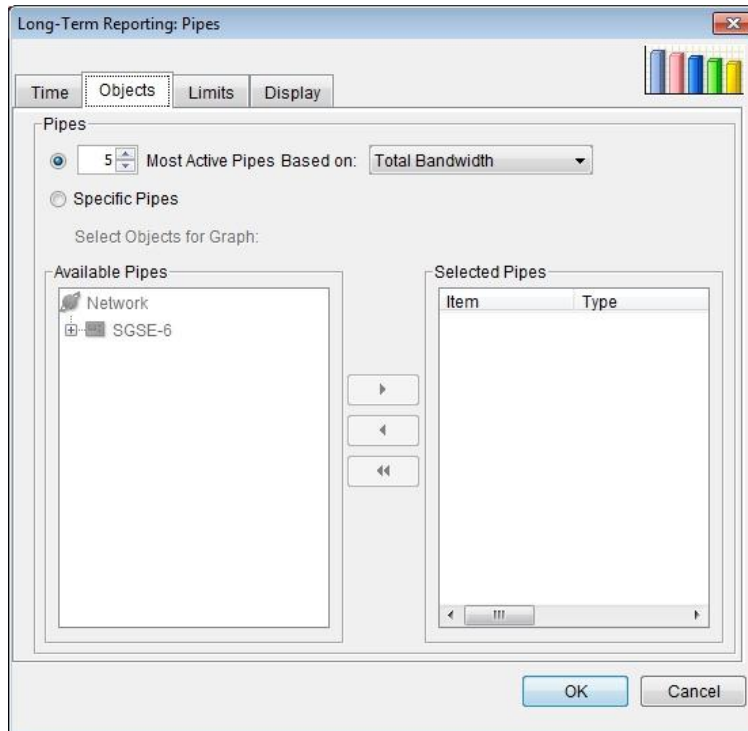


Figure 7-19: Long-Term Reporting: Pipes dialog, Objects tab

6. To generate a **Most Active...** report, select the upper radio button, set the number of objects you wish listed, and set the parameter you wish the report to be based on (Total Bandwidth, In Bandwidth, Out Bandwidth, Live Connections (30 Second intervals only), New Connections, Dropped Connections, In Packets or Out Packets).
7. To generate other reports based on objects of the type selected, click the **Specific Objects** radio button.

Use the arrow keys to move objects from the **Available** list to the **Selected** list.

NOTE It is not recommended to generate distribution reports on very large Pipes or VC templates in order not to decrease performance.

8. Click the **Limits** tab. The following dialog is displayed.

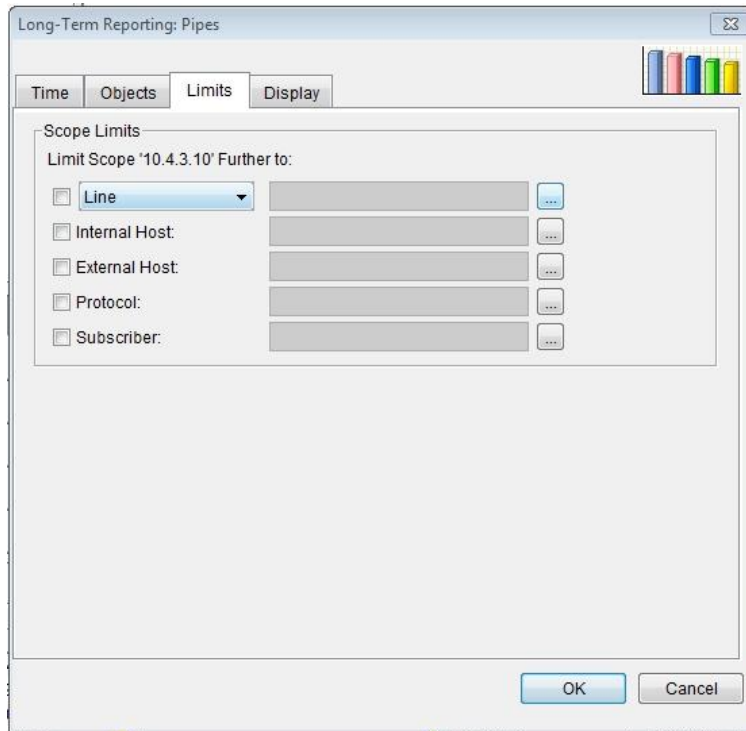


Figure 7-20: Long-Term Reporting: Pipes dialog, Limits tab

9. Use the Scope Limits parameters to refine your report to include only certain objects, Internal Hosts, External Hosts, Protocols or Subscribers (if available).

Click the appropriate check box, and click the ... button to browse the list of available objects of that type. Use the arrow keys to move objects from the **Available** list to the **Selected** list.

10. Click the **Display** tab. The following dialog is displayed.



Figure 7-21: Long-Term Reporting: Pipes dialog, Display tab

11. In the Data Structure area, there are two possible options:
 - **Data for the Period as a Whole:** This option is used with Most Active reports and will generate a pie chart which shows the proportionate distribution of traffic over different Entities, where 100% represents all of the objects chosen.
 - **Data Over Time:** This option is used with Distribution reports and will generate a graph which presents the distribution of traffic over the selected Entities during a set period of time.
12. From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Total Bandwidth, In Bandwidth, Out Bandwidth, New Connections, Dropped Connections, In Packets or Out Packets).
13. Select the **Show “All Others” in Graph** radio button to display all elements not selected in a single “All Others” category.
14. In the **Data Splitting** area, you can opt to see the stats for specific network entities separately.
15. In the **Data Mode** area, you can opt to display data by Rate or Volume.
16. Click **OK** to generate the graph.

Hosts/Conversations Reports

Hosts/Conversations reports can be used to display the most active host objects over the period defined or the distribution of selected hosts over the period defined. These can include All Hosts, Internal Hosts, External Hosts and/or Conversations

Host/Conversations reports can be generated as Real Time Monitoring graphs or Long-Term Reports.

To generate an Host/Conversations Report

1. In the Navigation pane, right-click a level in the Navigation tree for which you want to generate a graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select the Host/Conversation type you wish to generate a report concerning. For example, right clicking a Service Gateway and selecting Hosts from the drop down menu will generate reports about Hosts on that Service Gateway.

The Real-Time Monitoring or Long Term Reporting dialog is displayed. The Stacked Bar Report icon is displayed in the upper right hand corner of the dialog box.

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display. Once minimum parameters have been defined, a report may be generated at any time by clicking the OK button

The Time tab is open by default.

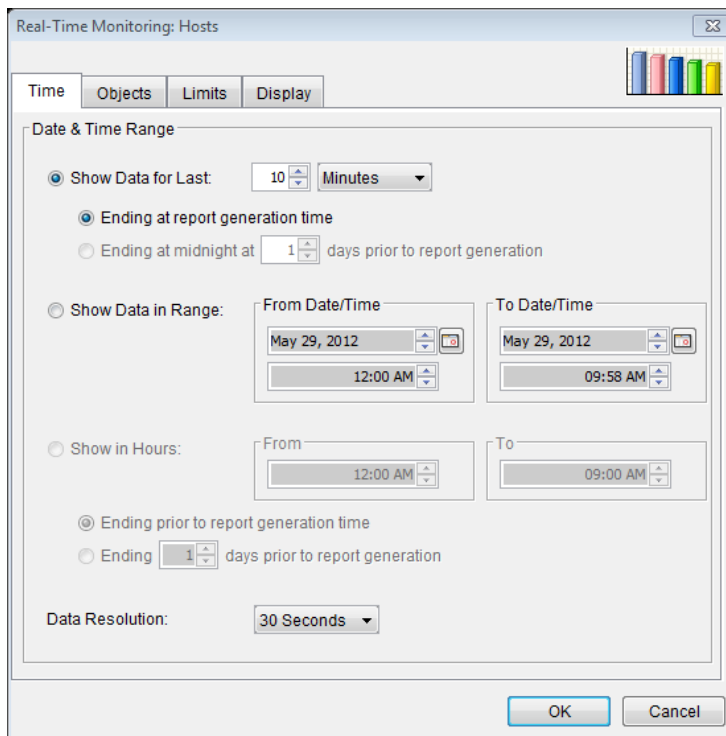


Figure 7-22: Real-Time Reporting: Hosts dialog box, Time tab

3. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

4. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
5. Click the **Objects** tab. The following dialog is displayed.

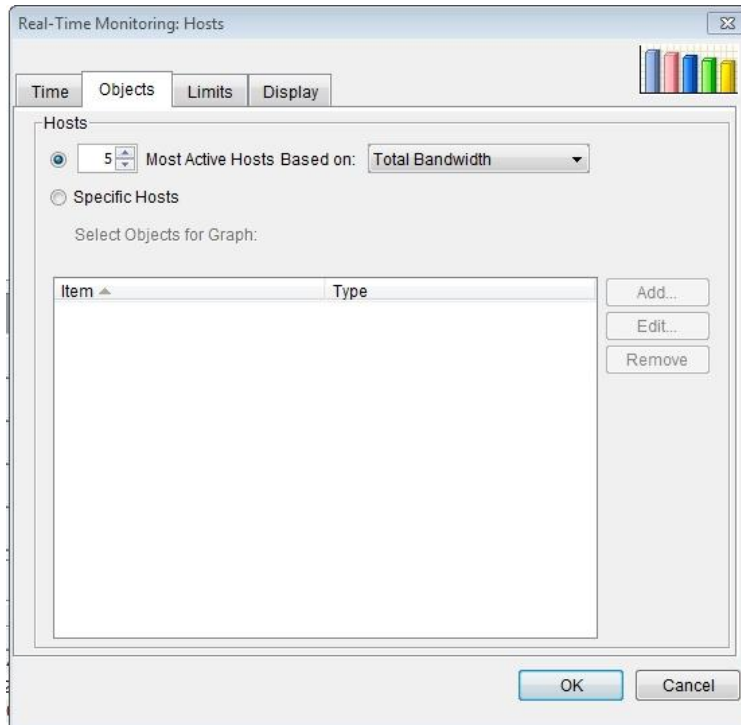


Figure 7-23: Real-Time Reporting: Hosts dialog, Objects tab

6. To generate a **Most Active...** report, select the upper radio button, set the number of objects you wish listed, and set the parameter you wish the report to be based on (Total Bandwidth, In Bandwidth, Out Bandwidth, Live Connections (30 Second intervals only), New Connections, In Packets or Out Packets).
7. To generate other reports based on objects of the type selected, click the **Specific <OBJECT>** radio button.

Use the arrow keys to move objects from the **Available** list to the **Selected** list.
8. Click the **Limits** tab. The following dialog is displayed.

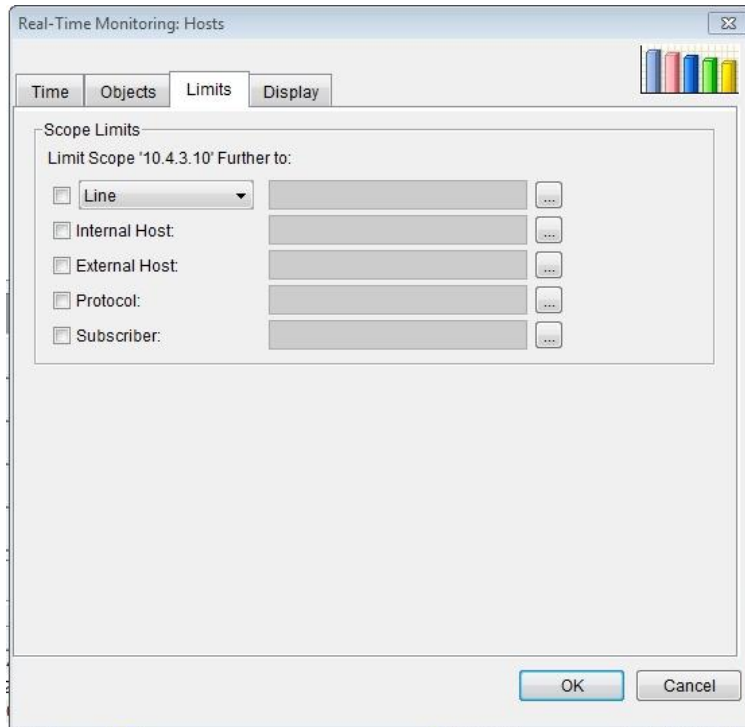


Figure 7-24: Real-Time Reporting: Hosts dialog, Limits tab

9. Use the Scope Limits parameters to refine your report to include only certain Policy Entities, Internal Hosts, External Hosts or Protocols or Subscribers (if available).

Click the appropriate check box, and click the ... button to browse the list of available objects of that type. Use the arrow keys to move objects from the **Available** list to the **Selected** list.

10. Click the **Display** tab. The following dialog is displayed.

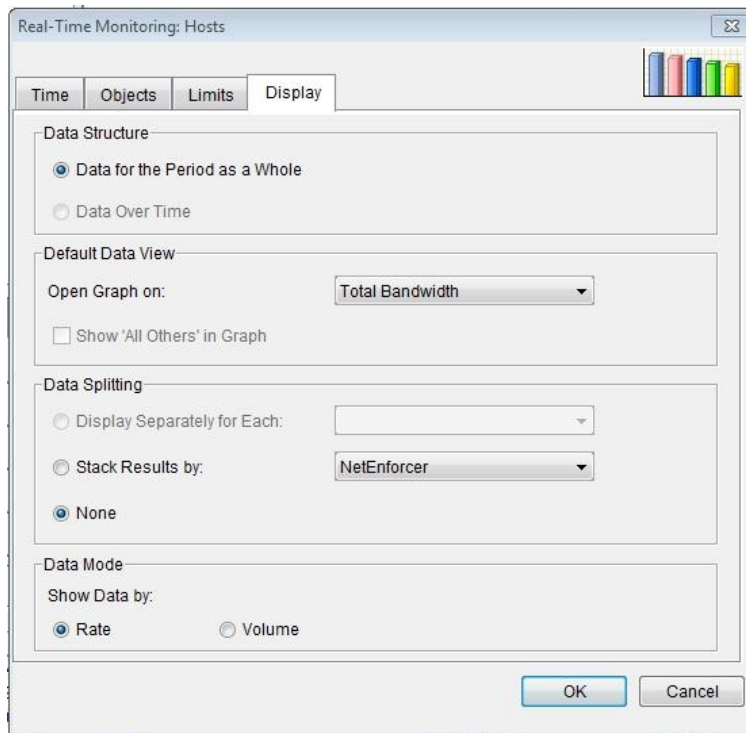


Figure 7-25: Real-Time Reporting: Hosts dialog, Display tab

11. In the Data Structure area, there are two possible options:
 - **Data for the Period as a Whole:** This option is used with Most Active reports and will generate a pie chart which shows the proportionate distribution of traffic over different objects, where 100% represents all of the objects chosen.
 - **Data Over Time:** This option is used with Distribution reports and will generate a graph presents the distribution of traffic over a set period of time.
12. From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Total Bandwidth, In Bandwidth, Out Bandwidth, New Connections, Dropped Connections, In Packets or Out Packets).
13. Select the **Show “All Others” in Graph** radio button to display all elements not selected in a single “All Others” category.
14. In the **Data Splitting** area, you can opt to see the stats for specific network entities separately.
15. In the **Data Mode** area, you can opt to display data by Rate or Volume.
16. Click **OK** to generate the graph.

Additional Graphs

Utilization Reports

The Utilization Report is available for Lines, Pipes and Virtual Channels. It displays the inbound and outbound bandwidth consumed by the selected Line, Pipe or Virtual Channel, in relation to the minimum and maximum bandwidth defined for a NetEnforcer or Service Gateway or the selected Line, Pipe or Virtual Channel.

The Utilization graph is displayed as two horizontal bars representing inbound and outbound bandwidth. You cannot change this display. The bandwidth consumed is displayed in the horizontal bar and, above the horizontal bar, the consumed bandwidth as a percentage of the maximum bandwidth is displayed.

NOTE **The Utilization graph is not available for a Line, Pipe or Virtual Channel for which no maximum bandwidth has been defined (in the QoS Catalog entry selected as the value for the QoS of the Line, Pipe or Virtual Channel).**

To generate a Utilization Report

1. In the Navigation pane, right-click a Line, Pipe or Virtual Channel in the Navigation tree for which you want to generate a graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select a Line, Pipe or Virtual Channel in the Navigation tree for which you want to generate a graph and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select a Line, Pipe or Virtual Channel in the Navigation tree for which you want to generate a graph and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select **Utilization**. The Real-Time Monitoring: Utilization or Long Term Reporting: Utilization Properties dialog is displayed. The Utilization Report icon is displayed in the upper right hand corner of the dialog box.

Figure 7-26: Real-Time Monitoring: Utilization dialog box

- To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.

NOTE When generating a Long-Term Report, the available options are 1 hour, 1 day or 1 month.

- Click OK to generate the graph.

Typical Time Reports

A Typical Time report represents the traffic in a typical time interval based on an average calculated over the selected time period. For example, in order to plan their network capacity a Service Provider may wish to see the bandwidth consumption of a specific protocol or group of protocols from hour to hour over a typical day, to see at what hours demand is highest. Alternatively, using a Typical Week report a Service Provider can view differences between weekday and weekend consumption over a typical week.

Typical Time Reports are available for all graph types and both Real-Time Monitoring and Long Term Reporting.

To display a Typical Time report:

1. In the Navigation pane, right-click the entity in the Navigation tree for which you want to generate a monitoring graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select the entity in the Navigation tree and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

The Real-Time Monitoring or Long Term Reporting submenu is displayed.

2. Select **Typical Time** to display the submenu.
3. Select the required type of graph from the submenu. The Typical Time report dialog is displayed.

The Time tab is open by default.

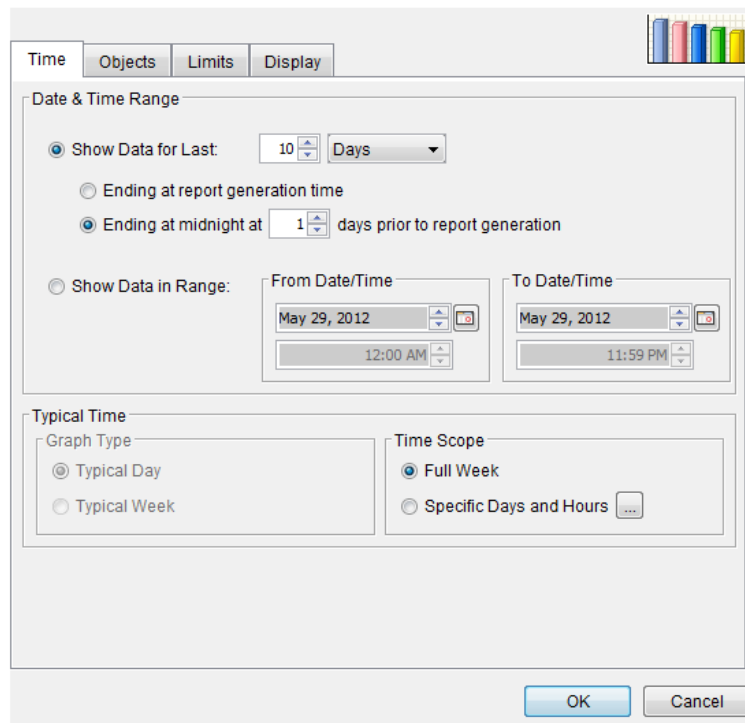


Figure 7-27: Long Term Reporting Typical Time dialog box – Time tab

4. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

5. You may opt to display a graph to display a **Typical Day** or a **Typical Week** from the selected time period using the radio buttons in the Graph Type area.
6. Select the Typical Time to be displayed. Set the Scope to **Full Week** or **Specific Days or Hours**. Click the ... button to open the Time Scope Selections dialog box.

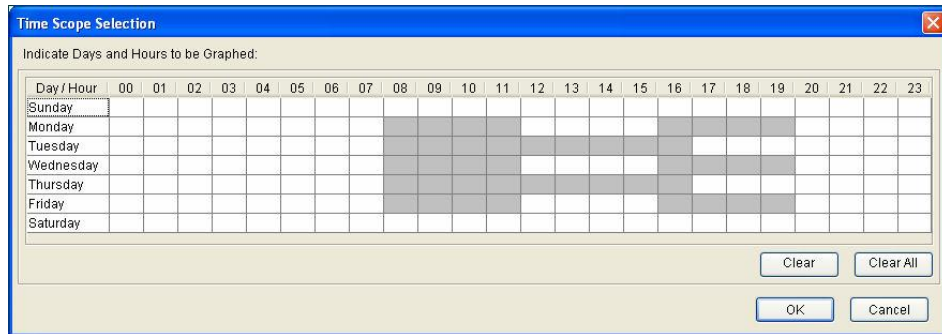


Figure 7-28: Time Scope Selections dialog box

7. Highlight the times to be included in the Typical Time Report and click **OK**.
8. All other Tabs (Objects, Limits and Display) are configured as they are in other Object reports, see page 7-21.
9. Click **OK** to open the graph.

Popularity Reports

Rather than quantifying objects by bandwidth or packets, Popularity Reports evaluates traffic by number of subscribers or IPs. A Popularity Report concerning subscribers is only available if the Subscriber Management Platform is enabled.

Popularity Reports are available in Long-Term Reporting only.

Most Popular graphs include:

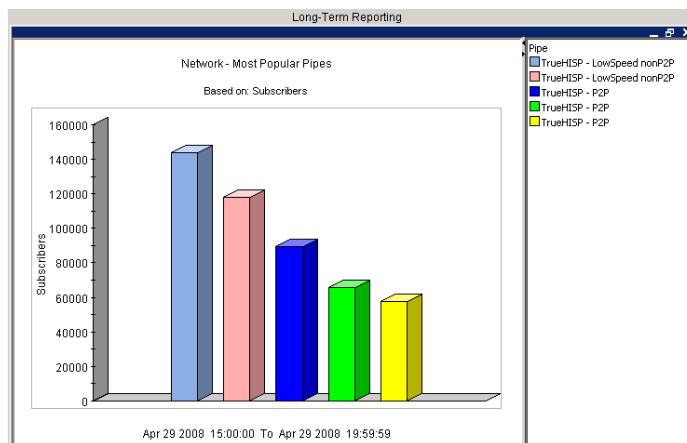


Figure 7-29: Most Popular Pipes on Network – Bar Chart

- **Pipe Popularity:** This option generates a Most Popular Pipes monitoring graph which displays the most popular Pipes based on the number of subscribers. This graph is available on the Network, NetEnforcer and Line levels.

- **Virtual Channel Popularity:** This option generates a Most Popular VCs monitoring graph which displays the most popular VCs based on the number of subscribers. This graph is available on the Network, NetEnforcer, Line and Pipe levels.
- **Average Protocol Popularity (Average Most Popular Protocols):** This monitoring graph displays the most popular Protocols, based on an average of all subscribers. This graph is available on the Network and NetEnforcer/Service Gateway levels for those devices that have first enabled “service” bucket collection. For more information see the CLI chapter in the Hardware Guide for that device.

To generate an Popularity Report

1. In the Navigation pane, right-click a level in the Navigation tree for which you want to generate a graph and select **Long Term Reporting**.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then select **Long Term Reporting** from the View menu.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then click the **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select Pipe Popularity, Virtual Channel Popularity or Average Protocol Popularity from the submenu.

The Long Term Reporting dialog is displayed. The Report Type icon is displayed in the upper right hand corner of the dialog box.

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display. Once minimum parameters have been defined, a report may be generated at any time by clicking the OK button

The Time tab is open by default.

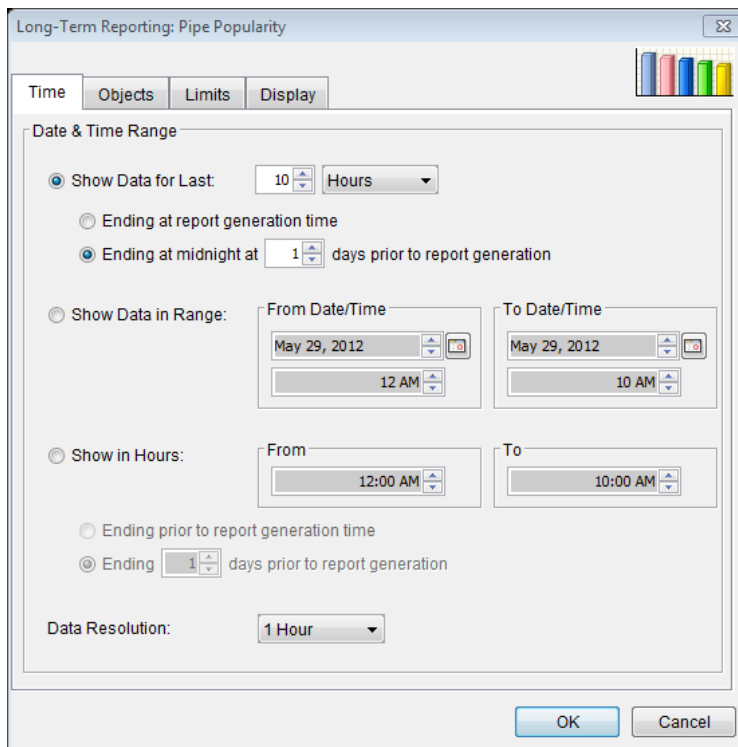


Figure 7-30: Long-Term Reporting: Pipe Popularity dialog box, Time tab

- To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
- Click the **Objects** tab. The following dialog is displayed.

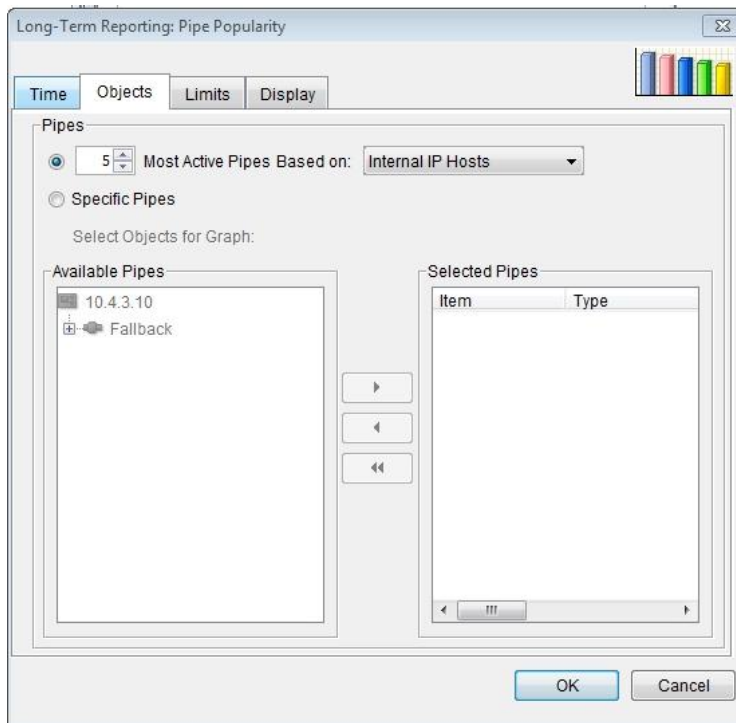


Figure 7-31: Long-Term Reporting: Pipe Popularity dialog, Objects tab

6. To generate a **Most Active...** report, select the upper radio button, set the number of objects you wish listed, and set the parameter you wish the report to be based on. In Pipe Popularity and Virtual Channel Popularity reports only Internal IP Hosts is available, and in Average Protocol Popularity reports only Internal Subscribers is available.
7. To generate other reports based on objects of the type selected, click the **Specific <OBJECT>** radio button.
Use the arrow keys to move objects from the **Available** list to the **Selected** list.
8. Click the **Limits** tab. The following dialog is displayed.

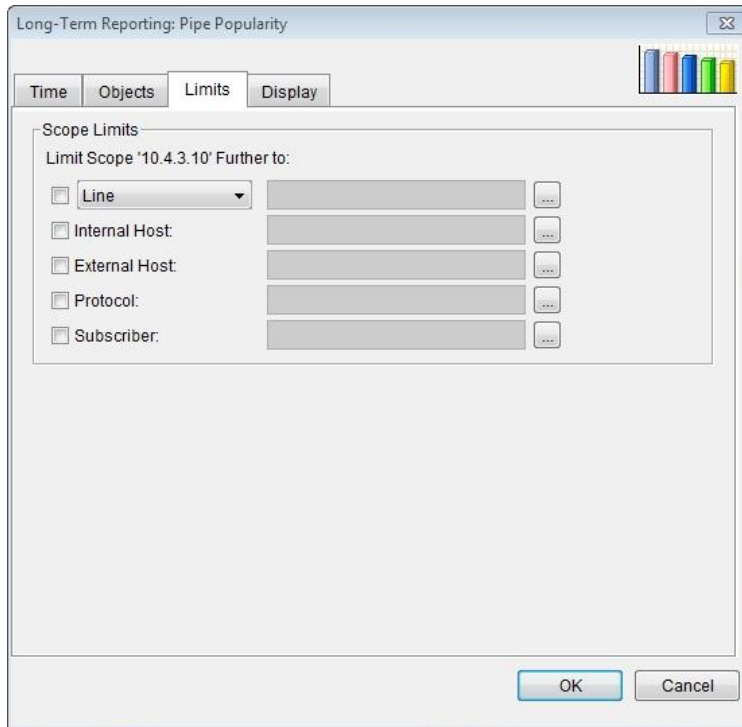


Figure 7-32: Long-Term Reporting: Pipe Popularity dialog, Limits tab

9. Use the Scope Limits parameters to refine your report to include only certain Policy Entities, Internal Hosts, External Hosts or Protocols or Subscribers (if available).

Click the appropriate check box, and click the ... button to browse the list of available objects of that type. Use the arrow keys to move objects from the **Available** list to the **Selected** list.

10. Click the **Display** tab. The following dialog is displayed.

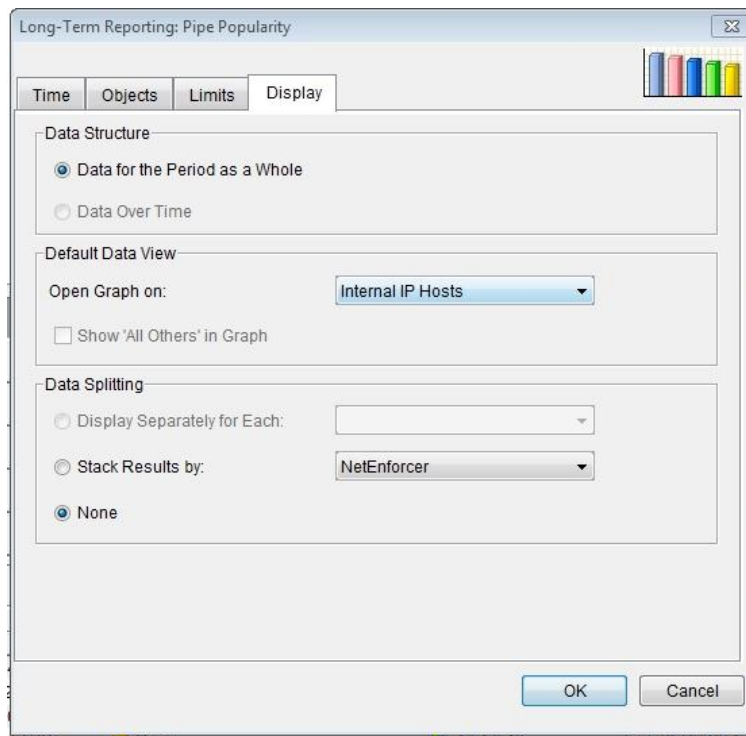


Figure 7-33: Long-Term Reporting: Pipe Popularity dialog, Display tab

11. In the Data Structure area, there are two available options:
 - **Data for the Period as a Whole:** This radio button will generate a pie chart which shows the proportionate distribution of traffic over different objects, where 100% represents all of the objects chosen. When you have specified most active objects in the Objects tab, this radio button will generate a bar chart for the whole period selected.
 - **Data Over Time:** This radio button will generate a graph presents the distribution of traffic over a set period of time. When you have specified most active objects in the Objects tab, this radio button will present the distribution over time of as calculated in the specified time period.
12. From the **Open Data On** dropdown list, select the parameter you wish to see Statistics about. In Pipe Popularity and Virtual Channel Popularity reports only Internal IP Hosts is available, and in Average Protocol Popularity reports only Internal Subscribers is available.
13. In the **Data Splitting** area, you can opt to see the stats for specific network entities separately.
14. Click **OK** to generate the graph.

Asymmetry Traffic Report

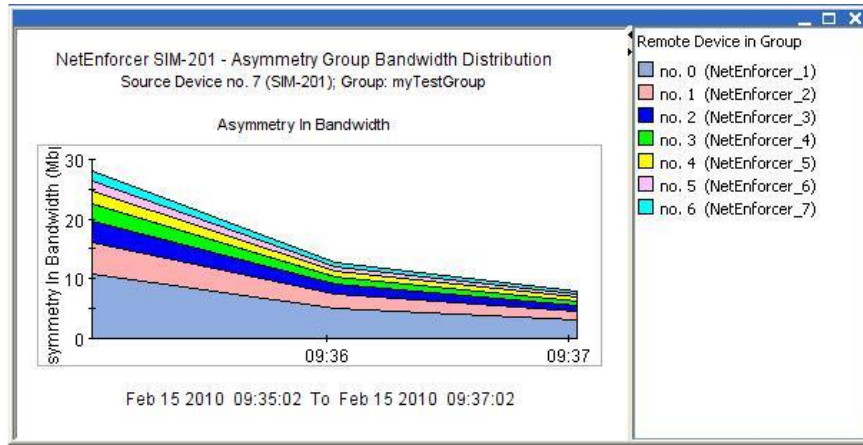


Figure 7-34: Asymmetry Traffic Graph

This report, which is only available for AOS devices, shows the traffic being used by each device in an Asymmetry Device Group (ADG). This report is available on the device level (as long as a device has Asymmetry enabled) as a Long-Term or Real Time Distribution graph, showing Asymmetry In Bandwidth, Asymmetry Out Bandwidth and Number of Asymmetry Sessions.

To generate an Asymmetry Traffic Report

1. In the Navigation pane, right-click a level in the Navigation tree for which you want to generate a graph and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select an entity in the Navigation tree for which you want to generate a graph and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select Asymmetry Traffic from the submenu.

The Real-Time Monitoring or Long Term Reporting dialog is displayed. The Stacked Bar Report icon is displayed in the upper right hand corner of the dialog box.

You may configure the parameters of your report using the two tabs of the dialog box; Time and Display. Once minimum parameters have been defined, a report may be generated at any time by clicking the OK button

The Time tab is open by default.

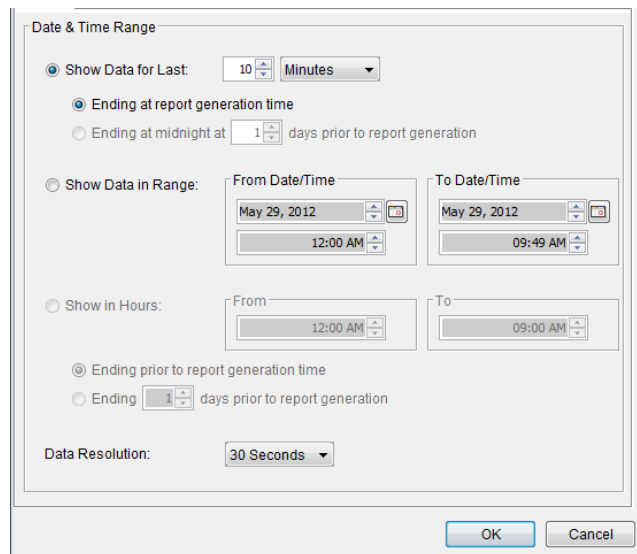


Figure 7-35: Real-Time Reporting: Asymmetry Traffic dialog box, Time tab

3. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

4. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
5. Click the **Display** tab. The following dialog is displayed.

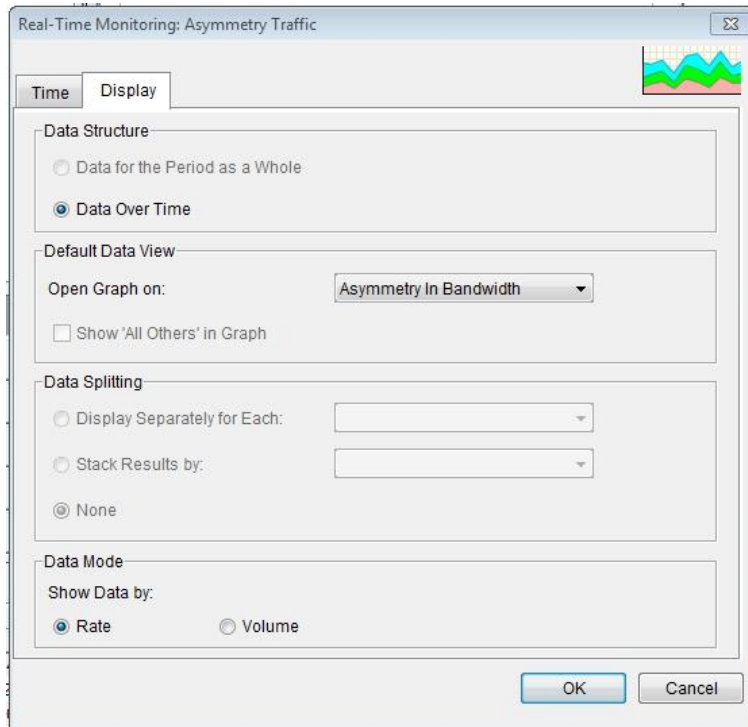


Figure 7-36: Real-Time Reporting: Asymmetry Traffic dialog, Display tab

6. In the Data Structure area, only one option is available:
 - **Data Over Time:** This radio button will generate a graph presents the distribution of traffic over a set period of time.
7. From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Asymmetry In Bandwidth, Asymmetry Out Bandwidth, Asymmetry Sessions).
8. In the **Data Splitting** area only one option, None, is available and it is selected by default.
9. In the **Data Mode** area, you can opt to display data by Rate or Volume.
10. Click **OK** to generate the graph.

Services Reports

A series of service reports are available on AOS devices only. The different reports are detailed below.

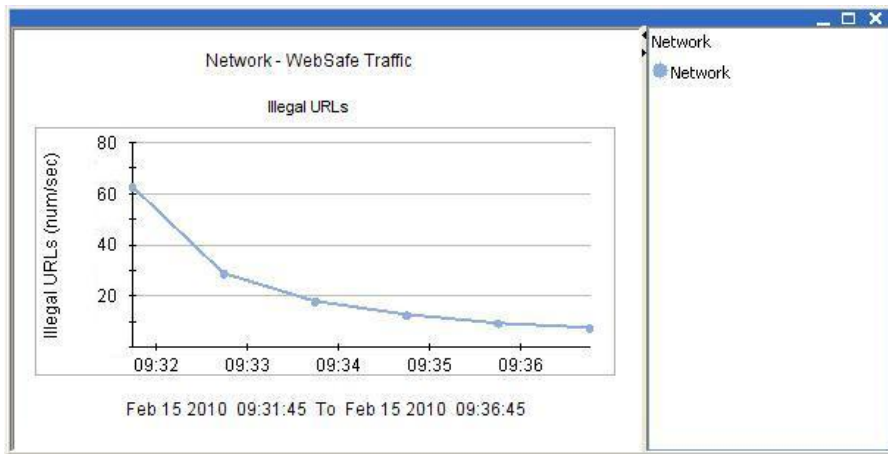


Figure 7-37: WebSafe Traffic

- WebSafe Traffic:** This report shows the HTTP traffic being checked and filtered by WebSafe (if WebSafe is enabled). This report is available on a device or network level as a Long –Term or Real Time Report, showing Inspected Requests and Illegal URLs per second.

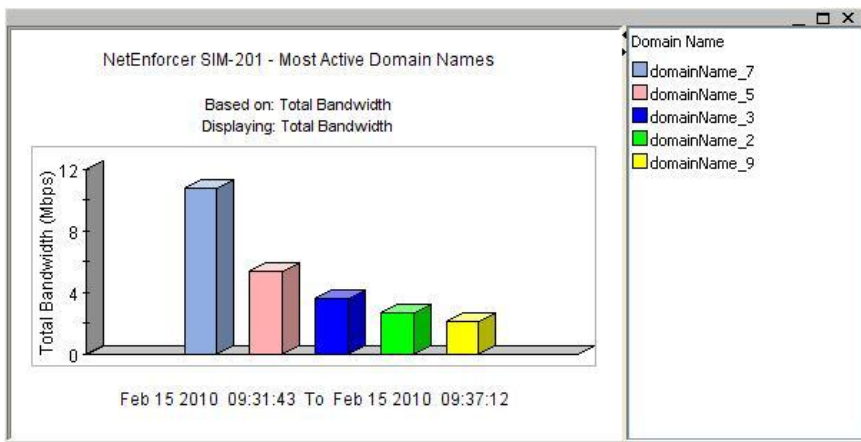


Figure 7-38: HTTP

- HTTP:** This report shows the most active domain names for the Enforcement Policy entities on which HTTP Monitoring is selected as an action (when working in “Enforcement Policy based mode” when it is assigned to each NetEnforcer or Service Gateway individually via the Enforcement Policy Editor) or for all Enforcement Policy entities (when working in “always enabled” mode, when it assigned to all NetEnforcers or Service Gateways automatically).

The default HTTP Monitoring behavior may be set to Always Enabled, Always Disabled or

Enforcement Policy Based from the Integrated Service tab in the Network Configuration window. See page 3-37 for details.

The report is available on a device level (as long as URL Monitoring is enabled) as a Long-Term or Real Time “Most Active” graph, showing In Bandwidth, Out Bandwidth, Total Bandwidth, Live Connections, New Connections, Number of Hits, Packets In, Packets Out and Number of Subscribers.

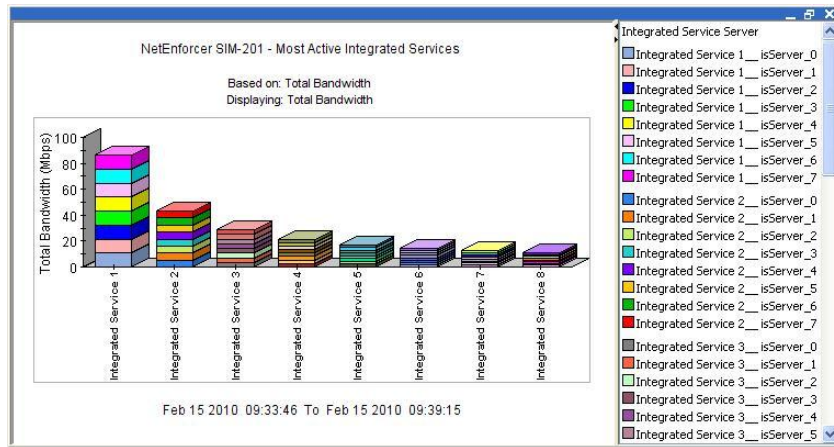


Figure 7-39: Integrated Services

- Integrated Services:** This report shows the traffic which is steered to the various Integrated Services deployed. The report is available on a device level (as long as Integrated Services are enabled) as a Long-Term or Real Time graph. Most Active Integrated Services, Most Active Integrated Services by Server, Integrated Services Distribution and Integrated Services Server Distribution graphs are available, showing Total Bandwidth, In Bandwidth, Out Bandwidth and Live Connections.

Percentile Reports

Percentile reports break down traffic use as a percentage of the whole.

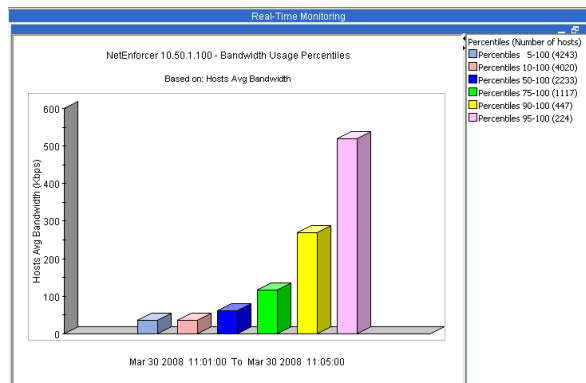


Figure 7-40: Bandwidth Usage Percentiles

- Bandwidth Usage Percentiles:** This report shows the average usage for different subscriber groups according to the percentile of the used bandwidth. Based on the samples measured for each subscriber, the report will show the average bandwidth per different subscriber groups that contain 5%, 10%, 25%, 50%, 90% and 95% of the most active subscribers. This report is available based on either subscribers or IPs.

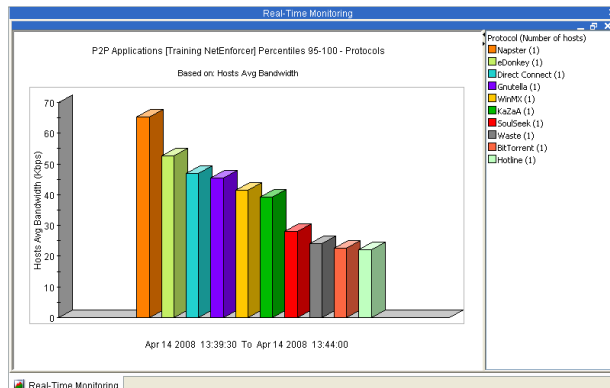


Figure 7-41: Percentile Protocols

- Protocols Percentile Distribution:** This report allows viewing protocol distribution of the average bandwidth per specific subscribers/hosts group as described in the “**Bandwidth Usage Percentiles**” report. This report is available based on either subscribers or IPs.

The report can be opened from the right click menu on the Network Tree or as a drill down into one of the bars from the “**Bandwidth Usage Percentiles**” report.

- 95th Percentile Report:** The 95th value (metered bandwidth) is used for billing by most Tier-1 operators and carriers. The 95th percentile value is calculated based on 5 minutes samples over 1 day for real-time graphs, and on 1 hour samples over 1 month for long-term graphs. This report can be generated on the Line, Pipe, or VC level.

VoIP Reports

VoIP reports provide tools for identifying trends and tracking usage volume of OTT VoIP applications. VoIP reports can be generated on the Network level only as Real Time Monitoring graphs or Long-Term Reporting reports.

NOTE This report must be enabled from the **Service Activation** tab of the **NetEnforcer Configuration** screen.

To generate a VoIP Minutes of Use Report

1. In the Navigation pane, right-click the Network in the Navigation tree and select **Real-Time Monitoring** or **Long Term Reporting**.

OR

Select the Network in the Navigation tree and then select **Real-Time Monitoring** or **Long Term Reporting** from the View menu.

OR

Select the Network in the Navigation tree and then click the **Real-Time Monitoring** or **Long Term Reporting** button on the toolbar.

The graphs submenu is displayed.

2. Select **VoIP Minutes of Use**. The Real-Time Monitoring: VoIP Minutes of Use or Long Term Reporting: VoIP Minutes of Use Properties dialog is displayed. The Report Type icon is displayed in the upper right hand corner of the dialog box.

The Time tab is open by default.

Figure 7-42: Real-Time Monitoring: VoIP Minutes of Use dialog box, Time tab

3. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

4. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.

NOTE When generating a Long-Term Report, the available options are 1 hour, 1 day or 1 month.

5. Click the **Limits** tab. The following dialog is displayed.

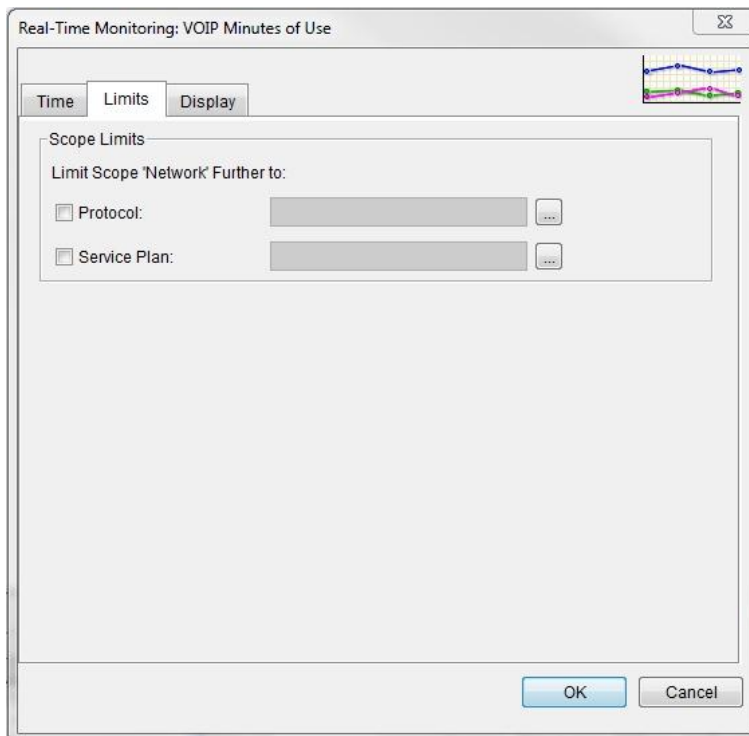


Figure 7-43: Real-Time Monitoring: VoIP Minutes of Use dialog, Limits tab

6. Use the Scope Limits parameters to refine your report to include only certain Protocols or Service Plans.

Click the appropriate check box, and click the ... button to browse the list of available objects of that type. Use the arrow keys to move objects from the **Available** list to the **Selected** list.

7. Click the **Display** tab. The following dialog is displayed.

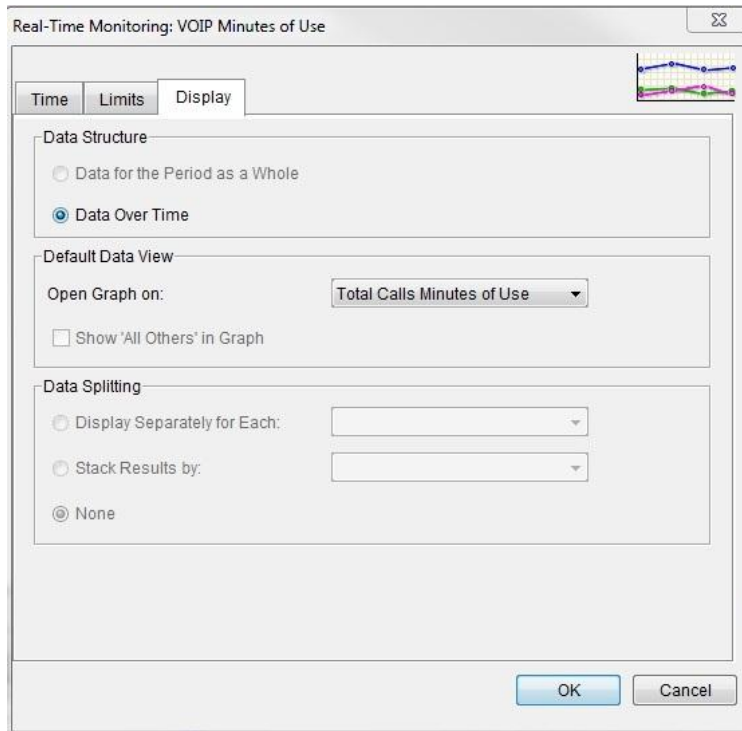


Figure 7-44: Real-Time Monitoring: VoIP Minutes of Use dialog, Display tab

8. In the **Data Structure** area, only Data Over Time is available for this report.
9. From the **Open Data On** dropdown list, only Total Calls Minutes of Use is available for this report.
10. In the **Data Splitting** area, you can opt to see the stats for specific network entities separately.
11. Click **OK** to generate the graph.

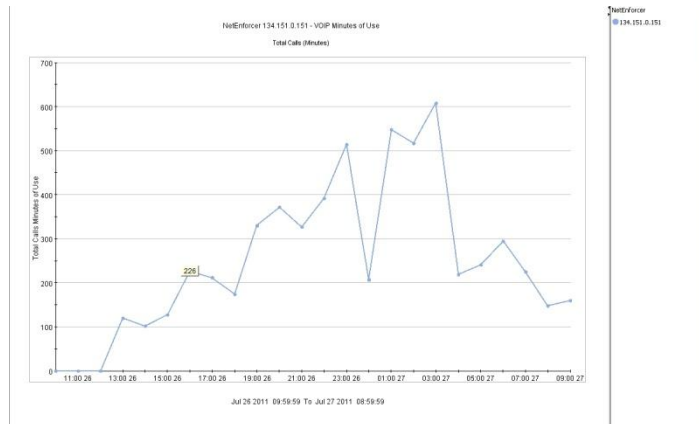


Figure 7-45: VoIP Minutes of Use Report

Subscriber Graphs

SMP Reports

SMP Reports display aspects of Subscriber behavior and are only available when an SMP unit is installed and the SMP has been enabled by entering the appropriate key in the NetXplorer.

When working with a “session management” license, the Most Active Subscribers graph is disabled. Subscriber distribution graphs are supported, with data aggregated from each session into a single subscriber element.

Subscribers Reports

These reports, which are available from both the Real-Time Monitoring and the Long Term Reporting menus, allow the monitoring of subscriber bandwidth. Depending on the “subscribers” setting in the Objects tab, the reports can be displayed in two ways:

- **Most Active Subscribers:** This report shows the most active subscribers based on total bandwidth, in/out bandwidth, new connections or in/out packets.

NOTE

The Most Active Subscribers graph cannot be created and will be unavailable from the **Objects** tab when the SMP is working in Session Management mode and when **Single IP Session per APN** or **Multiple IPs per Subscriber** has been selected in the IPs/Sessions per Subscriber Field on the Network Configuration SMP tab.

- **Subscribers Distribution:** This report shows the bandwidth distribution over time for selected subscribers.

NOTE When the SMP is performing session management (integrated with a PCRF over a Gx interface) and the system is configured for “Multiple PDP sessions are allowed; single IP session per APN” or “Multiple PDP sessions are allowed; multiple IP sessions per subscriber” modes, the “Most Active Subscriber” report is disabled. The Subscriber distribution report will work as usual.

Subscriber Usage Reports

NOTE These reports will only appear in the GUI if Quota Management is enabled in the server license.

These reports, which are only available as Long Term Reports on the network level, allow the monitoring of quota usage on a selected service plan per subscriber. Depending on the “service plan subscribers” setting in the Objects pane, the report can be displayed in two ways:

- **Most Active Subscribers for a Given Service Plan:** This report shows the most active subscribers for a given service plan based on the monthly or daily quota usage. For each subscriber, the report can be defined to display either a percentage of the available quota, or a total quota volume.
- **Subscribers Usage Distribution:** This report shows the quota usage distribution over time for selected subscribers for whatever service plan they have been assigned.

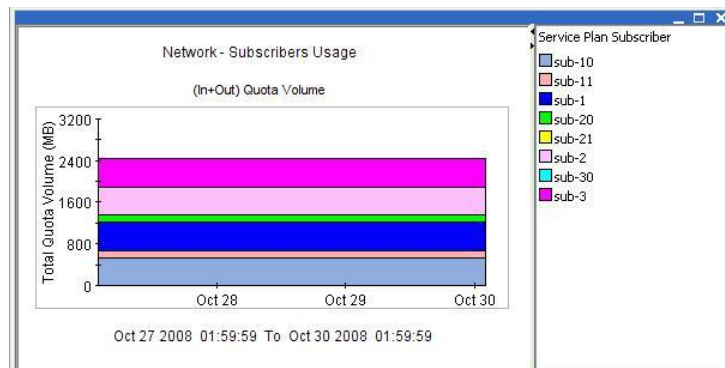


Figure 7-46: Subscribers Usage Report

Service Plans Usage Report

NOTE This report will only appear in the GUI if Quota Management is enabled in the server license.

This report, which is only available as a Long Term Report and can only be run on the network entity, allows the monitoring of the actual usage of selected quota-based service plan(s) over a selected period of time. This report may be based on volume or bandwidth usage.

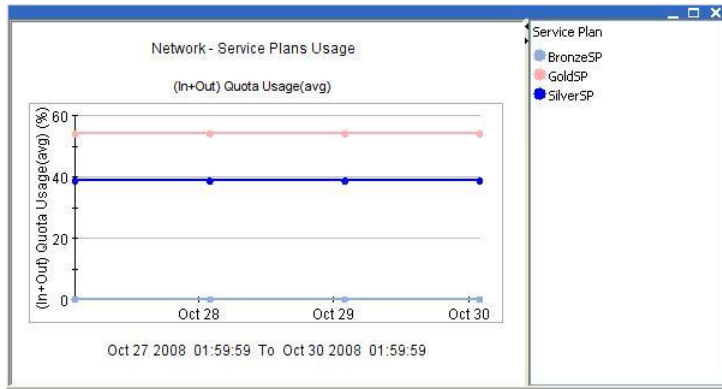


Figure 7-47: Service Plan Usage Report

Service Plans Popularity Reports

These reports, which are available as both Real-Time and Long Term Reports, can only be run on the network entity. They display the popularity of selected service plan(s) over a selected period of time. Service Plan popularity is measured by the number of active subscribers. Depending on the “service plan subscribers” setting in the Objects pane, the report can be displayed in two ways:

- **Most Popular Service Plans:** Showing the most popular service plans for the defined time period
- **Service Plans Popularity Distribution:** Showing the distribution of the selected service plan(s) over the defined time period

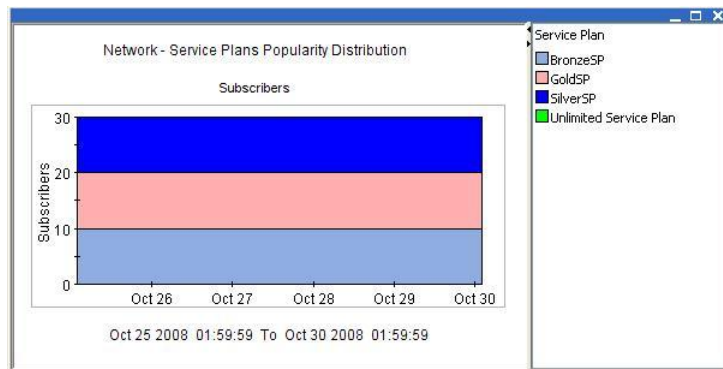


Figure 7-48: Service Plan Popularity Distribution

Quota Analysis Reports

NOTE These reports will only appear in the GUI if Quota Management is enabled in the server license.

The three quota *analysis* graphs are particularly useful where Service Plans have been defined which include multiple quota catalogs. For example, in a pipe service plan, different daily quotas may be defined for ingoing or outgoing traffic at different times of the day. These graphs enable a Service Provider to analyze and compare how different quotas have been utilized within a specified Service Plan.

- Service Plan Quota Usage Analysis:** This report, which is available as a Long Term Report and can only be run on the network entity, displays the average (daily or monthly) quota usage over all the subscribers for a selected service plan. Average quota usage is displayed as a percentage of the assigned quota for that service plan. If the selected service plan includes several different quotas, the graph will display data for each quota definition.

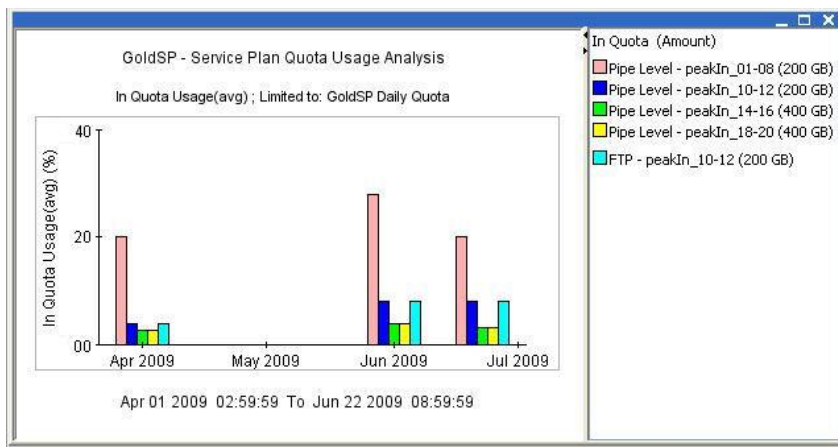


Figure 7-49: Service Plan Quota Usage Analysis

- Service Plan Quota Volume Analysis:** This report, which is available as a Long Term Report and can only be run on the network entity, displays the average (daily or monthly) quota volume over all the subscribers for a selected service plan. If the selected service plan includes several different quotas, the graph displays data for each quota definition of the selected Service Plan.

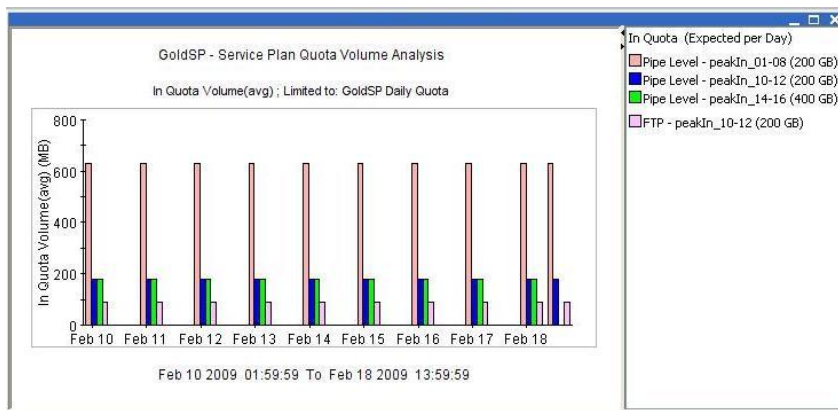


Figure 7-50: Service Plan Quota Volume Analysis

- Service Plan Quota Popularity Analysis:** This report, which is available as a Long Term Report and can only be run on the network entity, displays the number of active subscribers for a selected service plan. The data is displayed over the time period selected with a daily resolution for daily quotas and a monthly resolution for monthly quotas. If the selected service plan includes several different quotas, the graph will display data for each quota definition

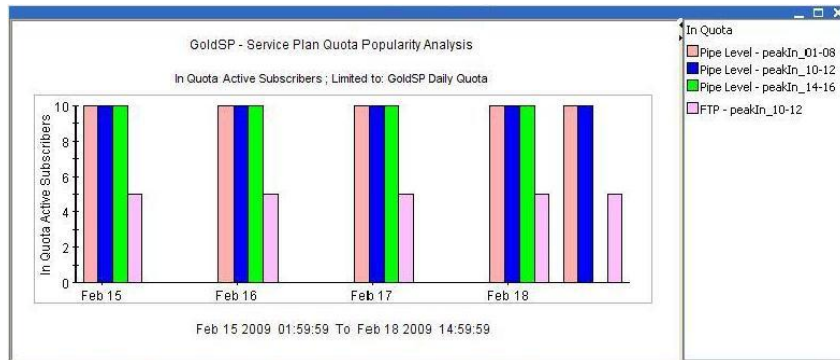


Figure 7-51: Service Plan Quota Popularity Analysis

NOTE It is possible to right click on a Quota Based SMP graph and choose to see “details” of the Service Plan. It reveals a “read-only” version of the service plan for you to remind yourself.

Cellwise Reports

CellWise reports are only available to SMP users with a Cell-Aware license.

- Cell Distribution:** This report shows the distribution of bandwidth over time across the mobile network.

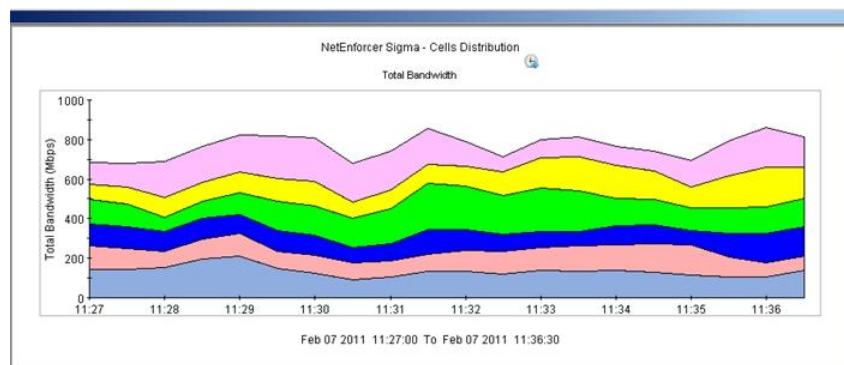


Figure 7-52: Cell Distribution Report

- Most Active Cells:** This report presents the cells carrying the most bandwidth during the selected time period.

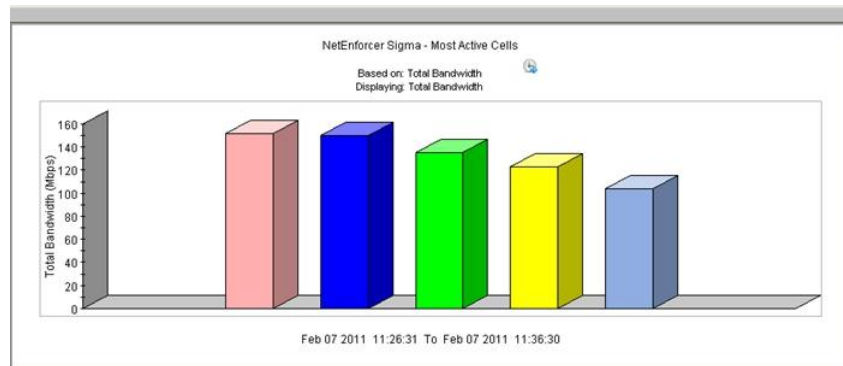


Figure 7-53: Most Active Cells Report

Mobile Analytics Reports

These 8 mobile analytics graphs process vast amounts of data in order to produce meaningful and highly accessible representations of your mobile traffic. They are designed to be configured and scheduled in advance as “User Defined Reports”. While it is possible to generate these reports manually on an ad-hoc basis from the “Mobile Analytics” menu or shortcut button, keep in mind that ad-hoc generation of each of these graphs can take a significant amount of time depending on the size of your network and the amount of mobile traffic.

When generating these graphs in the NetXplorer GUI, both as an online report, or as a scheduled report (using the “user defined reports” functionality), the total time-period covered in the report may be up to 7 days.

Mobile Analytics Reports are available on the Network level only when enabled by license.

NOTE Mobile Analytics can be produced about data dating from 36 hours or longer after SDRs first began being generated. Therefore if you enabled SDR generation at 1:00 PM on the 1st of January, only the data generated from 1:00 AM on the 3rd of January and after can be used in Mobile Analytics. All data from the previous 36 hours is permanently unavailable.

To schedule a Mobile Analytics Report:

1. Click **Actions** in the Tool bar and select New Report Entry > New Report.

OR

Select **Reports** in the Navigation Pane and right-click on User Defined Reports. Select **New Report** from the popup menu.

The Report Identity dialog of the Report Definition Wizard is displayed.

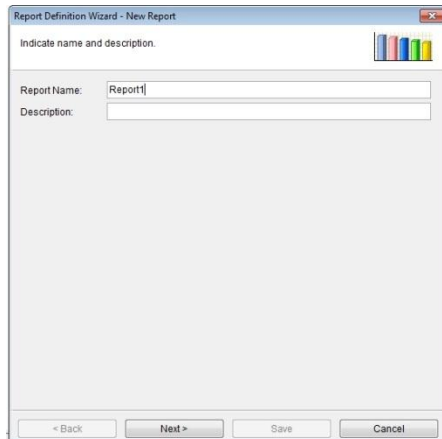


Figure 7-54: Report Identity Window

2. Enter the name of the report and a brief description of the report in the designated fields, and click **Next**.

The Report Topic dialog of the Report Definition Wizard is displayed.

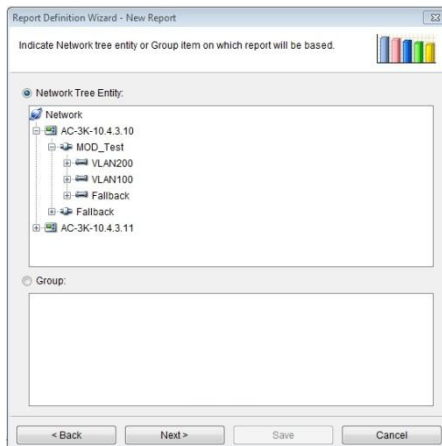


Figure 7-55: Report Topic

3. Select Network entity and click **Next**. The Report Subject dialog of the Report Definition Wizard is displayed.

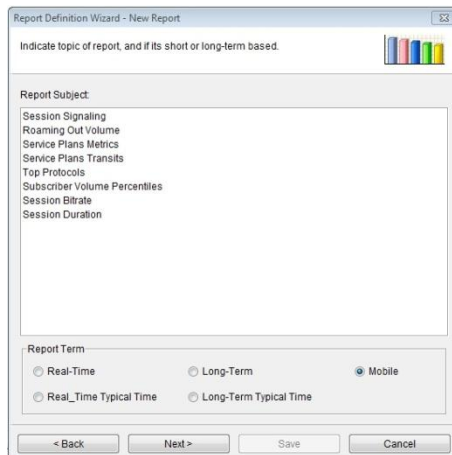


Figure 7-56: Report Subject – Mobile Analytics

4. In the Report Term area, select **Mobile**.
5. In the Report Subject area, select the topic of the report.
6. Click **Next**. The first configuration tab of the Report Definition Wizard relevant for your selected Mobile Analytics Report is displayed.
7. Click **Next** to continue to each configuration dialog until you reach the Schedule dialog.

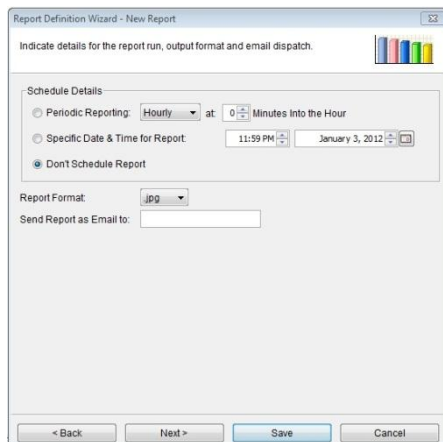


Figure 7-57: Report Schedule

8. In the Schedule Details area you may opt to select a time for this report to be consistently generated on an hourly, daily, weekly or monthly basis, a specific date and time for this report to be generated, or to leave the report unscheduled at this time.
9. A Report Format (JPG, PNG, CSV, XML, HTML or PDF) must be selected from the drop down menu and an email for the report to be sent to must be entered.

NOTE **An email can only be sent if an SMTP server is properly configured.**

10. Click **Next**. The Report Definition Summary dialog of the Report Definition Wizard is displayed.
11. Click **Save**. The scheduling information is saved and the new report definition is added to the list of available customized reports.

To generate a Mobile Analytics Report manually:

1. In the Navigation pane, right-click the Network and select **Mobile Analytics**.

OR

Select the Network in the Navigation tree and then select **Mobile Analytics** from the View menu.

OR

Select the Network in the Navigation tree and then click the **Mobile Analytics** button on the toolbar.

The graphs submenu is displayed.

2. Select the Mobile Analytics report you wish to generate from the submenu.

The Mobile Analytics dialog is displayed.

3. Use the on screen tabs to change configuration dialogs.

4. Click **OK** to generate the report.

Mobile Analytics Report Definition

Session Signaling

This report shows the average number of signaling events per active subscriber. A Signaling Events refers to either a session start or session stop (RADIUS) message. The report shows the amount of signaling events over time.

The Session Signaling Report may be viewed as a Bar Graph or as a Table.

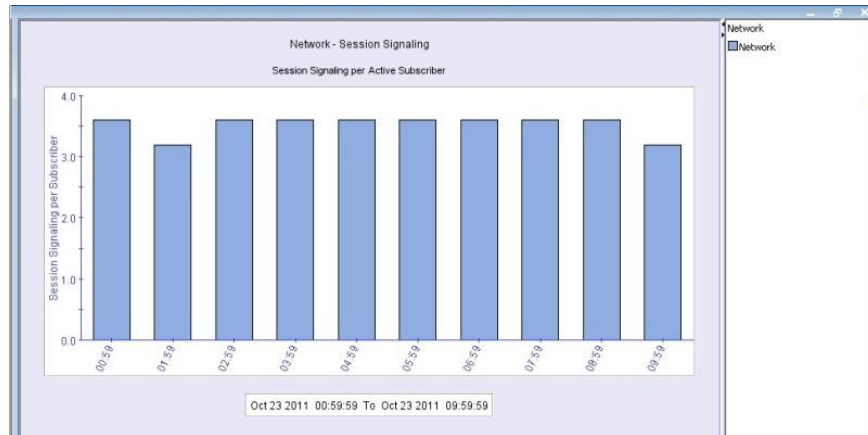


Figure 7-58: Session Signaling Report – Bar Graph

Table Time	Device Model Category	Session Signaling per Active Subscriber	Number of Session Signaling Events	Number of Active Subscribers
Oct 17 2011 04:59:59	BrickPhone Category	1.5	300	200
Oct 17 2011 05:59:59	Regular Phone Category	1.5	600	400
Oct 17 2011 06:59:59	SmartPhone Category	1.5	900	600
Oct 17 2011 07:59:59				
Oct 17 2011 08:59:59				
Oct 17 2011 09:59:59				
Oct 17 2011 10:59:59				
Oct 17 2011 11:59:59				
Oct 17 2011 12:59:59				
Oct 17 2011 13:59:59				

Figure 7-59: Session Signaling Report – Table

To configure a Session Signaling Report:

You may configure the parameters of your report using the two tabs of the dialog box; Time and Display.

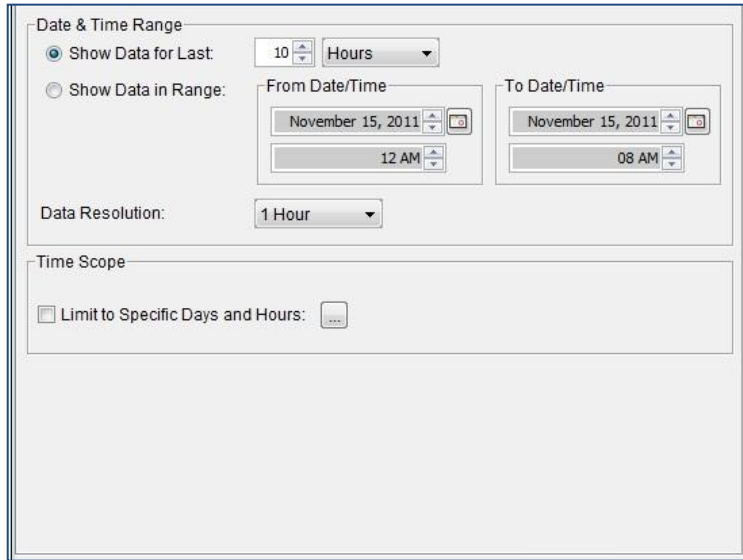


Figure 7-60: Mobile Analytics: Session Signaling, Time dialog

1. In the **Time** dialog, the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown.
- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

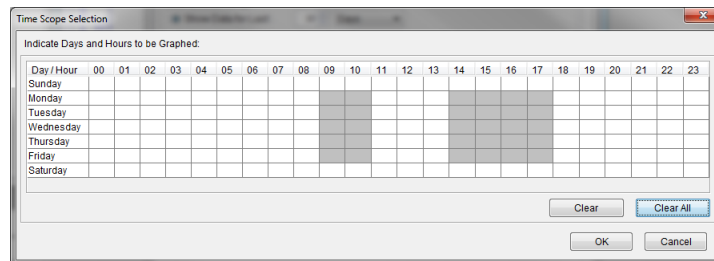


Figure 7-61: Mobile Analytics: Time Scope Selection dialog box

2. In the **Display** dialog the following fields are displayed:

The screenshot shows a dialog box with three main sections:

- Data Structure:** Contains two radio buttons. 'Data for the Period as a Whole' is unselected, and 'Data Over Time' is selected.
- Default Data View:** Contains a label 'Open Graph on:' followed by a dropdown menu showing 'Session Signaling per Subscriber'. Below it is a checkbox labeled 'Show 'All Others' in Graph' which is unchecked.
- Data Splitting:** Contains three radio buttons. 'Display Separately for Each:' is unselected and followed by an empty dropdown. 'Stack Results by:' is unselected and followed by a dropdown menu showing 'Device Model Category'. 'None' is selected.

Figure 7-62: Mobile Analytics: Session Signaling, Display dialog

- In the Data Structure area, only one option, Data Over Time, is available.
- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Number of Active Subscribers, Number of Signaling Events or Session Signaling per Subscriber).
- In the **Data Splitting** area you may select None or to stack results by Device Model Category. None is selected by default.

NOTE The available **Device Model Categories** are defined in the TAC file.

Roaming Out Volume

This report shows the volume consumed by roaming out subscribers vs. the volume consumed by local subscribers.

- **Roaming Out** refers to those subscribers who have connected remotely through another operator network, therefore incurring Roaming charges.
- **Local** refers to those subscribers that connect directly through the operator's local network.

NOTE In order to enable the system to distinguish between “local” and “roaming” sessions, the NetXplorer Administrator must first configure the list of SGSNs within the network. This is detailed in the SMP Installation and Administration Guide.

The Session Signaling Report may be viewed as a Pie Graph or as a Table.

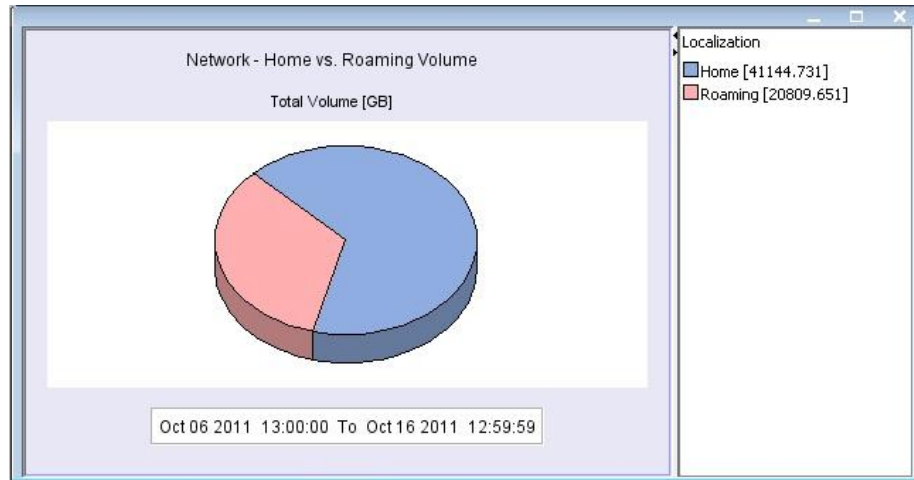


Figure 7-63: Roaming Out Volume Report – Pie Graph

Network - Home vs. Roaming Volume

Localization	Total Volume (GB)	In Volume (GB)	Out Volume (GB)	% Total Volume (%)	% In Volume (%)	% Out Volume (%)
Home	41144.731	0.0	41144.731	66.4	0.0	66.4
Roaming	20809.651	0.0	20809.651	33.6	0.0	33.6

Oct 06 2011 13:00:00 To Oct 16 2011 12:59:59

Figure 7-64: Roaming Out Volume Report – Table

To configure a Roaming Out Volume Report:

You may configure the parameters of your report using the two tabs of the dialog box; Time and Display.

Figure 7-65: Mobile Analytics: Roaming Out Volume, Time dialog

1. In the **Time** dialog the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.
 - OR
 - To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.
 - Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown.
 - Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

Figure 7-66: Mobile Analytics: Time Scope Selection dialog box

2. In the **Display** dialog the following fields are displayed:

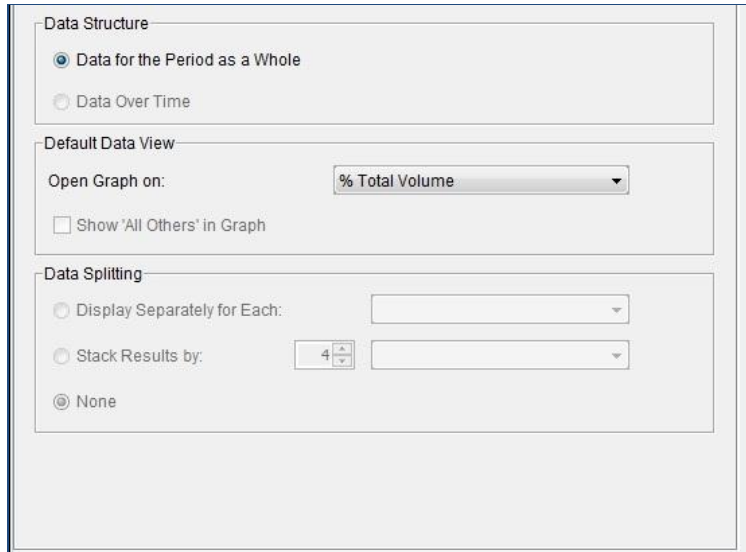


Figure 7-67: Mobile Analytics: Roaming Out Volume, Display dialog

- In the Data Structure area, only one option, **Data for the Period as a Whole**, is available:
- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Total Volume, Incoming Volume, Outgoing Volume, % Total Volume, % Incoming Volume, % Outgoing Volume).
- **Data Splitting** is unavailable and greyed out for this report.

Service Plans Metrics

This report shows the distribution over time of different metrics for service plan/s. Metrics that can be displayed are the number of active subscribers, sessions or the traffic volume.

The Service Plans Metrics Report may be viewed as a Stacked Area Graph or as a Table.



Figure 7-68: Service Plans Metrics Report – Stacked Area Graph

The figure is a table window titled "Network - Service Plans Metrics". It contains a list of time intervals on the left and a data table on the right. The data table has the following columns: Service Plan, Total Vol... (GB), In Volume (GB), Out Volu... (GB), Number of Active Su..., and Number of Sessions.

Service Plan	Total Vol... (GB)	In Volume (GB)	Out Volu... (GB)	Number of Active Su...	Number of Sessions
Default Servic...	15437.334	0.0	15437.334	1999	1999
Gold	15571.226	0.0	15571.226	1999	1999

The table also shows a time range at the bottom: "Oct 11 2011 13:00:00 To Oct 11 2011 13:59:59".

Figure 7-69: Service Plans Metrics Report – Table

To configure a Service Plan Metrics Report:

You may configure the parameters of your report using the three tabs of the dialog box; Time, Objects and Display.

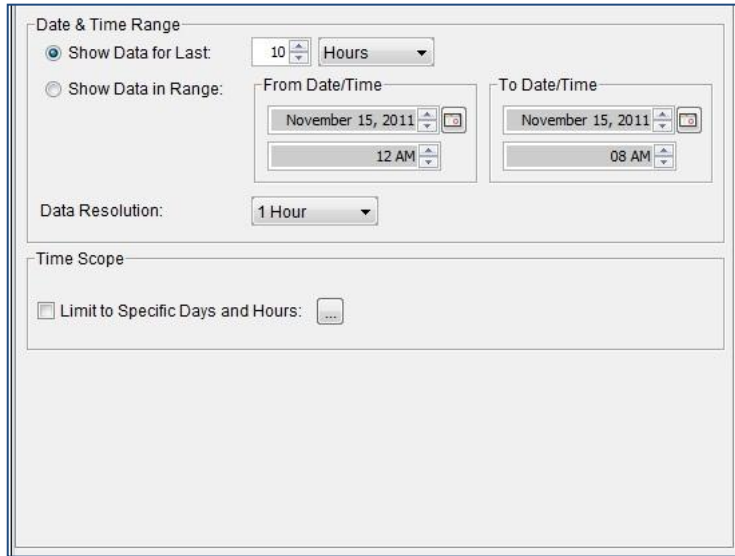


Figure 7-70: Mobile Analytics: Service Plan Metrics, Time dialog

1. In the **Time** dialog the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

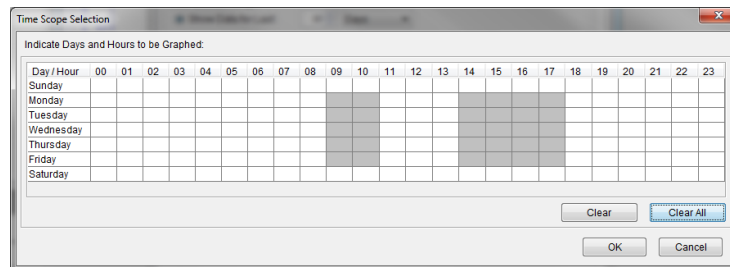


Figure 7-71: Mobile Analytics: Time Scope Selection dialog box

2. In the **Objects** dialog the following fields are displayed:

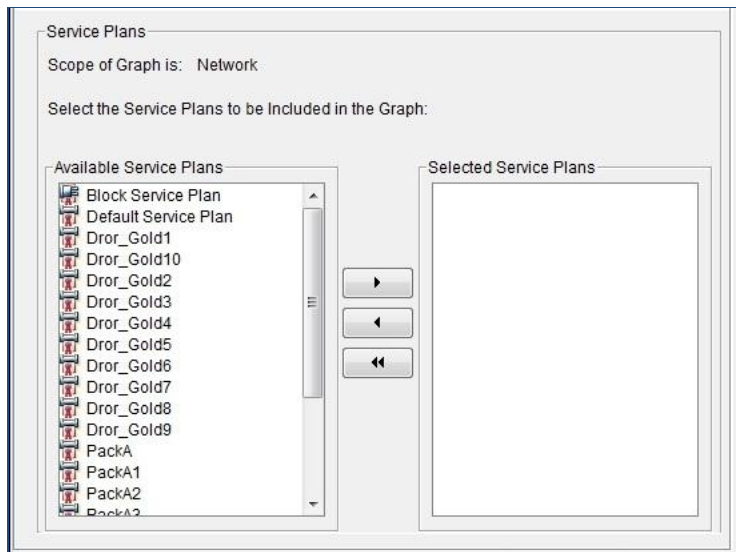


Figure 7-72: Mobile Analytics: Service Plans Metrics, Objects dialog

- Use the arrow keys to select the Service Plans to be included in the graph, moving Service Plans from the **Available** list to the **Selected** list.

3. In the **Display** dialog the following fields are displayed:

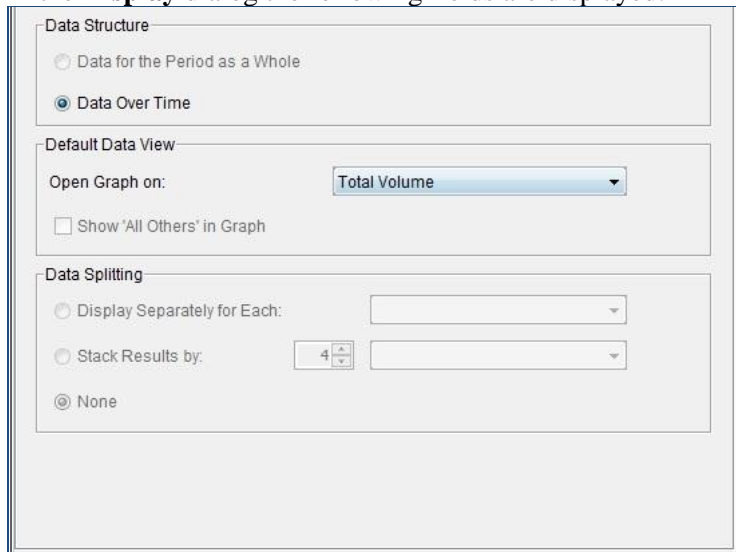


Figure 7-73: Mobile Analytics: Service Plans Metrics, Display dialog

- In the Data Structure area, only one option, Data Over Time, is available:

- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Total Volume, In Volume, Out Volume, Number of Active Subscribers, Number of Sessions).
- **Data Splitting** is unavailable and greyed out for this report.

Service Plans Transits

NOTE To generate Service Plan Transit reports the SMP must, in addition to being in PCC mode, be opposite a PCRF.

This report shows the number of transitions that occurred during the report duration, aggregated for each 'from – to' pair. For each pair of service plans, two values will be displayed: number of transitions from service plan A to B, and number of transitions from B to A.

In a standard bar graph, the X axis will list each service plan while the Y axis shows the number of transitions. The data for each service plan will be sorted by the service plan that was changed to/from.

The Service Plans Metrics Report may be viewed as a Bar Graph or as a Pie Chart.

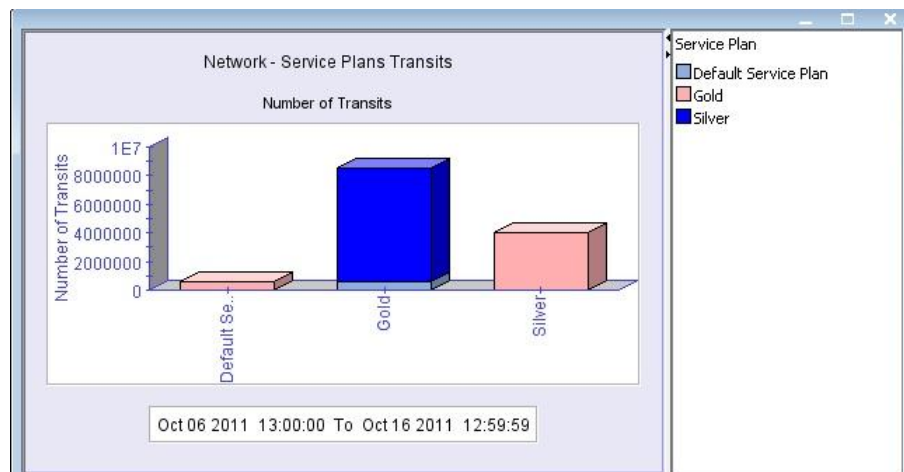


Figure 7-74: Service Plans Transits Report – Bar Graph

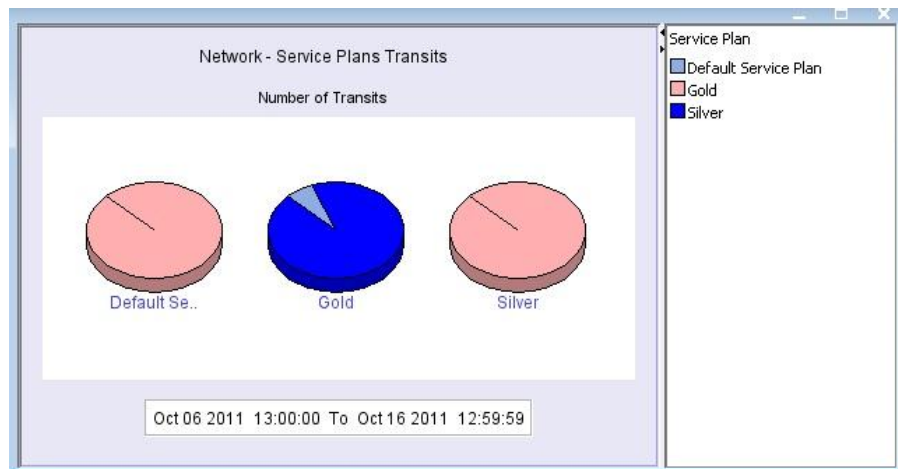


Figure 7-75: Service Plans Transits Report – Pie Chart

To configure a Service Plans Transits Report:

You may configure the parameters of your report using the three tabs of the dialog box; Time, Limits and Display.

Figure 7-76: Mobile Analytics: Service Plan Transits, Time dialog

1. In the **Time** dialog the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.
- OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

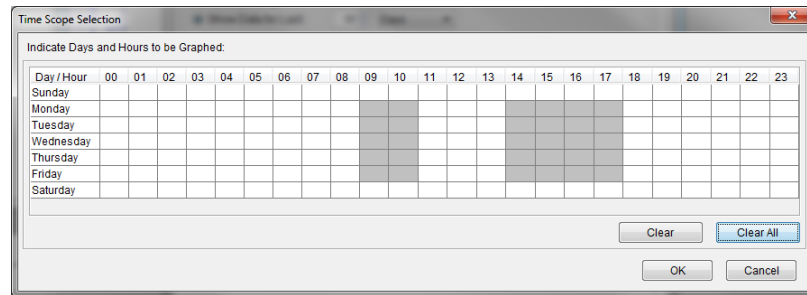


Figure 7-77: Mobile Analytics: Time Scope Selection dialog box

2. In the **Limits** dialog the following fields are displayed:

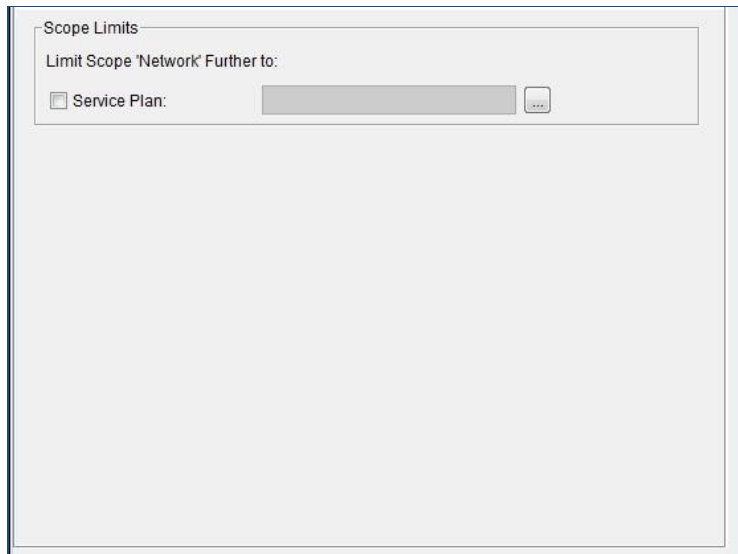


Figure 7-78: Mobile Analytics: Service Plans Transits, Limits dialog

- Select the Service Plan checkbox to limit the graph to certain Service Plans.

- Next to the Service Plan field, click the Browse button to open the Service Plans Selection dialog box. Use the arrow keys to select the Service Plans to be included in the graph, moving Service Plans from the **Available** list to the **Selected** list. Any selected Service Plans will be displayed in the Service Plans field on the Limits tab.

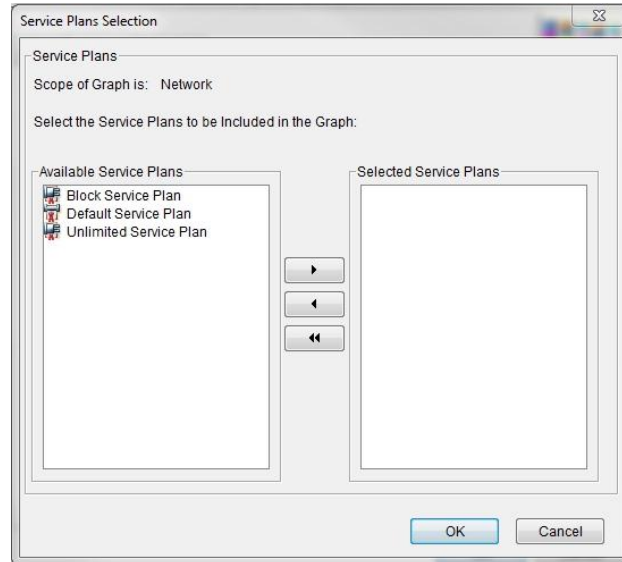


Figure 7-79: Mobile Analytics: Service Plans Selections dialog

3. In the **Display** dialog the following fields are displayed:

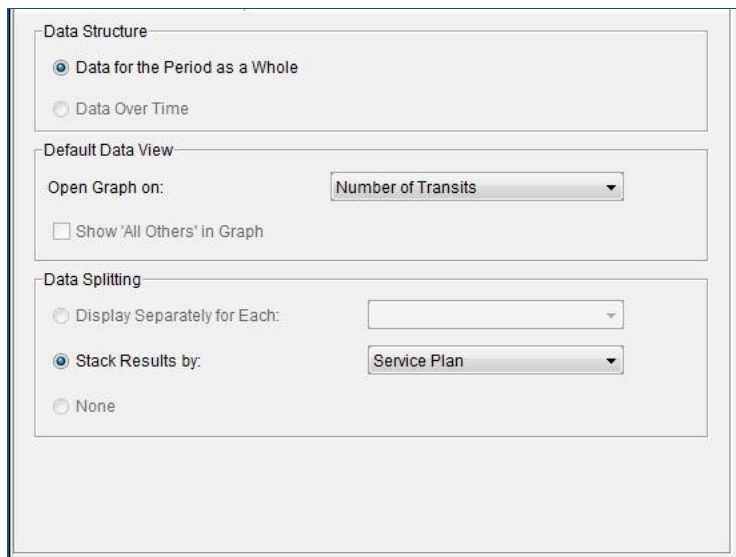


Figure 7-80: Mobile Analytics: Service Plans Transits, Display dialog

- In the Data Structure area, only one option, **Data for the Period as a Whole**, is available:

- From the **Open Graph On** dropdown list only one selection is available, **Number of Transits**.
- From the **Data Splitting** area only one selection is available, to Stack Results by Service Plan.

Top Protocols

This report shows the most active Protocols during the report time period. This data can be filtered or stacked by specific mobile device features. It is based both on SDR records and on Conversations tables.

The Top Protocols Report may be viewed as a Bar Graph or as a Table.

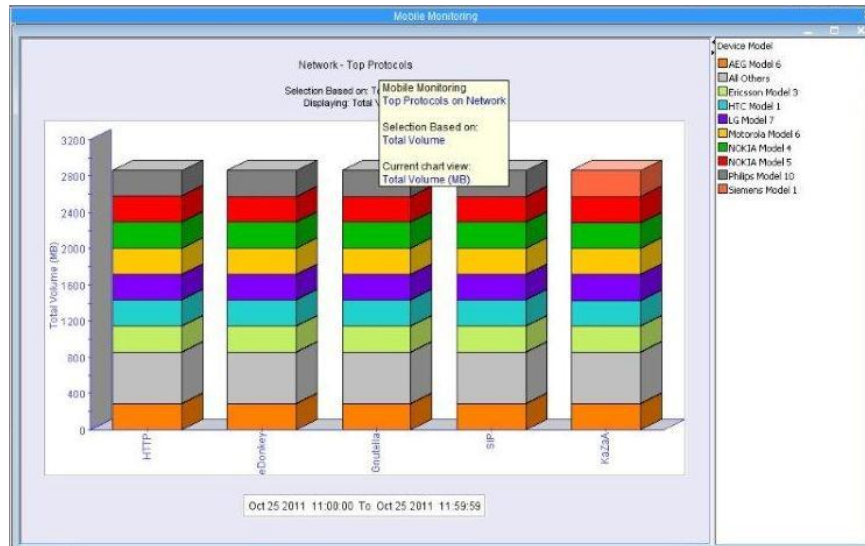


Figure 7-81: Top Protocols Report Stacked by Device – Bar Graph

The figure is a table titled "Network - Top Protocols". It is limited to "BrickPhone Categor..." and "Selection Based on: Total Volume". The table has four columns: Protocol, Device Model, Total Volume (MB), In Volume (MB), and Out Volume (MB). The protocols listed are Other TCP, Skype, BitTorrent, and ECHO. The data rows are as follows:

Protocol	Device Model	Total Volume (MB)	In Volume (MB)	Out Volume (MB)
Other TCP	All Others	968.255	968.255	0.0
Skype	ERICSSON GF 788 [Reg...	610.122	610.122	0.0
BitTorrent	MITSUBISHI MT179XFO...	475.581	475.581	0.0
ECHO	NOKIA 6190 [Regular Ph...	264.07	264.07	0.0
	SIEMENS G1050 [Regul...	343.547	343.547	0.0

The time range at the bottom is "Oct 17 2011 00:00:00 To Oct 17 2011 09:59:59".

Figure 7-82: Top Protocols Report by Device – Table

To configure a Top Protocols Report:

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display.

Figure 7-83: Mobile Analytics: Top Protocols, Time dialog

1. In the **Time** dialog the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.
 - OR
 - To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.
 - Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.

- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

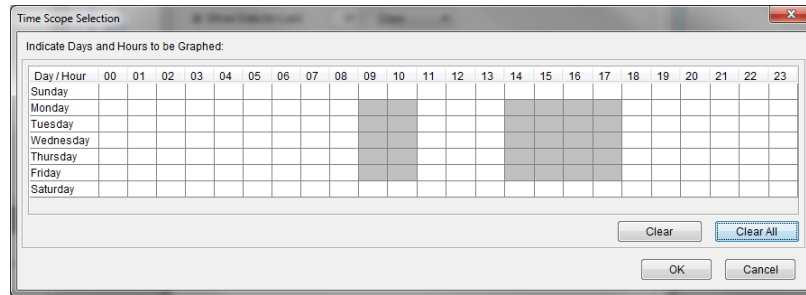


Figure 7-84: Mobile Analytics: Time Scope Selection dialog box

2. In the **Objects** dialog the following fields are displayed:

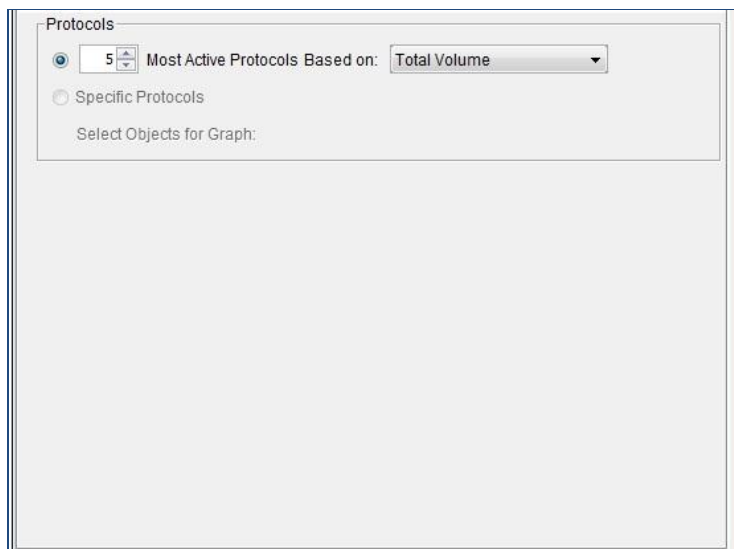


Figure 7-85: Mobile Analytics: Top Protocols, Objects dialog

- Set the number of protocols you wish listed, and set the parameter you wish the report to be based on (Total Volume, Incoming Volume or Outgoing Volume).
3. In the **Limits** dialog the following fields are displayed:

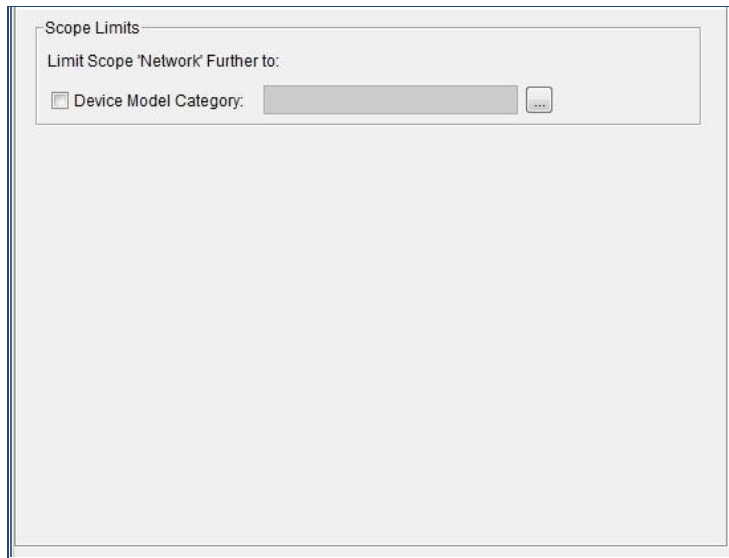


Figure 7-86: Mobile Analytics: Top Protocols, Limits dialog

- Select the Device Model Category checkbox to limit the graph to certain Device Model Categories.

NOTE

The available Device Model Categories are defined in the TAC file.

- Next to the Device Model Category field, click the Browse button to open the Service Plans Selection dialog box. Use the arrow keys to select a Device Model Category to be included in the graph and move it from the **Available** list to the **Selected** list. Any selected Categories will be displayed in the Device Model Category field in the Limits tab.

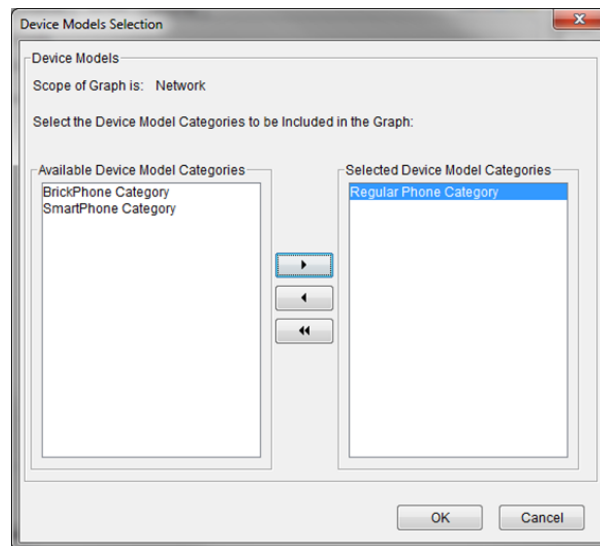


Figure 7-87: Mobile Analytics: Device Models Selections dialog

4. In the **Display** dialog the following fields are displayed:

The screenshot shows a dialog box with three main sections:

- Data Structure:** Contains two radio buttons. The first, "Data for the Period as a Whole", is selected. The second, "Data Over Time", is unselected.
- Default Data View:** Contains a label "Open Graph on:" followed by a dropdown menu showing "Total Volume". Below this is a checkbox labeled "Show 'All Others' in Graph" which is unchecked.
- Data Splitting:** Contains three radio buttons. The first, "Display Separately for Each:", is unselected and followed by an empty dropdown. The second, "Stack Results by:", is unselected and followed by a spinner box showing "4" and a dropdown menu showing "Device Model". The third, "None", is selected.

Figure 7-88: Mobile Analytics: Top Protocols, Display dialog

- In the Data Structure area, only one option, **Data for the Period as a Whole**, is available.
- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (Per Total Volume, Per Incoming Volume and Per Outgoing Volume).
- In the **Data Splitting** area you may select None or to stack results by Device Model. You can also select here how many devices to stack by. None is selected by default.

Subscriber Volume Percentiles

This report displays percentile groups of active subscribers according to the volume of traffic they use. Active subscribers are grouped into groups based on percentile, sorted from the group using the most traffic to the group using the least for the whole report period.

For each group, the report shows the total traffic volume that was consumed by that group.

The Subscriber Volume Percentiles Report may be viewed as a Bar Graph or as a Table.

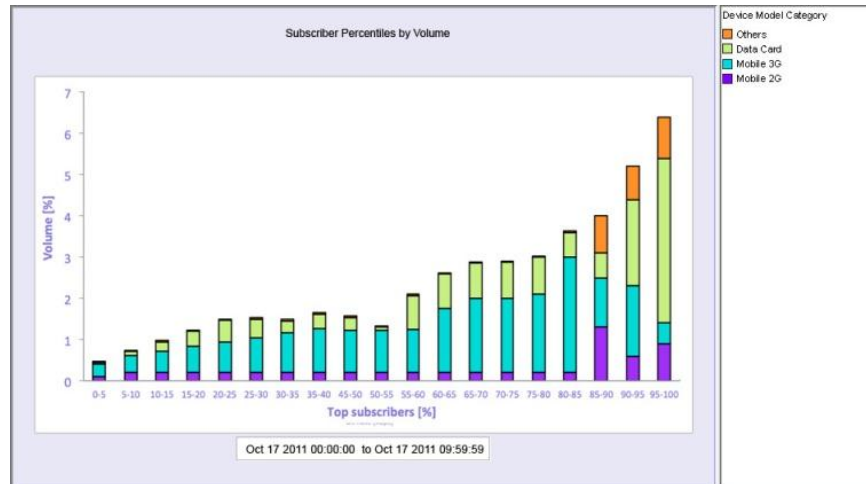


Figure 7-89: Subscriber Volume Percentiles Report Stacked by Device – Bar Graph

To configure a Subscriber Volume Percentiles Report:

You may configure the parameters of your report using the three tabs of the dialog box; Time, Objects and Display.

Figure 7-90: Mobile Analytics: Subscriber Volume Percentiles, Time dialog

- In the **Time** dialog the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

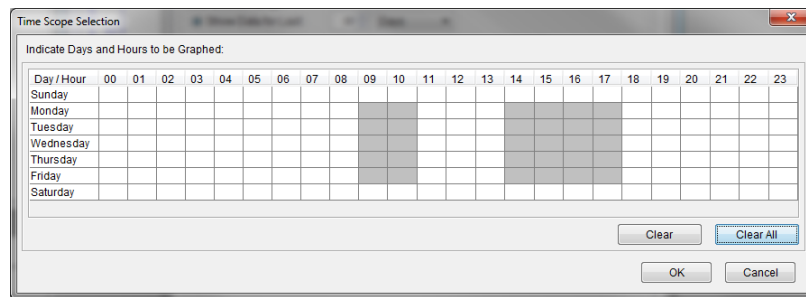


Figure 7-91: Mobile Analytics: Time Scope Selection dialog box

2. In the **Objects** dialog the following fields are displayed:

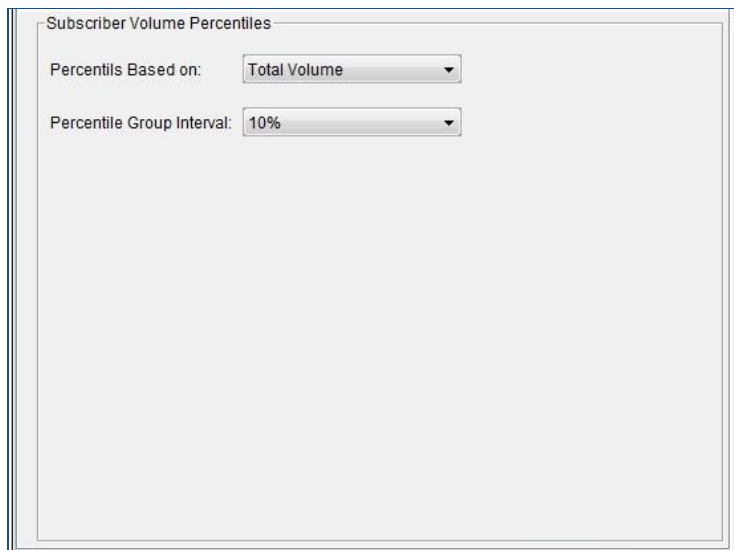


Figure 7-92: Mobile Analytics: Subscriber Volume Percentiles, Objects dialog

- In the **Percentils Based On** field, select Total Volume, In Volume or Out Volume from the drop down menu. Total Volume is selected by default.

- In the **Percentile Group Interval** field, select 5, 10 or 20 percent. 10 percent is selected by default.
3. In the **Display** dialog the following fields are displayed:

Figure 7-93: Mobile Analytics: Subscriber Volume Percentile, Display dialog

- In the Data Structure area, only one option, **Data for the Period as a Whole**, is available.
- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (% Total Volume or Total Volume).
- In the **Data Splitting** area you may select None or to stack results by Device Model Category. You can also select here how many devices to stack by. None is selected by default.

NOTE The available Device Model Categories are defined in the TAC file.

Session Bitrate

This report splits the total sessions in the report period according to bitrate ranges. The Bitrate represents the session bitrate during the time period of the report. The report displays the number or the percentage of sessions that fall into each range.

The Session Bitrate Report may be viewed as a Bar Graph or as a Table.

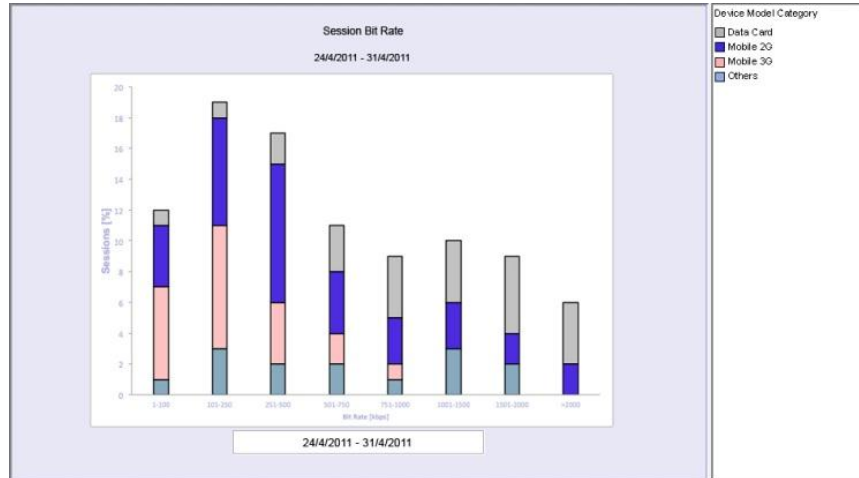


Figure 7-94: Session Bitrate Report Stacked by Device – Bar Graph

To configure a Session Bitrate Report:

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display.

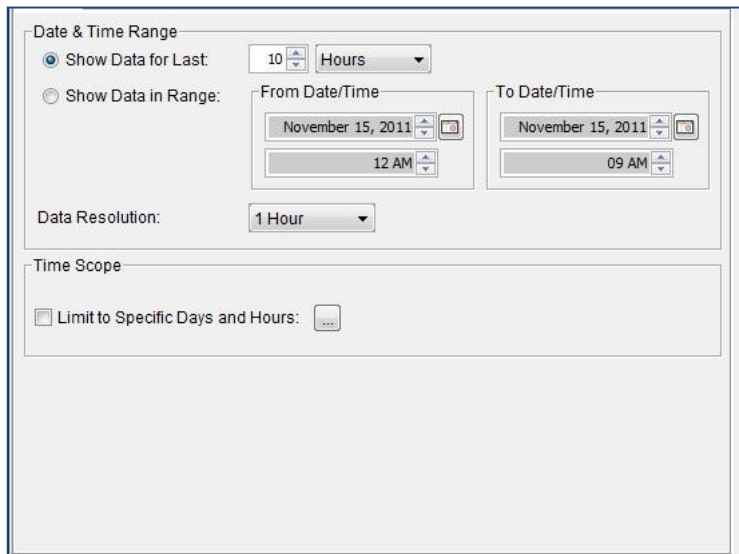


Figure 7-95: Mobile Analytics: Session Bitrate, Time dialog

- In the **Time** dialog, the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

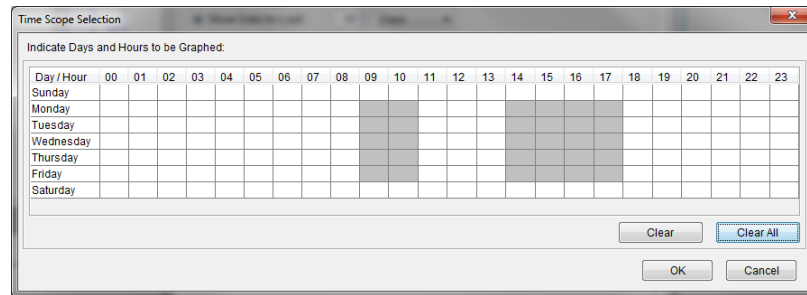


Figure 7-96: Mobile Analytics: Time Scope Selection dialog box

2. In the **Objects** dialog the following fields are displayed.

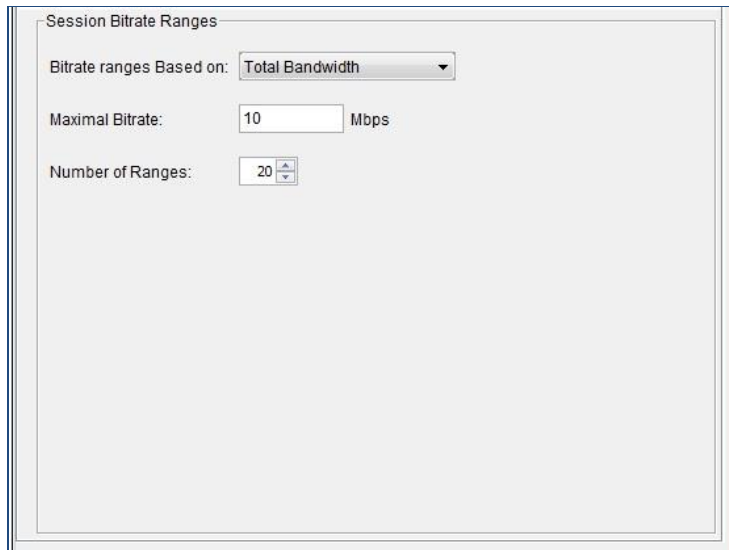


Figure 7-97: Mobile Analytics: Session Bitrate, Objects dialog

- Select if you wish the Bitrate Ranges to be based on Total Bandwidth, In Bandwidth or Out Bandwidth in the drop down menu.
- Set the Maximal Bitrate value to be displayed on the horizontal axis.

- Select the number of Ranges to be displayed in the report from the drop down menu.
3. In the **Limits** dialog the following fields are displayed:

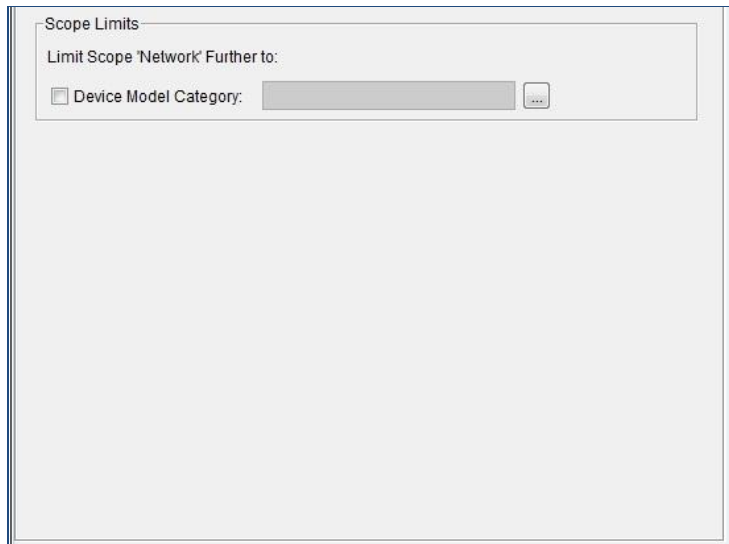


Figure 7-98: Mobile Analytics: Session Bitrate, Limits dialog

- Select the Device Model Category checkbox to limit the graph to certain Device Model Categories.

NOTE The available Device Model Categories are defined in the TAC file.

- Next to the Device Model Category field, click the Browse button to open the Service Plans Selection dialog box. Use the arrow keys to select a Device Model Category to be included in the graph and move it from the **Available** list to the **Selected** list. Any selected Categories will be displayed in the Device Model Category field in the Limits tab.

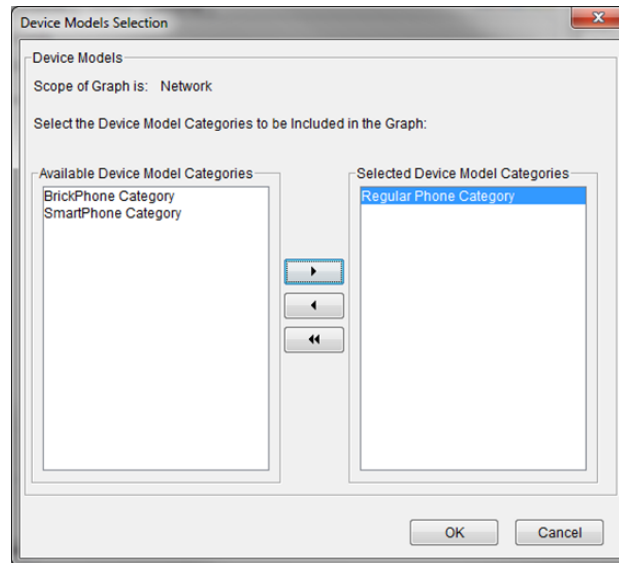


Figure 7-99: Mobile Analytics: Device Models Selections dialog

4. In the **Display** dialog, the following fields are displayed:

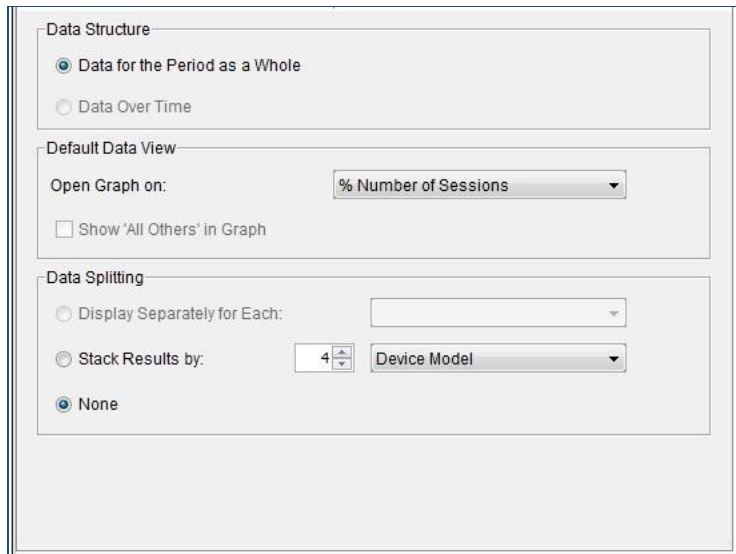


Figure 7-100: Mobile Analytics: Session Bitrate, Display tab

- In the Data Structure area, only one option, **Data for the Period as a Whole**, is available.
- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (% Number of Sessions or Number of Sessions).
- In the **Data Splitting** area you may select None or to stack results by Device Model. You can also select here how many devices to stack by. None is selected by default.

Session Duration

This report splits the total sessions into groups according to the session duration. Duration is the total session duration (start to stop). The report displays the number or percentage of sessions that fall into each Duration group.

The Session Duration Report may be viewed as a Bar Graph or as a Table.

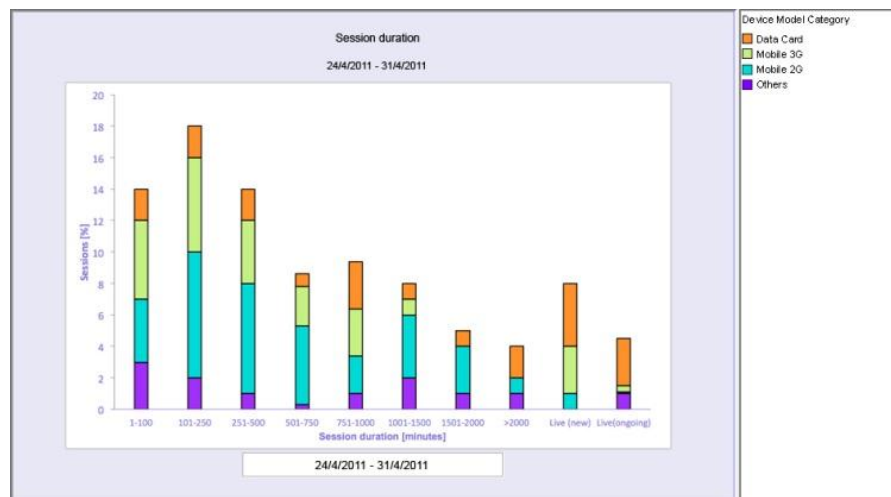


Figure 7-101: Session Bitrate Report Stacked by Device – Bar Graph

To configure a Session Duration Report:

You may configure the parameters of your report using the four tabs of the dialog box; Time, Objects, Limits and Display.

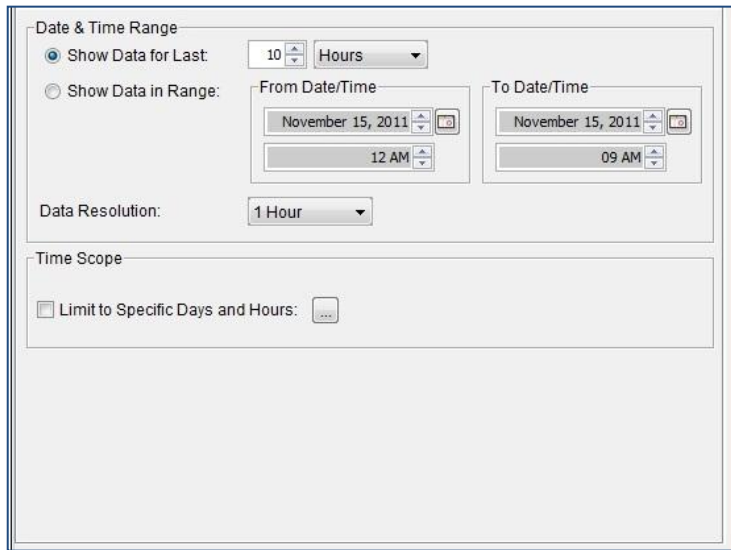


Figure 7-102: Mobile Analytics: Session Duration, Time dialog

1. In the **Time** dialog, the following fields are displayed:
 - To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time and select the unit of time (hours, days, weeks, months or years) in the designated fields.

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Then enter the relevant dates and times in the From Date Time and To Date Time areas.

- Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.
- Select the Limit to Specific Days and Hours checkbox to limit data to a certain time of day.

Clicking the Browse button opens the Time Scope Selection dialog to set the day of the week and hours for the graph to cover.

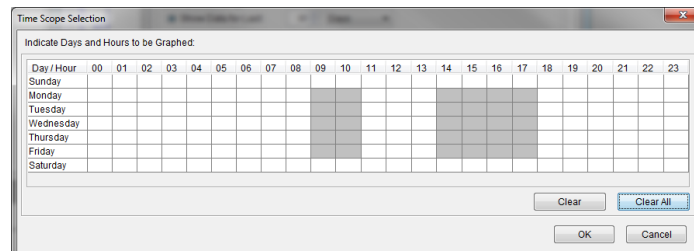


Figure 7-103: Mobile Analytics: Time Scope Selection dialog box

2. In the **Objects** dialog the following fields are displayed:

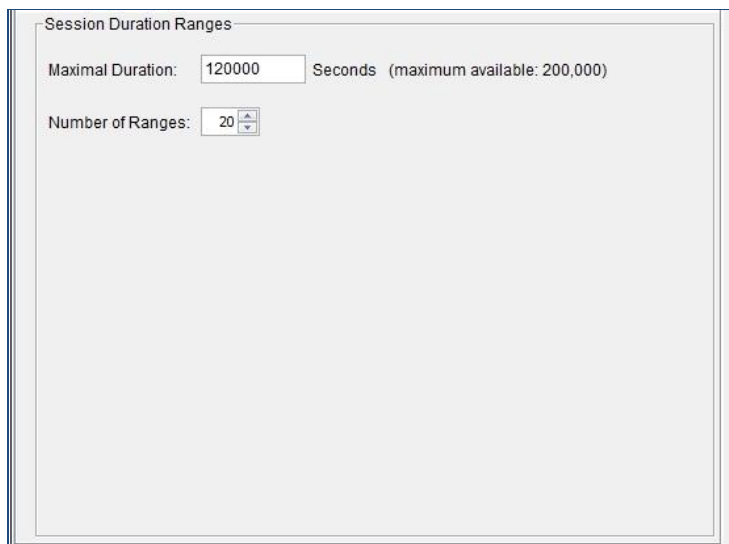


Figure 7-104: Mobile Analytics: Session Duration, Objects dialog

- Set the Maximal Duration value in seconds (200,000 seconds maximum).
- Select the number of Ranges to be displayed in the report from the drop down menu.

3. In the **Limits** dialog the following fields are displayed:

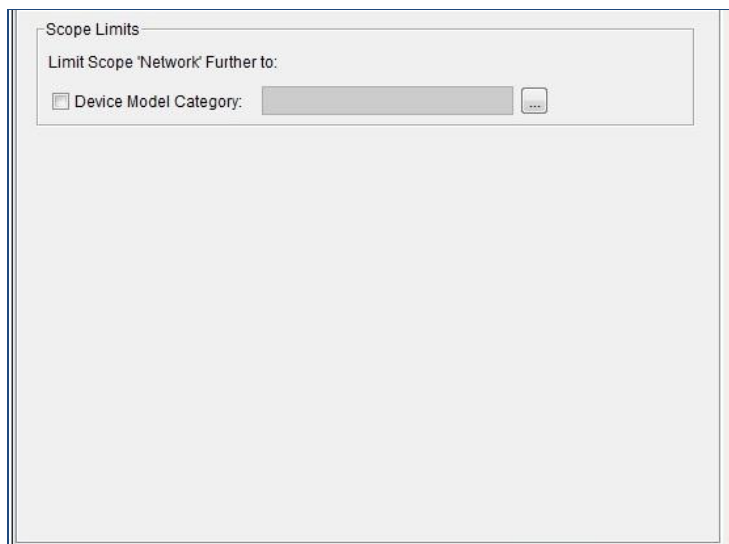


Figure 7-105: Mobile Analytics: Session Duration, Limits dialog

- Select the Device Model Category checkbox to limit the graph to certain Device Model Categories.

NOTE The available **Device Model Categories** are defined in the **TAC** file.

- Next to the Device Model Category field, click the Browse button to open the Service Plans Selection dialog box. Use the arrow keys to select a Device Model Category to be included in the graph and move it from the **Available** list to the **Selected** list. Any selected Categories will be displayed in the Device Model Category field in the Limits tab.

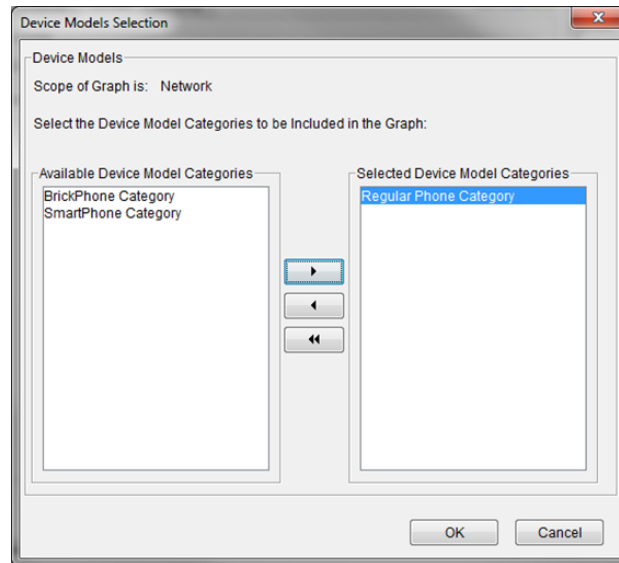


Figure 7-106: Mobile Analytics: Device Models Selections dialog

4. In the **Display** dialog the following fields are displayed:

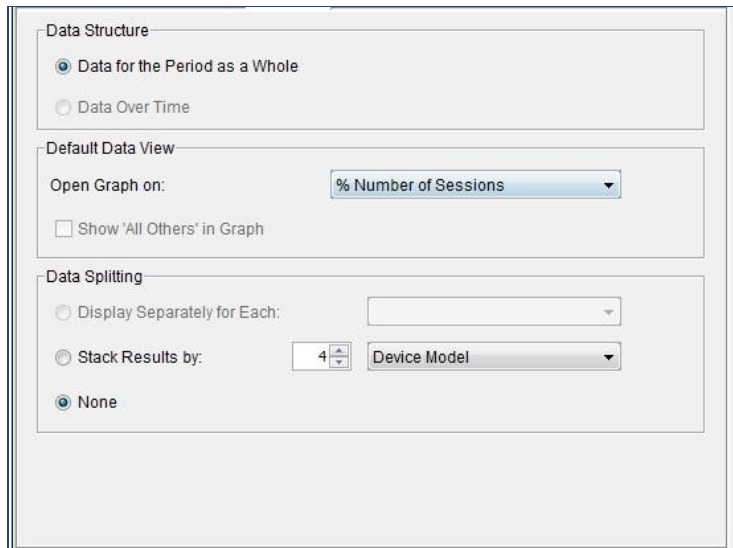


Figure 7-107: Mobile Analytics: Session Duration, Display dialog

- In the Data Structure area, only one option, **Data for the Period as a Whole**, is available.
- From the **Open Graph On** dropdown list, select the parameter you wish to see Statistics about (% Number of Sessions or Number of Sessions).
- In the **Data Splitting** area you may select None or to stack results by Device Model. You can also select here how many devices to stack by. None is selected by default.

Scheduling a Report

NetXplorer's User Defined Report Definition Wizard enables a user with Administrator privileges to create, save and distribute scheduled, customized reports that monitor performance data of particular interest to you and your Network. Scheduled reports created using the Report Definition Wizard may be prepared as email attachments and sent to a selected recipient or stored on the server rather than appearing in the GUI. In addition a report may be customized but not scheduled, so that it may be generated at any time from the Navigation pane.

All NetXplorer Real-Time Monitoring graphs may be generated and sent as reports. In addition Long-Term Reports may be generated which can encompass a much larger period of time with a less precise granularity than Real-Time Monitoring graphs. Allot recommends that due to the fact that Mobile Analytics reports can take a significant amount of time, depending on the size of your network and the amount of mobile traffic, they be scheduled using the User Defined Reports feature.

Scheduled Reports may be created by any user with Administrator access. In addition, each Administrator can see only the Scheduled Reports they have defined, and not the reports defined by any other Administrator.

Reports are managed in the NetXplorer Reports Navigation panel.

To view a list of available reports, click **Reports** in the Navigation pane. The available reports are listed in the upper portion of the Navigation pane.

To view the details of a specific report, select the report in the Navigation pane.

NOTE **It is possible to see some Reports in Real-Time by right clicking on the Report and selecting Show in Monitoring.**

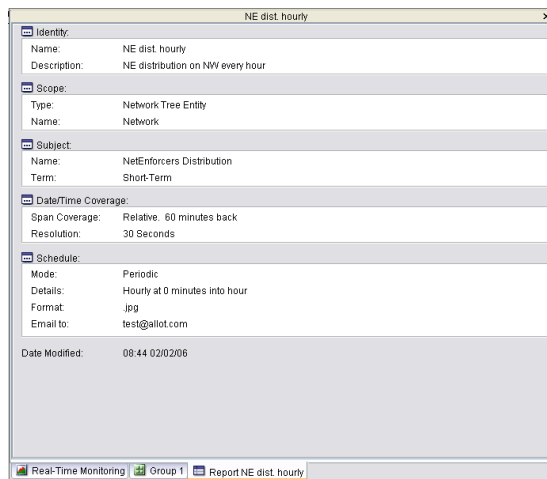


Figure 7-108: Report tab

Defining a Scheduled Report

NOTE Not all tabs and fields will appear for all reports.

To define a report:

1. Select Reports in the Navigation Pane.
2. Right-click in the Navigation Pane and select **New Report** from the popup menu. The Report Identity dialog of the Report Definition Wizard is displayed.

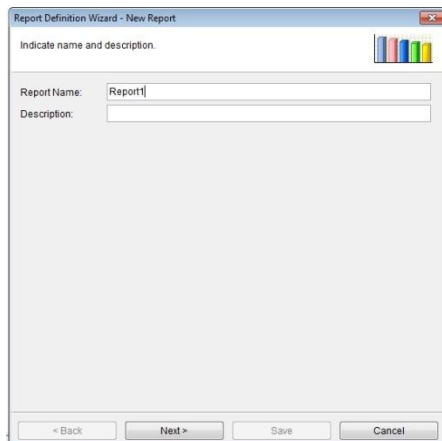


Figure 7-109: Report Identity Window

3. Enter the name of the report and a brief description of the report in the designated fields, and click **Next**.

The Report Topic dialog of the Report Definition Wizard is displayed.

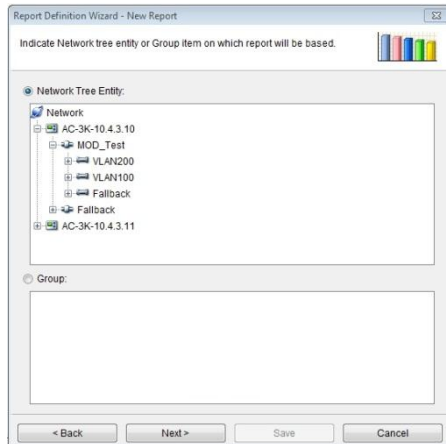


Figure 7-110: Report Topic

4. Select the Network entity or Group entity on which the report is to be based, and click **Next**. The Report Subject dialog of the Report Definition Wizard is displayed.



Figure 7-111: Report Subject

5. In the Report Subject area, select the topic of the report.
6. In the Report Term area, select the type of monitoring report to be produced: Real-Time, Real-Time Typical Time, Long-Term, Long-Term Typical Time or Mobile.
7. Click **Next**. The Report Objects dialog of the Report Definition Wizard is displayed (if applicable).

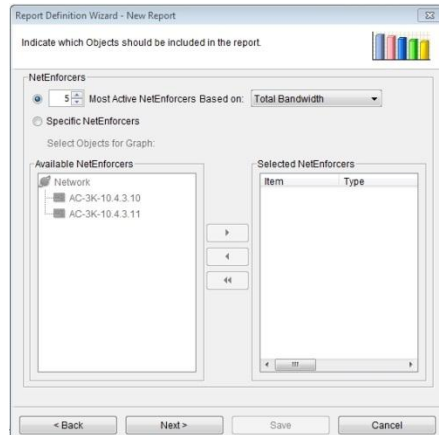


Figure 7-112: Report Objects

8. Configure the Report Objects, as follows:
 - To generate a **Most Active** report select the upper radio button, set the number of objects you wish listed, and set the parameter you wish the report to be based on.
 - Select the **Specific <OBJECT>** radio button to generate a graph showing only selected objects. Use the arrow keys to move individual Objects from the **Available** list to the **Selected** list.
9. Click **Next**. The Report Time dialog of the Report Definition Wizard is displayed.

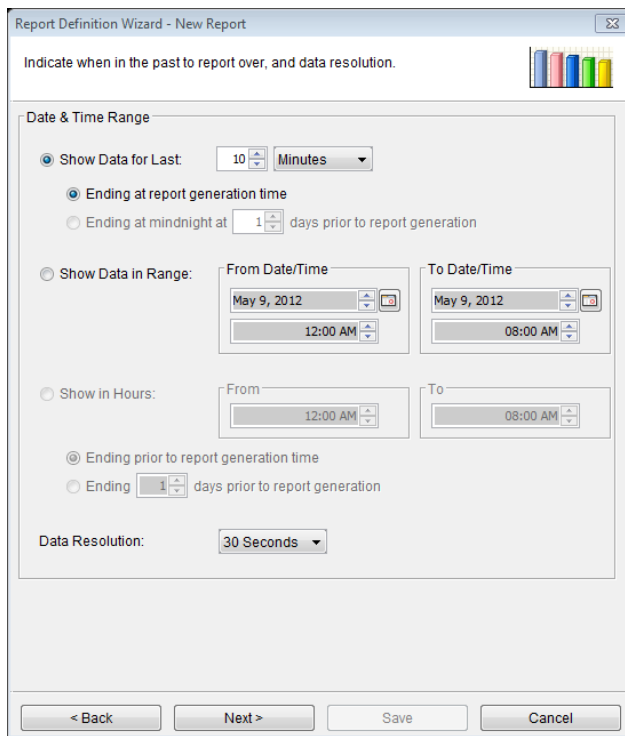


Figure 7-113: Report Time

10. To configure the graph to include the data from a specific point in time and forward, select the **Show Data for Last** radio button. Then enter the relevant quantity of time, select the unit of time (days, hours, minutes, or seconds) in the designated fields and indicate when you wish the report period to have ended (at the time the report is generated or at midnight of a specific day previously).

OR

To set a definite starting and end point for monitoring, select the **Show Data in Range** radio button. Enter the relevant dates and times in the From Date Time and to Date Time areas.

OR

To set a period of one or more hours for monitoring, select the **Show in Hours** radio button. Indicate when you wish the report period to have ended (at the time the report is generated or a certain number of days previously).

11. Select the time intervals at which data points are to be indicated in the graph from the **Data Resolution** dropdown list.

NOTE When generating a long-term monitoring report, the available options are (1 hour, 1 day, 1 month).

12. In the Data Display area select if you wish the data to be displayed by rate or by volume (if applicable).
13. Click **Next**. The Report Scope dialog of the Report Definition Wizard is displayed (if applicable).

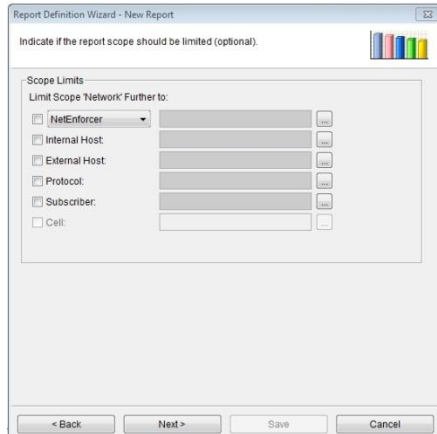


Figure 7-114: Report Scope

14. Configure the Report Scope, as follows:
 - **Scope Limits:** Select the entities that the graph will be monitoring.
15. Click **Next**. The Report Display dialog of the Report Definition Wizard is displayed.

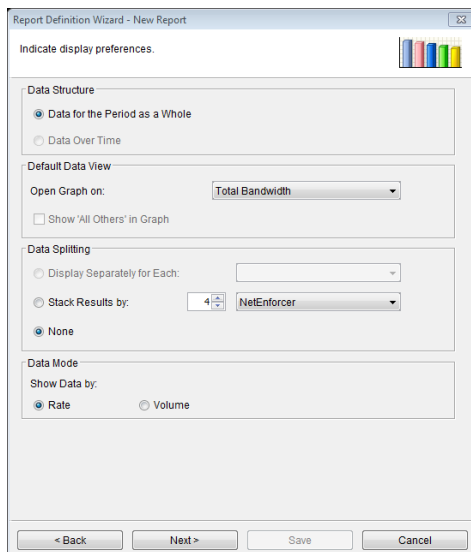


Figure 7-115: Report Display

16. Configure the Report Display, as follows:

- **Data Structure:** Select if you wish to display Data for the Period as a Whole or Data Over Time.
 - **Default Data View:** Select the data that the graph will open displaying.
 - **Data Splitting:** Select the way in which the data will be split and stacked in the graph.
 - **Data Mode:** Select if you wish data to be displayed by Rate or by Volume (if applicable)
17. Click **Next**. The Report Schedule dialog of the Report Definition Wizard is displayed.

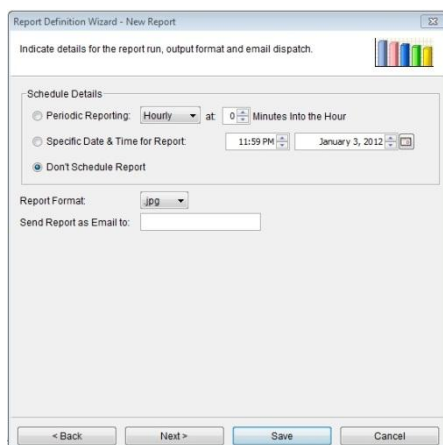


Figure 7-116: Report Schedule

18. In the Schedule Details area you may opt to select a time for this report to be consistently generated on an hourly, daily, weekly or monthly basis, a single date and time for this report to be generated, or to leave the report unscheduled.

If a report is not scheduled, it will be saved in the User Defined Reports list and may be generated manually at any time.

19. A Report Format must be selected from the drop down menu and an email for the report to be sent to must be entered.
20. Enter an email address for the Report to be sent to once generated.

NOTE An email can only be sent if an SMTP server is properly configured.

21. Click **Next**. The Report Definition Summary dialog of the Report Definition Wizard is displayed.

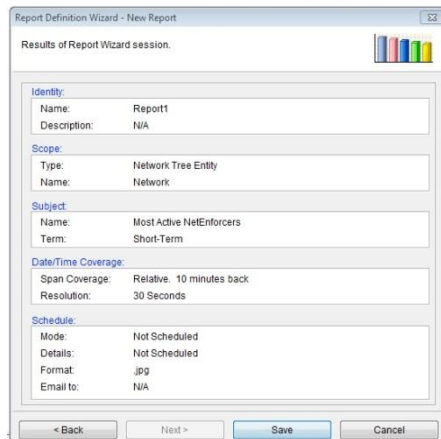


Figure 7-117: Report Definition Summary

22. Click **Save**. The new report definition is added to the list of available customized reports.

Editing a Scheduled Report Definition

1. Open Reports in the Navigation Pane.
2. Double click a Report to open the Summary dialog box.
3. Click on the Icon to the left of the area you wish to edit.
4. The appropriate dialog box opens. Make the changes you wish and click **Next** or **Save** to save the changes.

Deleting a Scheduled Report Definition

1. Open Reports in the Navigation Pane.
2. Click a Report to highlight it.
3. Click **Delete** on the Main Toolbar.

Compound Reports

Compound Reports are pre-defined combinations of User Defined reports. A Compound report offers a way to conveniently generate multiple reports together in a single PDF file, distributed via email.

To define a compound report:

1. Select Reports in the Navigation Pane.
2. Right-click on **User Defined Reports** in the Navigation Pane and select **New > Compound Report** from the popup menu.

OR

Select **New Report Entry > Compound Report** from the Actions menu.

The Compound Reports Properties dialog box is displayed.

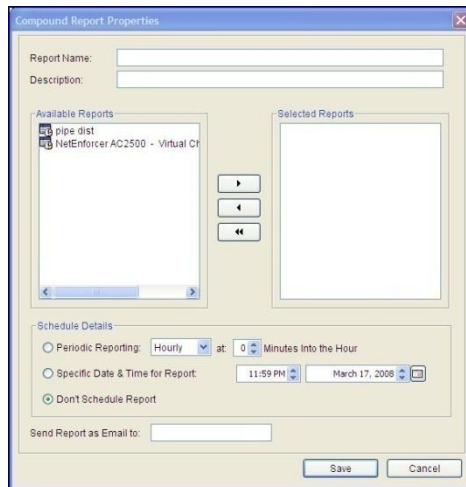


Figure 7-118: Compound Report Properties

3. Enter the name of the report and a brief description of the report in the designated fields.
4. Select those User Designed Reports from the **Available Reports** list you wish to include in the Compound Report and add them to the **Selected Reports** list using the arrow keys.

NOTE Any report added to a compound report must be configured when created to be generated as a PDF file.

5. In the Schedule Details area you may opt to select a time for this report to be consistently generated on a hourly, daily, weekly or monthly basis, a single date and time for this report to be generated, or to leave the report unscheduled.

NOTE Each simple report that was selected to the compound report, must also, by itself, be scheduled for generation. It should be understood that what the compound report does is simply to 'collect' the separately generated simple reports into one pdf. If a simple report is not scheduled, there will be nothing to include in the compound report pdf, although the report is included in the compound report definition.

6. An email for the report to be sent to must be entered.
7. Enter an email address for the Report to be sent to once generated.
8. Click **Save**. The new Compound Report is added to the list of available customized reports shown in the Reports Navigation pane.

Working with Graphs

Data Display Options

Monitoring information can be displayed in monitoring graphs according to the following criteria:

Total Bandwidth	Bandwidth consumed by both incoming and outgoing traffic.
In Bandwidth	Bandwidth consumed by incoming traffic only.
Out Bandwidth	Bandwidth consumed by outgoing traffic only.
In Packets	The number of packets in incoming traffic only.
Out Packets	The number of packets in outgoing traffic only.
Live Connections	The number of live connections (30 Second resolution only).
New Connections	The number of new connections.
Dropped Connections	The number of dropped connections

To determine the data display criteria, right-click anywhere in the graph and select **Show Data by** from the popup menu. Select the required criteria from the submenu is that is displayed. It is possible to opt to show data by percentage in **Most Active...** reports.

Clicking a point in a monitoring graph displays the value at the selected point.

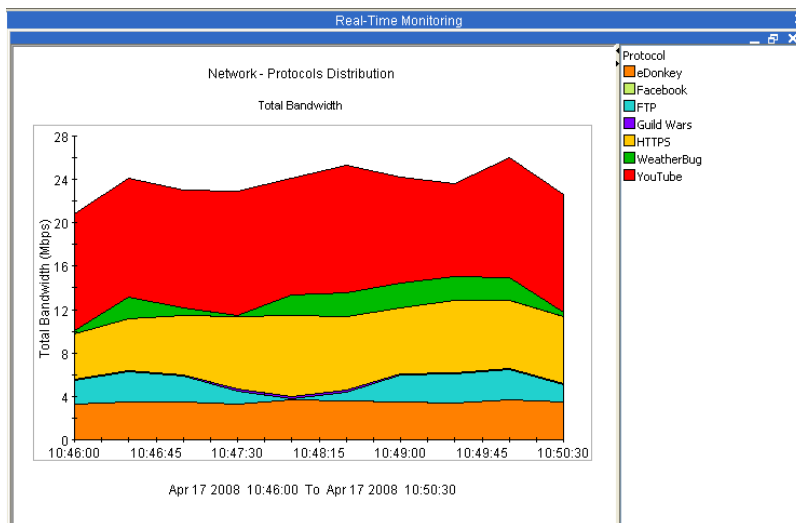


Figure 7-119: Displaying Bandwidth

Displaying All Others Data

You can opt to include a consolidated entry for multiple items entitled "All Others". For example, if you are generating a report on the 10 most active pipes, the data for all additional pipes can be consolidated into an All Others item.

To display consolidated data for all others, right-click anywhere in the graph and select **Display Options | All Others** from the popup menu.

Sorting Data in the Graph

You can sort the data in the graph according to total bandwidth, incoming bandwidth, outgoing bandwidth or according to alphabetical order. For example, if you are generating a bar chart on the 10 most active pipes, the data for all additional pipes can be shown in alphabetical order rather than sorted according to relative traffic.

To sort the data in the graph, right-click anywhere in the graph and select **Display Options | Order Display by** from the popup menu. Then select the criteria for sorting from the corresponding submenu. The available options vary according to the type of report.

Drilling Down into Graph Results

NetXplorer enables you to drill down within any Most Active graph to view a cross-section of data for a specific entity represented in the graph. For example, upon examining a Most Active Pipes graph for a specific NetEnforcer, you may want to view the breakdown of utilization for a specific VC or protocol.

There is no limit to the number of times that you can drill down within graphs.

NOTE **External Hosts collection is disabled and it is not possible to drill down into Most Active Conversations or Most Active External Hosts graphs. It is recommended that HTTP reports be used to access such data.**

The following example illustrates one possible progression of drilling down to view further details.

The first graph, a Long-Term Report, displays the Most Active Virtual Channels on the network (Figure 7-120).

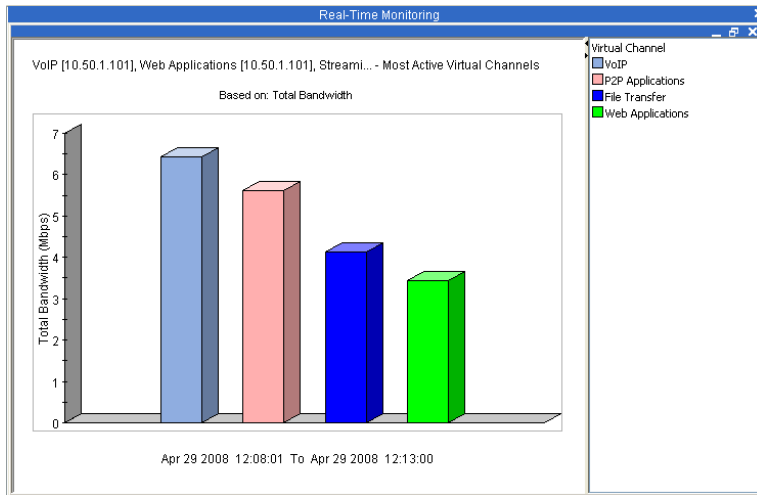


Figure 7-120: Most Active Virtual Channels

By right-clicking the corresponding bar and selecting Protocols Distribution from the popup menu, the example drills down to view the breakdown of protocols for the Virtual Channel VoIP (Figure 7-121).

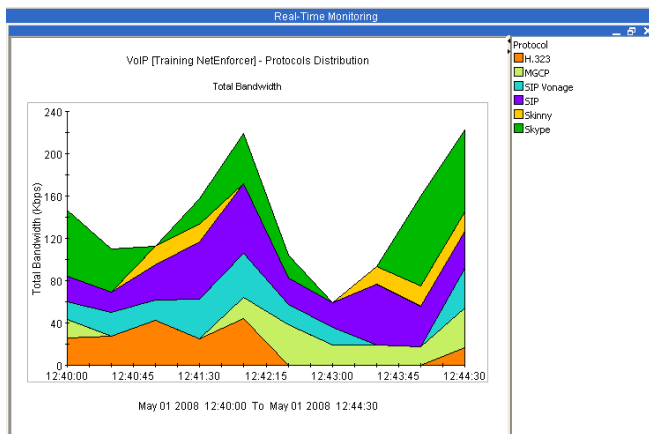


Figure 7-121: Protocols Distribution on Virtual Channel VoIP

By right-clicking the corresponding area in the graph and selecting Most Active Hosts from the popup menu, the example drills down to view Most Active Hosts for the protocols for the Virtual Channel VoIP.

Favorite View

You can display multiple monitoring windows at the same time and arrange them to suit your own needs. You can save a particular arrangement of monitoring windows as your Favorite View. Your Favorite View can include both real-time and long-term monitoring graphs.

By default, the following graphs are defined for Favorite View: Statistics on Network, Most Active Pipes on Network, Most Active VCs on Network, Most Active Protocols on Network, Most Active Internal Hosts on Network.

To display the Favorite View:

- From the View menu, select **Favorite View** or click  on the toolbar. The Favorite View is displayed.

To add a graph to the Favorite View:

1. Display the required graph and then select **Add to Favorite View** from the Actions menu or click the **Add** button on the toolbar.


OR

Right-click the graph and select **Add to Favorite View** from the popup menu.

The graph is added to the Favorite View.

2. Display the Favorite View and arrange or resize the graphs, as required.

To delete a graph from the Favorite View:

- Select the graph in the Favorite View and then select **Delete** from the Edit menu or click  on the toolbar.

OR

- Right-click the graph in the Favorite view and select **Delete** from the popup menu.

The graph is removed from the Favorite view.

Monitoring Groups

NetXplorer's Groups enable you to consolidate monitoring information by defining customized groups of Line, Pipes or Virtual Channels. Real-time and long-term monitoring graphs generated for a Monitoring Group treat the members of the group as a single entity.

Separate Groups are defined for Lines, Pipes, and Virtual Channels.

Viewing Groups

You can view existing Groups in the Groups application.

To view groups:

1. Select **Groups** in the Navigation pane. The existing Groups are listed in the Navigation tree. The level of the Group is indicated by the type of icon in the tree.

NOTE The Groups list is not displayed in hierarchical format. The level of the Group (Line, Pipe, or Virtual Channel) is indicated by the displayed icon.

2. Select a Group in the Navigation tree. The members of the selected group are listed in the Application Details pane.

Defining a Line Group

A Line Group enables you to view monitoring graphs for a composite group of Lines.

To define a Line group:

1. From the Actions menu, select **New Line Group**.

OR

With Groups selected in the Navigation pane, right-click in the Navigation pane and select **New Line Group** from the popup menu.

The Group Properties dialog is displayed.

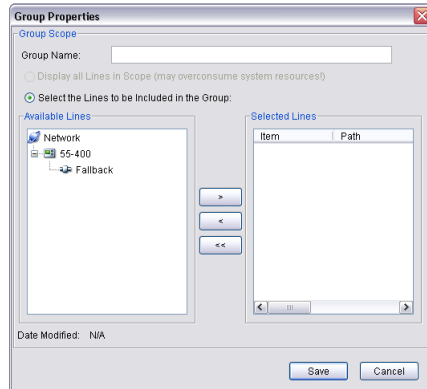



Figure 7-122: Group Properties – Line Group

2. Enter a name for the group in the **Group Name** field.
3. Configure the Lines to be included in the group, as follows:
 - Expand the required NetEnforcer/s or Service Gateway/s(s) in the tree in the **Available Lines** list.
 - Select the required Lines in the tree and click  to move the Lines to the **Selected Lines** list or double click the Line you wish to move.
 - Repeat for all additional Lines, as required.

NOTES You can select and move more than one line at a time using standard Windows multiple selection methods.

Select a line and click to move the line from the Selected Lines list to the Available Lines list. Click to clear the Available Lines list.

4. When all of the required Lines have been moved to the **Selected Lines** list, click **OK** to save the group. The group is added to the Groups list in the Navigation pane.

Defining a Pipe Group

A Pipe Group enables you to view monitoring graphs for a composite group of Pipes.

To define a Pipe group:

1. From the Actions menu, select **New Pipe Group**.

OR

With Groups selected in the Navigation pane, right-click in the Navigation pane and select **New Pipe Group** from the popup menu.

The Items Selection dialog is displayed.

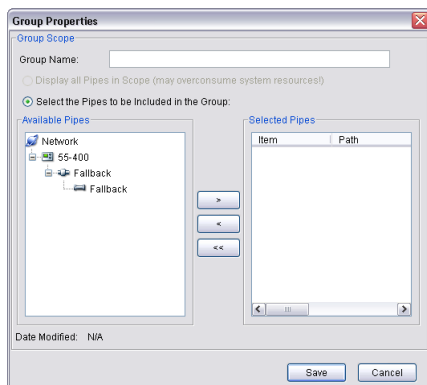


Figure 7-123: Group Properties – Pipe Group

2. Enter a name for the group in the Group Name field.
3. Configure the Pipes to be included in the group, as follows:
 - Expand the required NetEnforcer/s or Service Gateway/s(s) in the tree in the **Available Pipes** list.
 - Select the required Pipes in the tree and click to move the Pipes to the **Selected Pipes** list or double click the Pipe you wish to move.
 - Repeat for all additional Pipes, as required.

NOTES You can select and move more than one Pipe at a time using standard Windows multiple selection methods.

Select a Pipe and click  to move the line from the Selected Pipes list to the Available Pipes list. Click  to clear the Available Pipes list.

- When all of the required Pipes have been moved to the **Selected Pipes** list, click **OK** to save the group. The group is added to the Groups list in the Navigation pane.

Defining a Virtual Channel Group

A Virtual Channel Group enables you to view monitoring graphs for a composite group of Virtual Channels.

To define a Virtual Channel group:

- From the Actions menu, select **New Virtual Channel Group**.

OR

With Groups selected in the Navigation pane, right-click in the Navigation pane and select **New Virtual Channel Group** from the popup menu.

The Items Selection dialog is displayed.

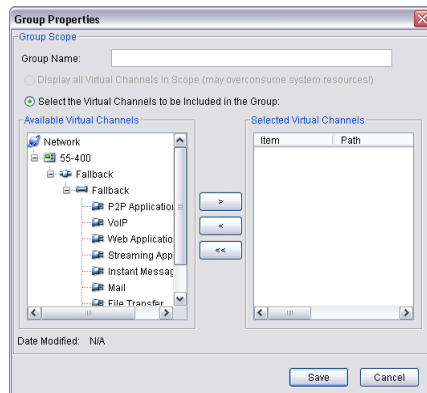



Figure 7-124: Items Selection – Virtual Channel Group

- Enter a name for the group in the **Group Name** field.
- Configure the Virtual Channels to be included in the group, as follows:
 - Expand the required NetEnforcer/s or Service Gateway/s in the tree in the **Available Virtual Channels** list.
 - Select the required Virtual Channels in the tree and click  to move the Virtual Channels to the **Selected Virtual Channels** list or double click the Virtual Channel you wish to move.
 - Repeat for all additional Virtual Channels, as required.

NOTE You can select and move more than one Virtual Channel at a time using standard Windows multiple selection methods.

4. When all of the required Virtual Channels have been moved to the **Selected Virtual Channels** list, click **OK** to save the group. The group is added to the Groups list in the Navigation pane.