a mind for networks

NetXplorer

Centralized NetEnforcer® Management Software

Administration Guide

(P/N D354005 R3)

AllOt communications

NetXplorer

Centralized NetEnforcer Management Software

Administration Guide

P/N D354005 R3

Important Notice

Allot Communications Ltd. ("Allot") is not a party to the purchase agreement under which NetEnforcer 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

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.

Printing History

First Edition: February, 2007
Second Edition: July, 2007
Third Edition: May, 2008

FIGURES

Chapter 1: Getting Started

Overview

NetXplorer is a highly scalable Network Business Intelligence system that enables strategic decision-making based on comprehensive network application and subscriber traffic analysis.

NetXplorer configures NetEnforcer devices and a central catalog, which enables global policy provisioning. Many network topologies can benefit from more than one NetEnforcer. In addition, NetXplorer provides a centralized management system for all NetEnforcers on the network. It provides easy access to devices and configuration parameters via the device tree.

By enabling real time monitoring of network troubleshooting and problem analysis, NetXplorer provides long term reporting for capacity planning, tracking usage and trend analysis; it allows for the proactive management of traffic and system-wide alarms; and it allows for the collection and export of auditing data for billing and quota purposes.

Terms and Concepts

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

NetXplorer

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

The NetXplorer server can be installed on any server running Windows Server 2003 or Windows XP SP2.

NetEnforcer

NetEnforcers are the traffic management devices that inspect and monitor network traffic.

Monitoring Collector

The Monitoring Collector is an Allot appliance that can be added between the NetXplorer Servers and the NetEnforcers in order to support large numbers of NetEnforcers or NetEnforcers installed in remote geographic locations.

QoS

QoS (Quality of Service) is the ability to define a level of performance in a data communications system. In NetXplorer, QoS is an action applied to a connection when the conditions of a filter are satisfied.

The QoS specified can include the following:

- **Prioritized Bandwidth**: Delivers levels of service based on class levels. During peak traffic periods, the NetXplorer will slow down lower priority applications, resulting in increased bandwidth delivery to higher priority applications.
- **Guaranteed Bandwidth**: Enables the assignment of fixed minimum and maximum amounts of bandwidth to specific Pipes, Virtual Channels and connections. By borrowing excess bandwidth when it is available, connections are able to burst above guaranteed minimum limits, up to the maximum guaranteed rate. Guaranteed rates also assure predictable service quality by enabling time-critical applications to receive constant levels of service during peak and non-peak traffic periods.
- **Reserved Bandwidth on Demand**: Enables the reservation of the minimum bandwidth from the first packet of a connection until the connection ends. This is useful when the bottleneck is not at the link governed by NetEnforcer. By limiting other connections (non-guaranteed), NetEnforcer reserves enough bandwidth for the required Pipe or Virtual Channel.

- **TOS Marking**: Enables the user to set the ToS bytes in the transmitted frame according to the DiffServ standard or free format.
- **Access Control**: Determines whether a connection is accepted, dropped or rejected. For example, you can specify the following policy: accept 1000 ICMP connections to Server1 and drop the rest. A NetEnforcer policy can also be to drop all P2P connections or accept new connections with a lower priority
- **Admission Control**: Determines the bandwidth granted to a flow based on your demand (for example, allocated minimum of 10kbps) and the available bandwidth on the line.

Catalog Editors

Catalog Editors enable you to define values to define your policy. The possible values for each condition of a filter and for actions 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 or action

Lines

A Line represents a physical or logical media 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 all of the conditions are met. A line is an address-based or VLAN-based entity, and is not service-based.

A Line can aggregate several Pipes, acting like a container of Pipes from a QoS point of view. The filter 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 all 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.

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. Pipes cannot stand alone and are always contained within a Line. A Pipe consists of one or more sets of conditions and a set of actions that apply when all 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 **Fallback** Virtual Channel filter cannot be modified or deleted. A connection coming into a line is matched to a Pipe according to whether the characteristics of the connection match all 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 and a set of actions that apply when all of the Conditions are met. A Virtual Channel is defined within a Pipe and cannot stand alone. A connection matched to a Pipe is further matched to a Virtual Channel according to whether the characteristics of the connection match all of the Conditions of the Virtual Channel.

Conditions

A Condition is defined at the Line level, Pipe level or Virtual Channel level. NetXplorer matches connections to conditions, first at the Line level then at Pipe level and then again at the Virtual Channel level within a Pipe.

Templates

Templates enable you to create a "master" Pipe or Virtual Channel that upon saving will create multiple Pipes or Virtual Channels similar to one another. Templates work with host group entries and LDAP-based hosts entries defined in the Host Catalog. For example, if a host group entry in the Host Catalog called Gold Customers consists 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 Policy Editor is saved.

A Pipe or Virtual Channel template enables the fast creation of Pipes and Virtual Channels on source/destination differentiation. This means that you do not need to define similar Pipes and Virtual Channels when the only difference between them is the IP address in the source or destination.

NetXplorer Architecture

This section introduces the NetXplorer concept and explains its components and architecture.

NetXplorer uses a highly scalable architecture that enables the monitoring of all NetEnforcer devices from a single user interface. In addition, NetXplorer can utilize distributed monitoring collectors, which increase the scalability of your deployment. The collectors gather short-term network usage statistics from the NetEnforcers.

NetXplorer's server-based, distributed architecture consists of four tiers: multiple NetEnforcers and associated distributed collectors, a NetXplorer server and GUI clients.

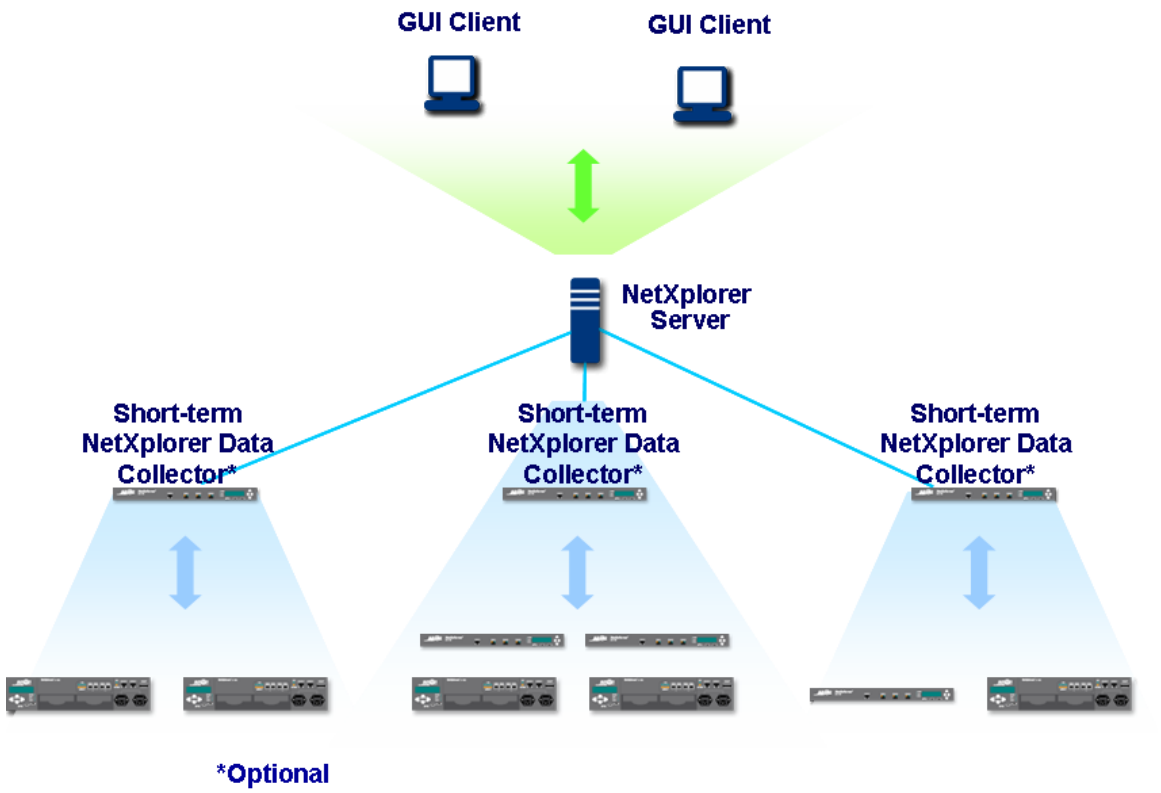

Figure 1-1: System Architecture

NetXplorer architecture consists of four layers:

1. **NetEnforcer layer**: NetEnforcers are the traffic management devices that inspect and monitor network traffic. There can be one or more NetEnforcers on a network. They manage network policies and collect network usage data.
2. **Monitoring Collectors –** Monitoring collectors increase scalability by supporting large numbers of NetEnforcers or NetEnforcers installed in remote geographic locations. Monitoring collectors are fully managed via the NetXplorer GUI.

3. **Server Layer**: The NetXplorer server is the actual application, which includes the databases and an integrated data collector. The NetXplorer server manages and communicates with the different clients that access the system, and facilitates NetEnforcer configuration, policy provisioning, alarms, monitoring and reporting. The integrated data collector included in the NetXplorer streamlines the required collection of data from the managed NetEnforcer devices. The Server layer includes additional servers such as SMP Servers, NPP Servers and stand along Accounting Servers.
4. **User Interface Layer**: The different clients connected to the NetXplorer Server are the *NetXplorer GUI application* users. Any network computer capable of connecting to the NetXplorer server can support the GUI interface.

The system offers simple integration with external systems using a wide range of interfaces, including SNMP, CSV Files (for report data export), XML and CLI.

Administration Role

NetXplorer uses a role-based security model. The role defined for each authorized user indicates the scope of operations that can be performed by that user. The Administrator role gives Admin users complete read/write privileges in the NetXplorer application including read/write configuration privileges.

The main functions of the Administrator role include:

- User Registration
- Device and Network Management
- Monitoring Collectors Management
- Database Maintenance

This document defines the main concepts and describes the various activities related to the installation and configuration of NetEnforcers and the NetXplorer, Monitoring Collectors, as well as the main tasks associated with Database Maintenance, such as backup and restore, changing location and installing the NetXplorer on a remote data base.

Chapter 2: Configuration

Overview

This chapter describes the processes used to configure, add and change NetEnforcers and other devices as well as how to register and maintain users.

The NetXplorer, once installed on the network, enables the central configuration of managed NetEnforcers and Monitoring Collectors. It has an easy GUI interface that provides access to all the devices via a device tree. All available configuration parameters can be accessed via the GUI.

Monitoring Collectors may be added between the NetXplorer Servers and the NetEnforcers, in order to support sparse and remote geographic regions.

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

For more information concerning the NetXplorer Server, contact Allot Customer Support at support@allot.com.

NOTE Once the NetXplorer is installed, you should pre-allocate disk space for the monitoring information that will be collected. Please see Chapter 4 – Database Management.

To enable NetXplorer Server:

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

   The NetXplorer Application Server Registration dialog box appears.

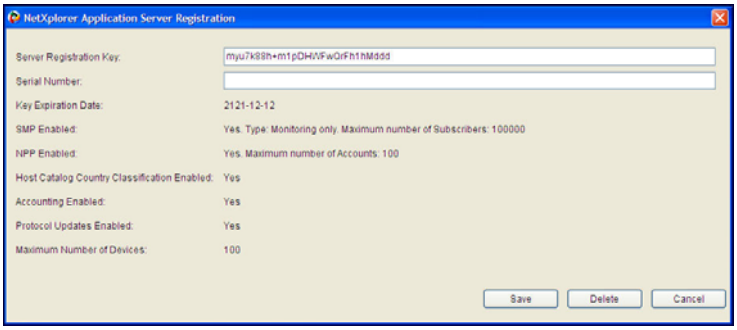

Figure 2-1: NetXplorer Application Server Registration Dialog

2. Enter the Server Registration Key and Serial Number provided by Allot to enable the NetXplorer Server functionality.
3. An Expiration Date will be generated automatically after clicking **Save**.
4. If Subscriber Management is enabled by the key that has been entered, it will be indicated (along with the type and the maximum number of subscribers) after **SMP Enabled**. For more information, see the SMP User Guide.
5. If Policy Provisioning is enabled by the key that has been entered, it will be indicated (along with the maximum number of accounts) after **NPP Enabled**. 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 **Host Catalog Country Classification Enabled**.
7. If Accounting information is enabled by the key that has been entered, it will be indicated after **Accounting Enabled**.
8. If Service Catalog updates via the web are enabled by the key that has been entered, it will be indicated after **Protocol Updates Enabled**.

9. The Maximum number of devices covered by the entered key is indicated.

10. Click **Save** to enter the key and close the dialog box.

Working with Devices

In order for NetXplorer to manage a Device (NetEnforcer, SMP, etc), it must be added to the NetXplorer's network and properly configured. The IP address of the NetEnforcer is required for this procedure.

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

To add a NetEnforcer:

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.

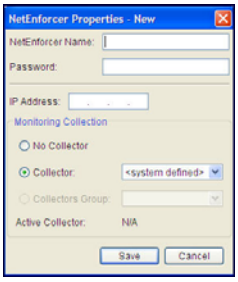

Figure 2-2: NetEnforcer Properties – New Dialog

2. Enter the User Name and Password of the NetXplorer administrator and the IP address of the NetEnforcer in the designated fields.

3. Assign a Monitoring Collector or Collector Group to the NetEnforcer from the drop down menus. This means that the new NetEnforcer 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 is added to the Navigation tree. The Add NetEnforcer operation can take up to a couple of minutes to complete.

To Import a NetEnforcer:

1. A NetEnforcer 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 is imported, its 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.

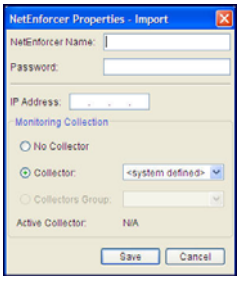

Figure 2-3: NetEnforcer Properties – Import Dialog

3. Enter the User Name and Password of the NetXplorer administrator and the IP address of the NetEnforcer in the designated fields.

4. Assign a Monitoring Collector or Collector Group to the NetEnforcer from the drop down menus. This means that the new NetEnforcer 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**.

5. Click **OK**. The NetEnforcer is added to the Navigation tree. The Import NetEnforcer operation can take up to a couple of minutes to complete.

To add a Monitoring Collector

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

   OR

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

   The Monitoring Collector Properties - New dialog is displayed.

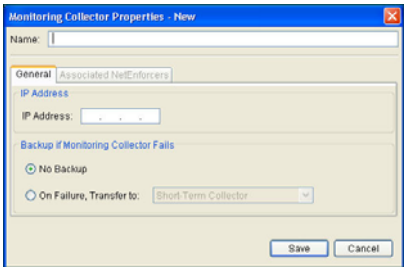

Figure 2-4: Monitoring Collector Properties – New Dialog

2. On the General tab, enter the Name and IP address of the Monitoring Collector.

3. In the Backup if Monitoring Collector Fails area, select one of the two radio buttons, **No Backup** or **On Failure, Transfer To…**. If **On Failure, Transfer To…** is selected, select the backup Monitoring Collector from the drop down menu.

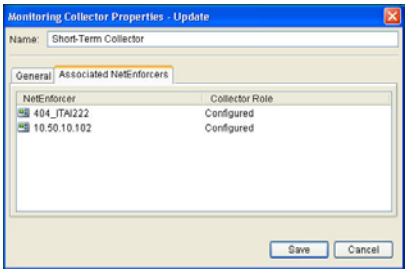

Figure 2-5: Monitoring Collector Properties – New Dialog

4. In the Associated NetEnforcers tab, a list of all NetEnforcers transmitting monitoring information to this Collector appears. They are assigned by right clicking on a NetEnforcer in the Network pane and selecting **Properties**.

5. Click **Save**. The Monitoring Collector is added to the Navigation tree. The Add Monitoring Collector operation can take up to a couple of minutes to complete.

NOTE For more information concerning Monitoring Collectors, see the NetXplorer Administration Guide.

To add a Collector Group

Collector Groups are made up of two Collectors, providing 1+1 redundancy.

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

The Collector Group Properties - New dialog is displayed.

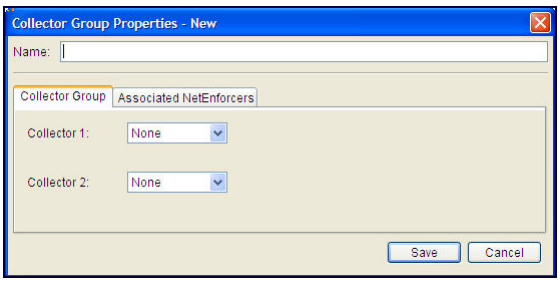

Figure 2-6: Collector Group Properties – New Dialog

2. In the Collector Group tab Select the two Collectors (already part of the network) to be included in the group. Collector 2 will act as the backup for Collector 1.
3. Those NetEnforcer's associated to the added Collectors will be listed in the Associated NetEnforcers tab.
4. Click **Save**. The Collector Group is added to the Navigation tree. The Add Collector Group operation can take up to a couple of minutes to complete.

To add an SMP

NOTE This feature is only available with the appropriate license key, enabling Subscriber Management. Contact Allot Customer Support at support@allot.com for more information concerning your license.

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

   OR

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

   The SMP Properties - New dialog is displayed.

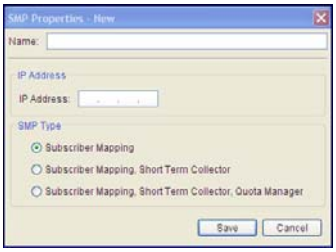

Figure 2-7: SMP Properties – New Dialog

2. Enter the Name and IP address of the SMP.
3. Select the SMP Type using the radio buttons. Select either Subscriber Mapping, Subscriber Mapping Short Term Collector or Subscriber Mapping Short Term Collector Quota Management.
4. Click **Save**. The SMP is added to the Navigation tree. The Add SMP operation can take up to a couple of minutes to complete.

NOTE For more information concerning SMPs, see the Allot SMP User's Manual.

To add an SMP Group

NOTE This feature is only available with the appropriate key. Contact Allot Customer Support at support@allot.com for more information.

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

   The SMP Group Properties - New dialog is displayed.

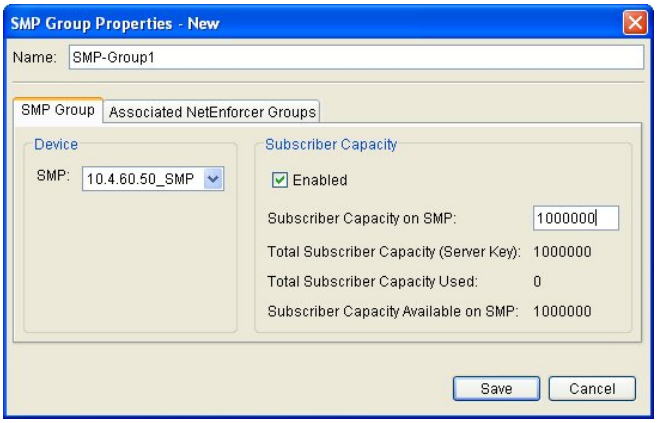

Figure 2-8: SMP Group Properties – New dialog

2. Select the SMP from the list in the Device area.
3. To activate and enforce the subscriber capacity you are about to define, retain the default **Enabled** subscriber capacity option.
4. Define the subscriber capacity in the Subscriber Capacity area, for example, type in 1000000.

NOTE Each SMP server supports up to 1 million subscribers and up to 500 updates per second. If the amount of NE and SMP Servers need to be increased to handle your Network subscribers, purchase and install the appropriate amount of SMP Servers.

5. You may save the SMP Group data you have entered by clicking **Save** or open the Associated NetEnforcer Group tab, and define up to 10 NetEnforcers for each named SMP/NE Group.

NOTE For more information concerning SMP Groups, see the Allot SMP User's Manual.

To change the IP of a NetEnforcer:

1. Select the NetEnforcer device in the Navigation tree and then select Properties from the Actions menu.

   The Device Properties-Update dialog is displayed.

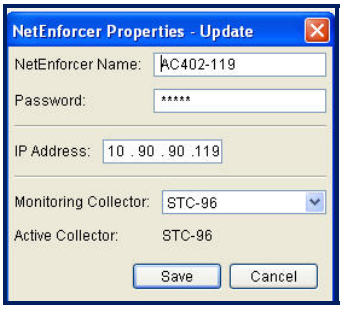

Figure 2-9: Device Properties Update dialog

2. Enter the User name, Password of the NetXplorer administrator
3. Enter the new IP address of the NetEnforcer in the designated field
4. Click **Save**

NOTE **If you change the IP of the NetEnforcer, you must also change the IP in the device configuration of the NetXplorer.**

To Remove a NetEnforcer from the network:

1. Right-click Network and select a NetEnforcer and select Delete.

   The following Delete message is displayed.

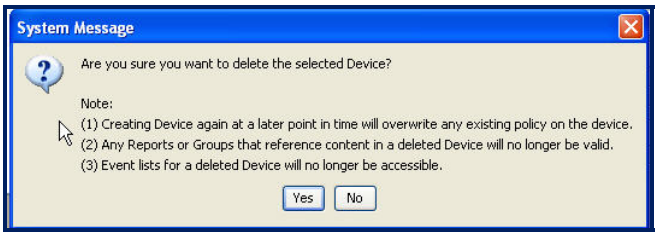

Figure 2-10: System Message

2. Click Yes to delete the NetEnforcer.

To configure a NetEnforcer via the NetXplorer:

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

   OR

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

   OR

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

   The Configuration window for the selected NetEnforcer is displayed.

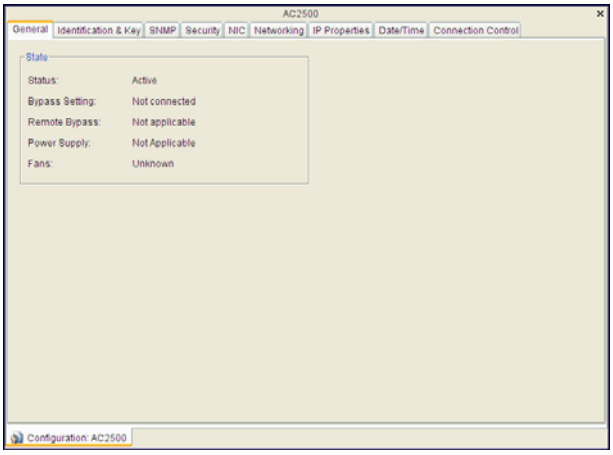

Figure 2-11: NetEnforcer Configuration

2. Configure the NetEnforcer parameters, as required.

3. Click  or select **Save** from the File menu to save the changes to the NetEnforcer configuration.

NOTE For detailed descriptions of the parameters in each of the NetEnforcer Configuration tabs, refer to *NetEnforcer Configuration Parameters* in the NetXplorer Operations Manual.

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

- **General** – indicates the NetEnforcer's bypass status.
- **Identification and Keys** – includes parameters that provide system information and activation keys
- **SNMP** – enter the contact person, location, system name and description for SNMP purposes
- **Security** – includes security and authorization parameters

- **NIC** – includes parameters to configure the system interfaces to either automatically sense the direction and speed of traffic or use default parameters as well as parameters to define ports
- **Networking** – includes parameters that enable you to configure network topology
- **IP Properties** – enables you to modify the IP and host name configuration of your network interfaces as well as the DNS and connection control parameters
- **Date/Time** – includes the date, time and NTP server settings for the NetEnforcer
- **Connection Control** - includes IP and Port Redirection Parameters

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. Resetting is required to ensure that some saved parameter values are committed and activated on the NetEnforcer.

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 configuration.

Network Configuration Parameters

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

- Servers, below
- SNMP v3, page 2-17
- SMP Domains, page 2-18
- Accounting, page 2-22
- Protocol Updates, page 2-24

Servers

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

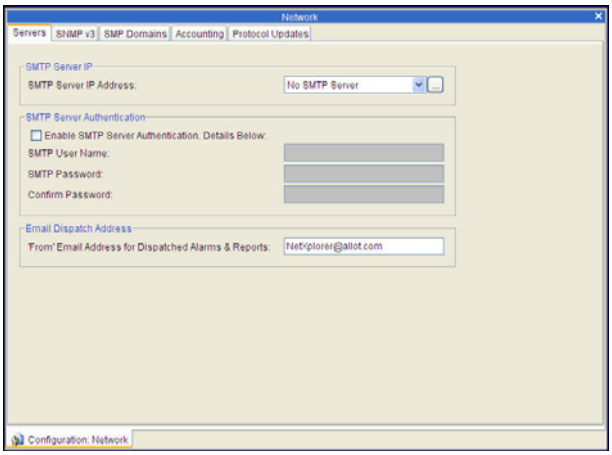

Figure 2-12: Network Configuration – Servers

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

Parameter	Definition
SMTP Server IP Address	The IP address of the SMTP server that is used for emailing alarms and reports.
Enable SMTP Server Authorization	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.

Parameter	Definition
Confirm Password	The password to be used for the defined SMTP username. (When assigning a password, the password is entered again here for confirmation.)
'From' Email Address for Dispatched Alarms & Reports	The Email address that will be shown as the source of any notifications of Alarms or Events.

SNMP v3

The **SNMP v3** tab includes parameters that enable secure communications between NetXplorer and the NetEnforcers. Secure communications can be configured to include authentication and/or encryption.

Upon saving any changes made in this SNMP panel, all NetEnforcer 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 NetEnforcers as well as on the network. See the NetXplorer Operation Guide for more information.

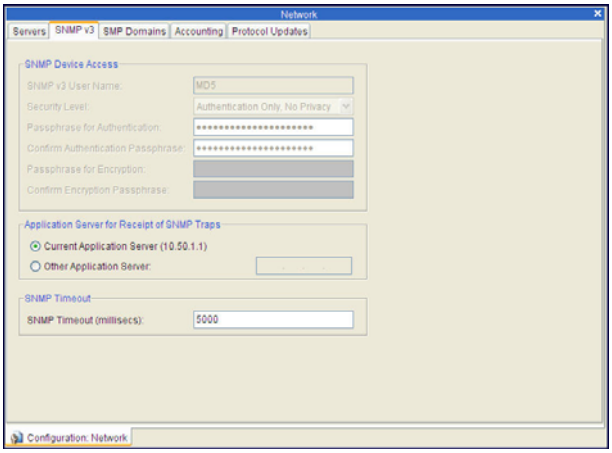

Figure 2-13: Network Configuration – SNMP v3

The **SNMP v3** tab includes the following parameters:

Parameter	Definition
SNMP v3 User Name	The user name defined for the SNMP Server.

Parameter	Definition
Security Level	The level of security for communications between the NetXplorer and NetEnforcers: **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).
Application Server for Receipt of SNMP Traps	The Application Server where SNMP traps are to be sent. The current server can be selected or IP address of another server can be entered.
SNMP Timeout	The SNMP timeout may be entered, in milliseconds.

WARNING **Upon saving any changes made in the SNMP panel, all NetEnforcer 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, contact Allot Customer Support at support@allot.com.**

To configure a NetEnforcer's SNMP via the CLI:

Log onto the NetEnforcer via Telnet and enter the following CLI command:

go config snmp <-OPTION> <VALUE>...

Options:

-snmpLogin <SecurityName:SecurityLevel[:AuthProtocol[:PrivProtocol]]> set security info

- Security level values are: noAuthNoPriv, authNoPriv, authPriv
- Auth protocol values are: usmHMACMD5, usmHMACSHA
- Priv protocol values are: usmDES, usmIDEA, usmAES128, usmAES192, usmAES256

-users <Prefix><USER>[,<Prefix><USER>,...] add/delete agent users

USER format : <SecurityName:SecurityModel[:Group:AuthProtocol:PrivProtocol]>

- Prefixes
  - + to add user, all parameters be specified
  - - to delete user, only SecurityName and SecurityModel can be specified
- Group: enter 'view snmp' command to see existing groups
- Security Model values are: any, v1, v2c, usm
- Auth protocol values are: usmNoAuth, usmHMACMD5, usmHMACSHA
- Priv protocol values are: usmNoPriv, usmDES, usmIDEA, usmAES128, usmAES192, usmAES256

-pass_change <SecurityName:AuthProtocol[:PrivProtocol]> change snmp agent user pass phrase

- Auth protocol values are: usmHMACMD5, usmHMACSHA
- Priv protocol values are: usmDES, usmIDEA, usmAES128, usmAES192, usmAES256

-trap_target <Prefix><TARGET>[,<Prefix><TARGET>,...] add/delete trap targets

TARGET format :
<Name[:SecurityName:SecurityModel:MPModel:SecurityLevel:IP[:Port]]>, default port=162

- Prefixes:
  - + to add trap target, all parameters must be specified except port number
  - - to delete trap target, in this case only Name can be specified
- MP Model values are: v1, v2c, v2u, v3

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.

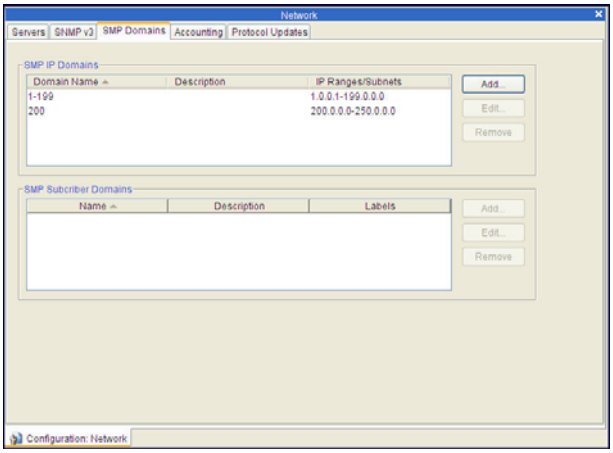

Figure 2-14: Network Configuration - SMP Domains tab

NOTE This feature is only available with the appropriate key. Contact Allot Customer Support at support@allot.com for more information.

Accounting

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

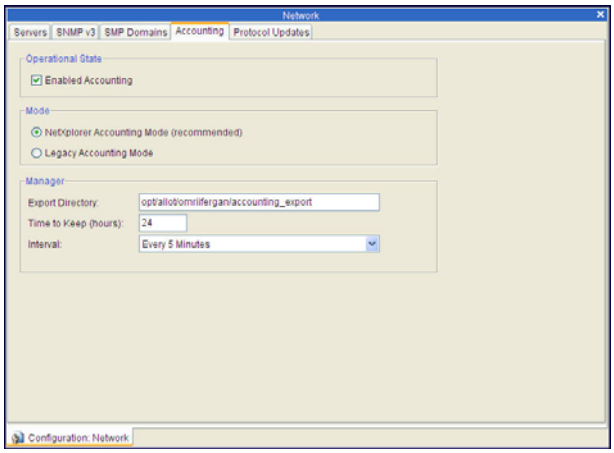

Figure 2-15: Network Configuration - Accounting tab

NOTE This feature is only available with the appropriate key. Contact Allot Customer Support at support@allot.com for more information.

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 Legacy 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.

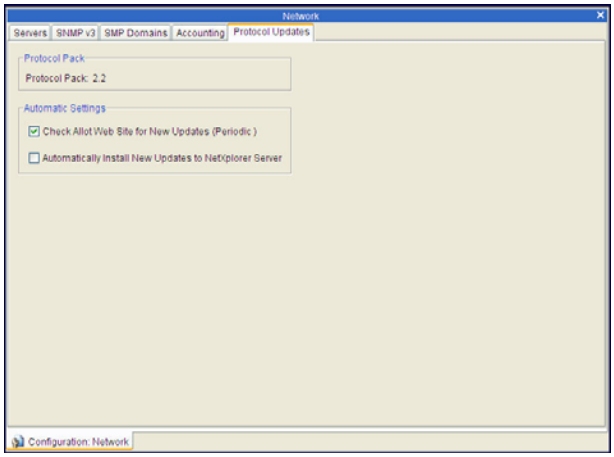

Figure 2-16: Network Configuration – Protocol Updates tab

NOTE This feature is only available with the appropriate key. Contact Allot Customer Support at support@allot.com for more information.

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.

Parameter	Definition
Automatically Install New Updates to NetXplorer Server	Enables NetXplorer to automatically install and new Updates onto the Server (but not individual NetEnforcers).

Configuring NetXplorer Users

NetXplorer implements a role-based security model. The role defined for each authorized user indicates the scope of operations that can be performed by the user.

There are three types of NetXplorer roles, as follows:

- **Regular:** Read/write privileges in the NetXplorer application not including User Configuration definitions.
- **Monitor**: Read-only access.
- **Administrator**: Read/write privileges in the NetXplorer application, which includes read/write privileges to define User Configurations.

This section describes the processes used to register and maintain users. It includes how to add a new user, change a user's information and how to delete a user.

To Add a New User:

1. Select the **Users Configuration Editor** from the Tools menu.
2. The Users Configuration Editor dialog is displayed, listing all currently defined NetXplorer users.

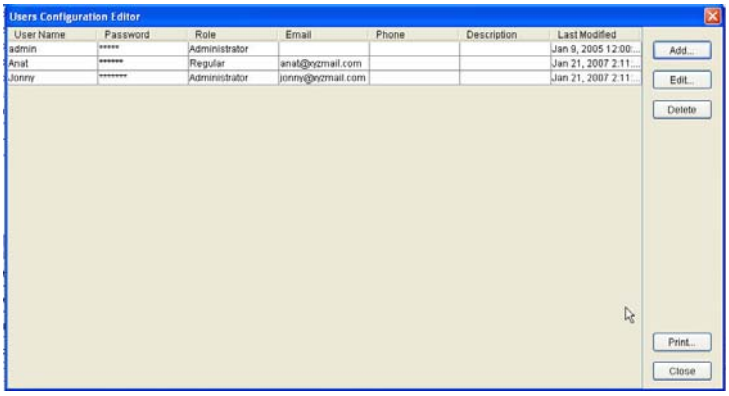

Figure 2-17: Users Configuration Editor

3. Click **Add**.

   The User Editor dialog is displayed.

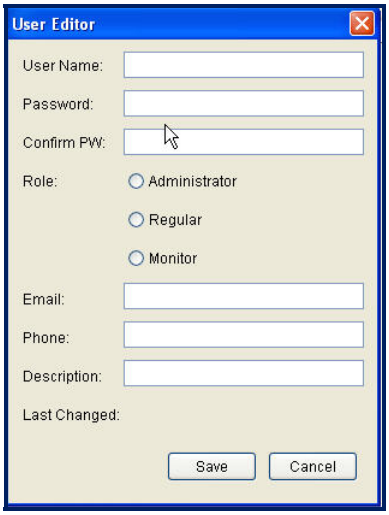

Figure 2-18: User Editor

4. Enter the name of the user in the **User Name** field.

5. Enter a password for the user in the **Password** field and then again in the **Confirm PW** field.

NOTE The user password must be at least six characters in length and include at least one numerical digit.

6. Set the permissions level of the user by selecting the radio button for the required role (Administrator, Regular or Monitor).
7. (Optional) Enter the user's contact information in the Email and phone fields. You can also enter a brief description in the designated field.
8. Click **OK**.
9. The new user has been added to the list of users in the Users Configuration Editor dialog.

To edit user information:

1. In the Users Configuration Editor dialog (Figure 3-18), select the user whose information you want to edit
2. Click **Edit**.

   The User Editor dialog is displayed.
3. Edit the user parameters, as required
4. Click **OK**.

To delete a user:

1. In the Users Configuration Editor dialog, select the user(s) to be deleted
2. Click Delete.
3. A confirmation message is displayed.
4. Click **Yes** to confirm the deletion.

The user is no longer able to access the NetXplorer.

WARNING: There must be at least one Administrator user in the system.

Chapter 3: Monitoring Collectors

Overview

Allot's NetXplorer utilizes Distributed Monitoring Collectors. The collectors gather short-term network usage statistics from the NetEnforcers.

The clearest reason to use distributed monitoring collectors is to increase the scalability of your deployment. Each collector can support several NetEnforcers. By deploying distributed collectors, you can increase the total number of NetEnforcers supported by a single NetXplorer server. This is possible because the NetXplorer can now split the storage of the real-time monitoring data between several short-term databases.

A second reason for using distributed monitoring collectors is to overcome connectivity issues in distributed networks. In order to support data collection, the line speed between the NetEnforcer and the collector must be at least 10Mbps mainly for the high throughput devices such as AC-1000 and 2500. If you are working with a low throughput device, for example an AC-400 with 2 or 10 Mbps, statistics can be collected over slower connections without the need for distributed collectors.

Up until now, the collectors have always been situated on the NetXplorer server. However, some cases the networks have topology that does not allow for a 10Mbps line between the NetEnforcer and the server. This can happen for example when the network is spread out over remote geographical locations. In such cases, the use of collectors is necessary. The line between the NetEnforcers and their collectors will be at least 10Mbps. The line between the collectors and the NetXplorer server can be of lower capacity however, a collector is needed for each network zone that cannot guarantee a 10Mbps connection to the server.

A third reason for deploying distributed monitoring collectors is redundancy. If a collector is unavailable, data from the NetEnforcers, which this collector supports, can automatically be collected by a defined backup collector.

Data Collection Process

In a NetXplorer implementation, which does not include external collectors, the NetXplorer server has its own internal short-term collector.

NOTE **This short-term collector cannot be deleted even if there are external collectors.**

Traffic statistics are collected in buckets. There are 30-second buckets and 5-minute buckets. The buckets are imported into the database by the collector per sample period. In a NetXplorer implementation, which does not include external collectors, the buckets are loaded into the short-term database, located on the NetXplorer, every 30 seconds or 5 minutes. Long-term buckets are created every hour on the NetXplorer and are then loaded into the long-term database on the same machine.

Implementations with external monitoring Collectors also collect samples in 30-second buckets and 5-minute buckets. The buckets are imported to the collector at every sample period. The data contained in the buckets is stored in the short-term database of the collector. The samples in the Database are aggregated into one-hour buckets, which are then loaded into the long-term database on the NetXplorer once an hour. Therefore, a NetXplorer implementation that includes external collectors will have additional traffic sent once an hour, namely, the long-term bucket. The short-term data, however, arriving every 30 seconds, will have a shorter distance to travel. This could be of great importance when NetEnforcers do not have constant connectivity to the server. External monitoring collectors can significantly lower the burden on the NetXplorer server.

The monitoring data is saved on the NetXplorer server, and can be displayed in the GUI

Collector Redundancy

In case a collector is unavailable, data from the NetEnforcers that this collector supports can automatically be collected by a defined backup collector.

There are two types of redundancy models possible:

One type of redundancy model is the N+1 model. In this case, several collectors are all backed up by a single collector dedicated to this purpose. This solution takes into account that the probability of more than one collector failing is very low. However, it may be difficult to locate the backup collector in close proximity to all of the configured collectors.

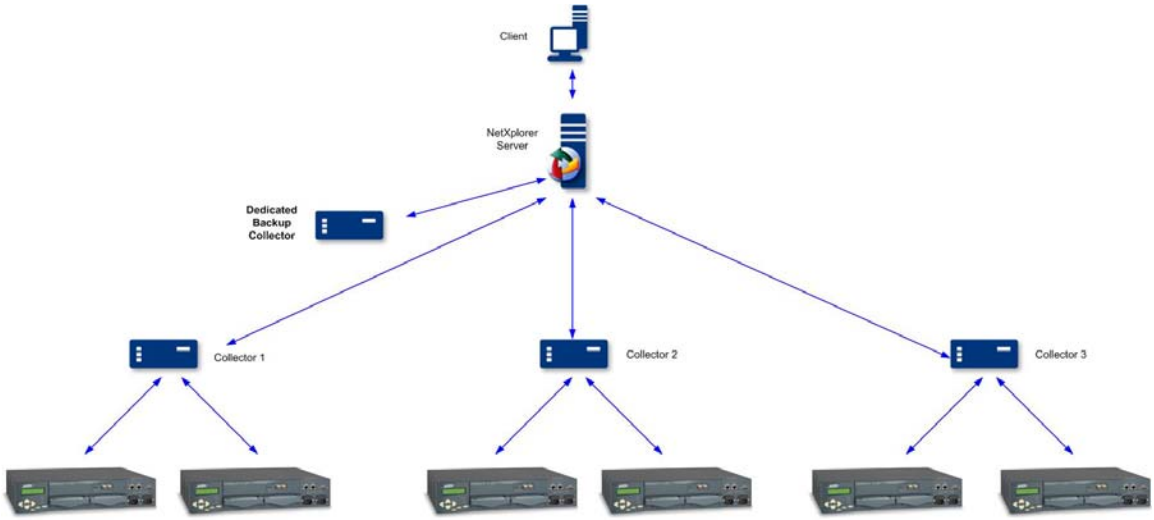

Figure 3-1 N+1 Collector Redundancy

Where high performance redundancy is of particular importance, or where the network topology does not allow for the use of a single collector for backup, you will need to use the 1 to 1 redundancy model. In this situation, each collector has a dedicated backup collector as part of a Collector Group.

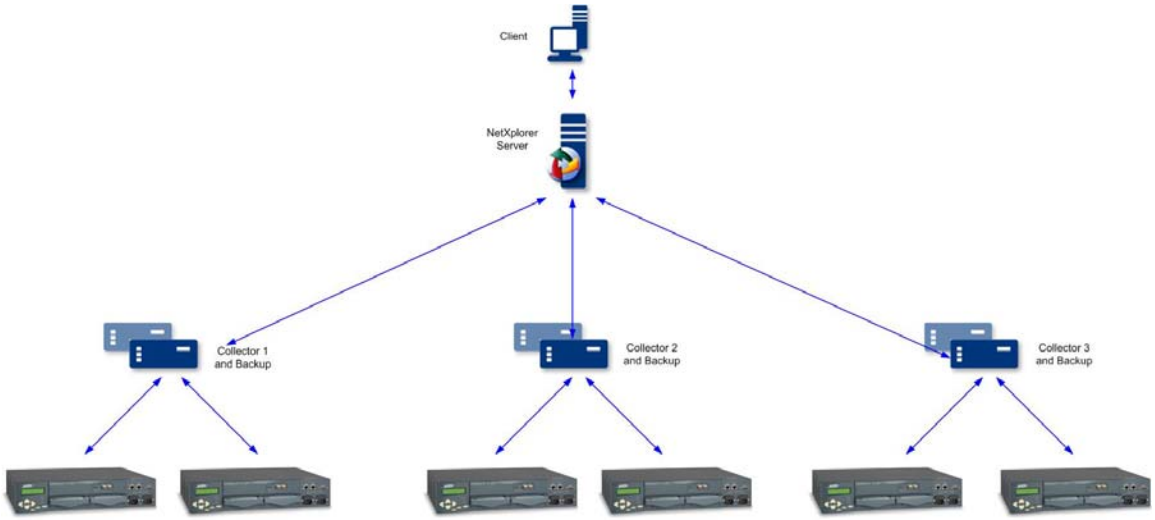

Figure 3-2 1+1 Collector Redundancy

NetXplorer Support

Each NetXplorer server can support up to five external short-term collectors in addition to its one built-in internal collector.

Each collector can support up to five (5) NetEnforcers of the AC-1000 or AC-2500 series, up to ten (10) NetEnforcers of the AC-800 or up to fifteen (15) NetEnforcers of the AC-400 series.

You can also combine NetEnforcers of different models according to this formula. For example, one collector can support three AC-1000s and six more AC-400s.

The NetXplorer's built in short-term collector can support additional NetEnforcers according to the same ratios.

NOTE: **This is a simple calculation based on a series of conservative assumptions. It is important to consult with Allot HQ to verify the exact number of collectors required.**

Installing Monitoring Collectors

The following steps must be taken in installing Monitoring Collectors:

- Set the collector's initial parameters
- Physically connect the Collector to the network
- Add the Collector to the NetXplorer using the NetXplorer user interface
- Associate NetEnforcers to the Collector to the NetEnforcer

To set initial parameters of the Monitoring Collector:

1. Connect a monitor and keyboard to the appropriate connectors of the Monitoring Collector.
2. When prompted, enter **admin** for the login and **allot** for the password.
3. Enter the following command to set the IP address, network mask and default gateway:

   go config ips –ip <IP ADDRESS>:<NETWORK MASK> -g <DEFAULT GATEWAY>

4. Change the password by entering the following command:

   passwd

5. When prompted, enter a new password, between 5 and 8 characters in length anc press **<enter>.**
6. Enter the new password again when prompted to confirm the change.

To add the new Monitoring Collector to the network:

1. Open NetXplorer.
2. In the Navigation pane, right-click Servers in the Network pane in the Navigation tree and select **New Collector** from the popup menu.

   The Monitoring Collector Properties - New dialog is displayed.

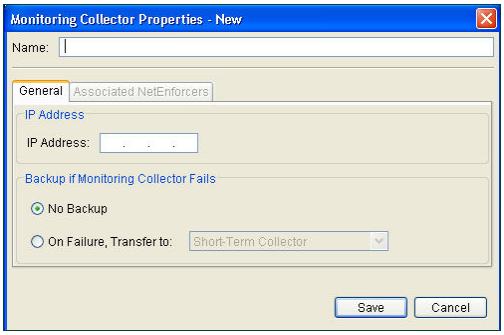

Figure 3-3: Monitoring Collectors Properties dialog – General tab

3. On the General tab, enter the IP address of the Monitoring Collector.
4. Enter a name for the Monitoring Collector.
5. In the Backup if Monitoring Collector Fails area, select one of the two radio buttons, **No Backup** or **On Failure, Transfer To**
6. If you select **On Failure, Transfer To**, select the backup Monitoring Collector from the drop down menu.
7. Click **Save**. The Monitoring Collector is added to the Navigation tree. The New Collector operation can take up to a couple of minutes to complete.

NOTE **There are no NetEnforcers associated with this collector yet, therefore the Associated NetEnforcers tab is disabled.**

8. Repeat this process to add additional Collectors to the network.

To assign NetEnforcers to the new Monitoring Collector:

1. In the Navigation pane, right-click a NetEnforcer in the Navigation tree and select **Properties** from the popup menu.

   The NetEnforcer Properties - Update dialog is displayed.

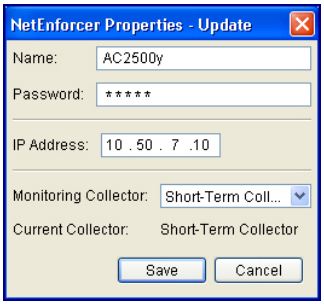

Figure 3-4: NetEnforcer Properties dialog

2. Assign a Monitoring Collector to the NetEnforcer from the drop down menu. This means that the NetEnforcer will transmit its monitoring data to that Collector only. If it does not matter which Collector is used, select **<system defined>.**
3. If there is currently a collector associated with this NetEnforcer, its unique name is displayed. Select a new monitoring collector from the drop down menu.
4. Click **Save.**

To verify that the new collector has been associated with the NetEnforcer, select the collector in the Navigator pane and click Properties. You should see the NetEnforcer in the Associated NetEnforcer tab.

NOTE: You cannot change the association from this dialog, but only from the NetEnforcer properties dialog.

To view the NetEnforcers associated with a Monitoring Collector

1. Right-click the selected collector and choose properties. The Associated NetEnforcers tab is not disabled and you can view a list of all NetEnforcers transmitting monitoring information to this Collector.

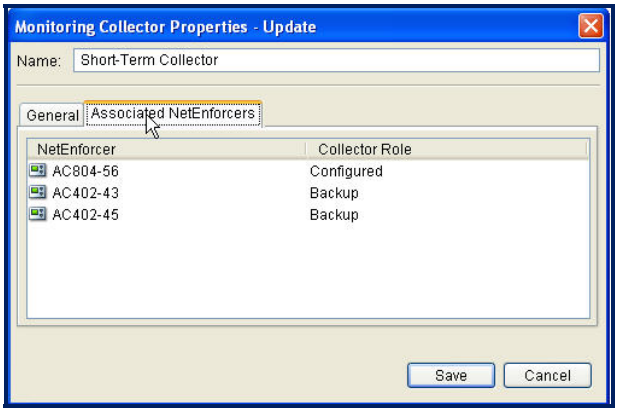

Figure 3-5: Monitoring Collector Properties - Update

To add a Collector Group

Collector Groups are made up of two Collectors, providing 1+1 redundancy for each other.

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

   The Collector Group Properties - New dialog is displayed.

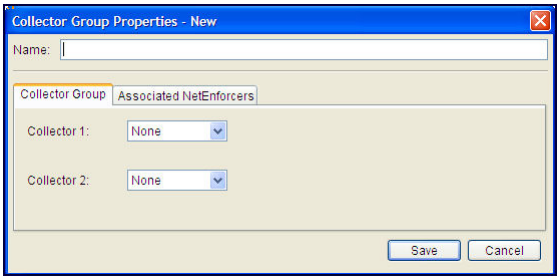

Figure 3-6: Collector Group Properties – New Dialog

2. In the Collector Group tab Select the two Collectors (already part of the network) to be included in the group. Collector 2 will act as the backup for Collector 1.
3. Those NetEnforcer's associated to the added Collectors will be listed in the Associated NetEnforcers tab.
4. Click **Save**. The Collector Group is added to the Navigation tree. The Add Collector Group operation can take up to a couple of minutes to complete.

Configuring Monitoring Collectors

To configure the Monitoring collector, you will use two dialogs. The first is the Configuration dialog and the second is the Properties dialog.

To configure the Collector's Settings - Configuration

1. In the Navigation pane, right-click the Collector and select Configuration

   The configuration window for that collector is displayed.

The dialog shows the following tabs:

- **General** – View the collector's serial number, software version and model

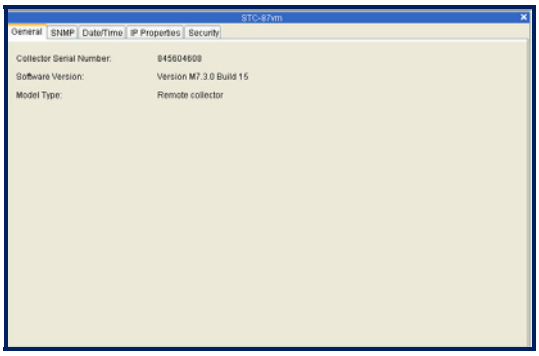

Figure 3-7 Collector Configuration Window - General Tab

- **SNMP** - Add a contact person, location and system name for SNMP purposes

Note: **The Collector, as well as the NetEnforcer supports SNMP (Simple Network Management Protocol) that includes standard MIB II traps.**

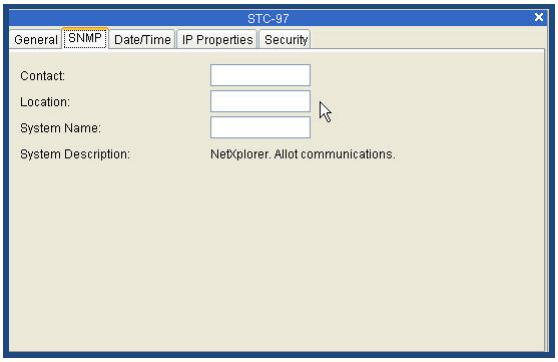

Figure 3-8 SNMP Tab

- **Date/Time** – Configure the time zone according to the geographical location of the collector

NOTE: The NTP server cannot be changed

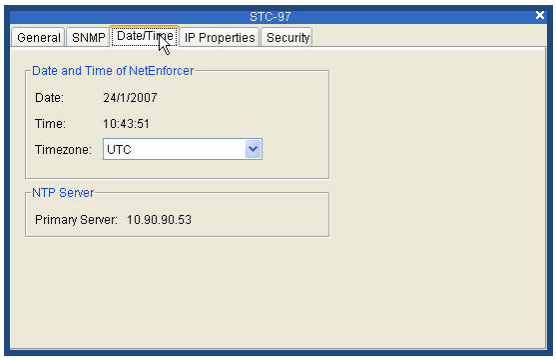

Figure 3-9 Date/Time Tab

- **IP Properties** – Inset the IP Address, Network Mask, Default Gateway, Host Name, Domain Name, Primary Server and the Secondary Server

NOTE: If you change the Collector's IP address, you must make the NetXplorer server aware of this change by changing the IP in the Collector's Properties dialog.

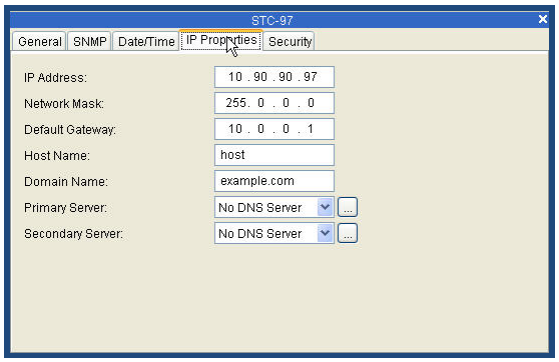

Figure 3-10 IP Properties Tab

- **Security** – Check the appropriate boxes to apply general security attributes. Select the radio button to limit access to specific hosts

NOTE: If you select Unrestricted Access Allowed, any host can access the system.

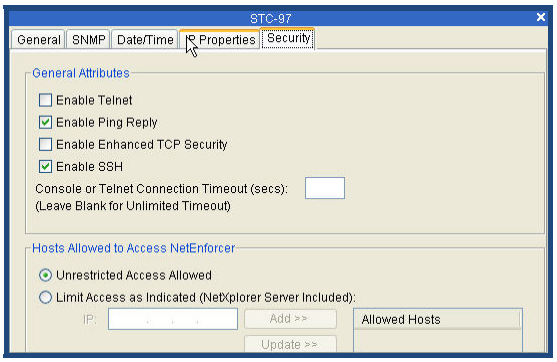

Figure 3-11 Securities Tab

To configure the Collector's Settings - Properties

1. In the Navigation pane, right-click the Collector and select Properties
2. The Monitoring Collectors Properties dialog is displayed.

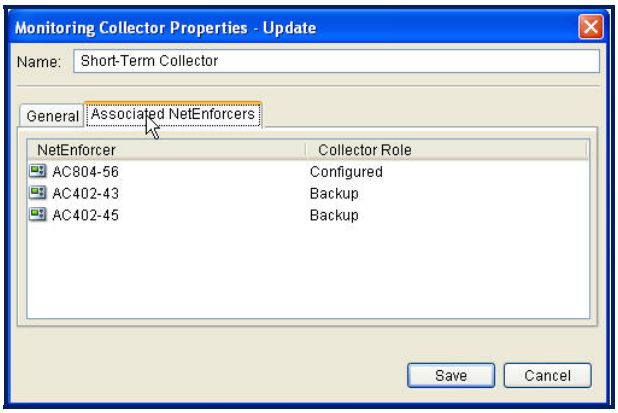

Figure 3-12 Monitoring Collector Properties – Update Dialog

The dialog shows two tabs:

- **General** – Set the name, IP and backup setting of the Collector
- **Associated NetEnforcers** - View the NetEnforcers currently associated with this collector.

NOTE **The Collector Role shows the collectors as configured. It will show a collector as backup only if the configured collector is unavailable and the backup collector is operating instead.**

Command Line Interface

To connect to the collector using an SSH connection

1. Login as user **admin** with the password **allot**.
2. Enter **go config,** with no additional parameters, to view all the available configuration commands
3. Enter **go config** plus parameter to view the available commands for that parameter

- For example, enter **go config ips** to view the available CLI options for ips

Troubleshooting the Collector

To check that all of the collector's processes are running, enter the command **keeperMgr –l**

The processes that should be running include:

- dbserv9
- AllSnmpAgent

The following processes must be running to insure proper data collection

- Converter.exe
- Loader.exe
- Poller.exe

Another useful troubleshooting tool is the log files, which are located in the directory: opt/allot/log.

To take a snapshot of a Collector, run the following script on the Collector:

host:/opt/allot/bin$ create_snapshot_logs.sh

Snapshots can be found in the tmp folder located at :

host:/opt/allot/tmp$

Chapter 4: Database Management

The NetXplorer is a centralized management system, which enables the ongoing collection and consolidation of data from multiple NetEnforcer devices that enable users to produce consolidated reports. The key to a centralized system is the ability to consolidate information from all the managed groups that are being monitored. Because NetXplorer allows for the ongoing collection and consolidation of data from multiple NetEnforcer devices, users are able to produce consolidated reports based the information collected.

In order to manage the collected data, there are three databases:

- **CFG Tables -** Configuration parameters
- **STC Database** – Short term database
- **LTC Tables** – Long term database

Backing Up and Restoring the Database

Backup Terms

- **Full Backup** – A backup process that copies all of the data to a location from which we can create an entire database.
- **Incremental Backup** – A process that preserves only the changes made since the latest backup, either full or incremental, the latest of them.
- **Database Restore** – A process to create a database using the backup copy. Typically, the restore process consists of copying the latest full backup to the restore directory, and then "applying" the incremental backups that were performed after that last full backup.

- **Backup generation** –Backups are kept cyclically as generations. Each generation is a full set of backup files capable of restoring the database to the point in time in which its last iteration was created. Each generation typically consists of one full backup and several incremental backups.
- **Incremental Backup serial number** – Within a certain generation, incremental backups are performed one after another, each one being part of a certain serial number.

Redundancy

The following scenario is one suggestion for using backups to achieve NetXplorer redundancy:

1. Install two NetXplorer servers, one used exclusively as backup.
2. Schedule regular backups for the CFG and STC databases.
3. Perform a manual backup of the LTC database once per day/week/months (depending on the requirements)
4. In the event that the main NetXplorer server fails, assign the same IP to the backup NetXplorer server.
5. Restore the CFG, STC, and LTC database backups to the new NetXplorer.

Backup Types

There are two kinds NetXplorer server.

- **Cold backup** – Performed with the NetXplorer server offline.
- **Hot backup** – Performed without interrupting NetXplorer operation

Cold Backup

To perform a Cold backup:

1. Stop the NetXplorer Service.
    - Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
    - Double-click **Administrative Tools** and open **Services**.
    - Right-click **NetXplorer** in the list of Services and select **Stop** from the drop-down menu.
    - Check the ***allot_ltc.txt, allot_stc.txt*** log files located under Allot Home Directory\Logs in order to verify that NetXplorer services are not running:

      The following lines should appear in both ***allot_ltc.txt, allot_stc.txt*** log files:
      "Disable all events"
      "End of current events"
2. Copy ***Allot Home Directory\data\db*** folder to a backup directory
3. Restart the NetXplorer Service.
    - Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
    - Double-click **Administrative Tools** and open **Services**.
    - Right-click **NetXplorer** in the list of Services and select **Start** from the drop-down menu.

To restore the Cold backup:

1. Stop the NetXplorer Service.

- Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
- Double-click **Administrative Tools** and open **Services**.
- Right-click **NetXplorer** in the list of Services and select **Stop** from the drop-down menu.
- Check the ***allot_ltc.txt, allot_stc.txt*** log files located under Allot Home Directory\Logs in order to verify that NetXplorer services are not running:

  The following lines should appear in both ***allot_ltc.txt, allot_stc.txt*** log files:
  "Disable all events"
  "End of current events"

2. Restore the database by copying the backup to the following folder: ***Allot Home Directory\data\db***.

   If you get a "Confirm Folder Replace" pop-up window, then press "Yes to All".

3. Restart the NetXplorer Service.
   - Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Start** from the drop-down menu.

Hot Backup

Database Types

- **Configuration Tables (CFG)** –Full backup and periodical incremental backups, manually or scheduled. Full backup is performed once a day while the incremental backup is performed every hour. All values are configurable by the user and can be changed according to requirements.
- **Short Term Collector Database (STC)** –Full backups only, manually or scheduled. STC full backup only backs up a set of files that hold the values kept in key tables (such as param) but the actual **traffic data is NOT saved**. The restore process, therefore, recreates a new database from scratch, performs a delete and then loads the key tables mentioned.
- **Long Term Collector table (LTC)** – Full backups only. **This is a manual process only**. This is due to the database's potential size.

Backing up CFG Tables

NOTE The following commands should not cut and pasted into the DOS window, but typed in. They may not function properly unless entered manually.

To perform an incremental hot backup manually:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

db_maint –a backup –n cfg –t incremental

To perform a full hot backup manually:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

db_maint –a backup –n cfg –t full

To check the hot backup parameters:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –sa list

The backup parameters will indicate what scheduled backups are enabled, when they are scheduled, and how many generations will be backed up.

To enable incremental scheduled hot backups:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –t incremental –sa enable

To schedule an incremental hot backup for a specific time:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –t incremental –sa change_sched –ns <TIME>

To set the amount of time between scheduled incremental hot backups:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. Enter the following command:

   db_maint –a backup_status –n cfg –t incremental –sa change_sched –ni <VALUE> –nt <UNIT OF TIME>

For example, to set a period of 2 hours between incremental backups, enter the following command

db_maint –a backup_status –n cfg –t incremental –sa change_sched –ni 2 –nt hours

To schedule a full hot backup for a specific time:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –t full –sa change_sched –ns <TIME>

To set the amount of time between scheduled full hot backups:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –t full –sa change_sched –ni <VALUE> –nt <UNIT OF TIME>

For example, to set a period of 20 hours between full backups, enter the following command

db_maint –a backup_status –n cfg –t full –sa change_sched –ni 20 –nt hours

To change the backup directory:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –sa change_dir –nd <NEW LOCATION PATH>

For example, to change the database directory to cfg1, enter the following command

db_maint –a backup_status –n cfg –sa change_dir –nd D:\backup\cfg1

To change the number of generations:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

db_maint –a backup_status –n cfg –sa change_gen –ng <VALUE>

Restoring CFG Tables

To check the hot backup parameters:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n cfg –sa list

The backup parameters will indicate the generation numbers of the backups.

The increment number must be found in the correct folder under the backup folder (for example: D:\Allot\backup\cfg\5\incremental).

To restore the database:

1. Stop the NetXplorer Service.
   - Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Stop** from the drop-down menu.

- Check the ***allot_ltc.txt, allot_stc.txt*** log files located under Allot Home Directory\Logs in order to verify that NetXplorer services are not running:

  The following lines should appear in both ***allot_ltc.txt, allot_stc.txt*** log files:
  "Disable all events"
  "End of current events"

2. Open a Microsoft DOS window on the NetXplorer Server.
3. Open the Allot\Bin directory (by default D:\Allot\bin).
4. At the prompt enter the following command:

   db_maint –a restore –n cfg –s <D:\Allot\backup\cfg or LOCATION PATH> –g <GENERATION NUMBER> –i <INCREMENT NUMBER> –d <D:\Allot\data\db\cfg or LOCATION PATH> -b <TEMP LOCATION TO KEEP CURRENT CONFIGURATION>

5. Restart the NetXplorer Service.

   - Click **Start** on the Windows Task Bar and select **Settings** > **Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Start** from the drop-down menu.

Backing up STC Databases

To perform a full hot backup manually:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup –n stc –t full

To check the hot backup parameters:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n stc –sa list

The backup parameters will indicate what scheduled backups are enabled, when they are scheduled, and how many generations will be backed up.

To schedule a full hot backup for a specific time:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n stc –t full –sa change_sched –ns <TIME>

To set the amount of time between scheduled full hot backups:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n stc –t full –sa change_sched –ni <VALUE> –nt <UNIT OF TIME>

For example, to set a period of 20 hours between full backups, enter the following command

db_maint –a backup_status –n stc –t full –sa change_sched –ni 20 –nt hours

To change the hot backup directory:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n stc –sa change_dir –nd <NEW LOCATION PATH>

For example, to change the database directory to cfg1, enter the following command

db_maint –a backup_status –n cfg –sa change_dir –nd D:\backup\cfg1

To change the number of generations:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

db_maint –a backup_status –n stc –sa change_gen –ng <VALUE>

Restoring STC Databases

To check the hot backup parameters:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n stc –sa list

The backup parameters will indicate the generation numbers of the backups

To restore the database:

1. Stop the NetXplorer Service.
   - Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Stop** from the drop-down menu.

- Check the ***allot_ltc.txt, allot_stc.txt*** log files located under Allot Home Directory\Logs in order to verify that NetXplorer services are not running:

  The following lines should appear in both ***allot_ltc.txt, allot_stc.txt*** log files:
  "Disable all events"
  "End of current events"

2. Open a Microsoft DOS window on the NetXplorer Server.
3. Open the Allot\Bin directory (by default D:\Allot\bin).
4. At the prompt enter the following command:

   db_maint –a restore –n stc –s <D:\Allot\backup\stc or LOCATION PATH> –g <GENERATION NUMBER> –i 0 –d <D:\Allot\data\db\stc or LOCATION PATH>

5. Restart the NetXplorer Service.

   - Click **Start** on the Windows Task Bar and select **Settings** > **Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Start** from the drop-down menu.

Backing up LTC Tables

To perform a full hot backup manually:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup –n ltc –t full

To check the hot backup parameters:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n ltc –sa list

To change the hot backup directory:

1. Open a Microsoft DOS window on the NetXplorer Server.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n ltc –sa change_dir –nd <NEW LOCATION PATH>

For example, to change the database directory to cfg1, enter the following command

db_maint –a backup_status –n ltc –sa change_dir –nd D:\backup\cfg1

To change the number of generations:

1. Access the NetXplorer via Telnet.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

db_maint –a backup_status –n ltc –sa change_gen –ng <VALUE>

Restoring LTC Tables

To check the hot backup parameters:

1. Access the NetXplorer via Telnet.
2. Open the Allot\Bin directory (by default D:\Allot\bin).
3. At the prompt enter the following command:

   db_maint –a backup_status –n ltc –sa list

The backup parameters will indicate the generation numbers of the backups

To restore the database:

1. Stop the NetXplorer Service.
   - Click **Start** on the Windows Task Bar and select **Settings > Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Stop** from the drop-down menu.

- Check the ***allot_ltc.txt, allot_stc.txt*** log files located under Allot Home Directory\Logs in order to verify that NetXplorer services are not running:

  The following lines should appear in both ***allot_ltc.txt, allot_stc.txt*** log files:
  "Disable all events"
  "End of current events"

2. Open a Microsoft DOS window on the NetXplorer Server.
3. Open the Allot\Bin directory (by default D:\Allot\bin).
4. At the prompt enter the following command:

   db_maint –a restore –n ltc –s <D:\Allot\backup\ltc or LOCATION PATH> –g <GENERATION NUMBER> –d <D:\Allot\data\db\ltc or LOCATION PATH>

5. Restart the NetXplorer Service.

   - Click **Start** on the Windows Task Bar and select **Settings** > **Control Panel**.
   - Double-click **Administrative Tools** and open **Services**.
   - Right-click **NetXplorer** in the list of Services and select **Start** from the drop-down menu.

Chapter 5: Appendices

Troubleshooting

Snapshot of all log files

This will prepare a zip-file that contains log and configuration files from all NetXplorer components (Application Server, Collector, Databases); the last backup of the CFG (configuration allot_cfg) database.

To Use:

Open MSDOS command window (cmd.exe). Run from command-line - **%ALLOT_HOME%\bin\ create_snapshot_logs.bat**.

A message will appear in the command window indicating that the snapshot was taken successfully and its location.

Zip-file - *snapshot_<yyyy_mm_dd_hh_mi>.tar.gz* will be located in %ALLOT_HOME%\tmp directory.

Message Example –

Snapshot zip-file - D:\Allot\tmp\snapshot_2005_10_26_19_09.tar.gz is ready

How to restore CFG (allot_cfg) database from the Snapshot-File

1. Install the appropriate NetXplorer version from <snapshot>\conf\install_log.txt file.
2. From the <snapshot>\conf\dynamic.ini file discover the CFG path.

3. After installation, reboot the computer and stop the NetXplorer service.
4. Restore allot_cfg database using db_maint.exe from %ALLOT_HOME%\bin directory using the following command line operation:

   db_maint -a restore -n cfg -t incremental -s <snapshot>\backup_cfg -g 1 -i <max incr number(1-22)> -d %ALLOT_HOME%\data\db\cfg
5. <max incr number> - max number(1-22) in directory name from <snapshot>\backup_cfg\1\incremental (example: 10)
6. Start the NetXplorer service

The NetXplorer server is now ready to work with snapshot allot_cfg database

Recreate Default Databases

This will recreate empty (default) collectors databases for STC and LTC. It is useful for quick collector databases changes. Data for the Device table will be loaded from the Application Server (CFG database) first time the NetXplorer Server service starts.

This utility removes current database files (according to configuration files (%ALLOT_HOME%\conf) – static.ini and dynamic.ini that were created during installation process) and creates empty database in the same place.

Prior to running the “recreate” command, the NetXplorer Server should be stopped.

1. Open the MSDOS command window (cmd.exe). Run from command-line -

   %ALLOT_HOME%\bin\ recreate_default_db.bat <STC| LTC>.

   Parameter STC – recreate STC database; Parameter LTC – recreate LTC database.
2. As the result of the command execution, the following message will appear in the command window

- Recreate database <STC|LTC> successful or failed.

3. In case of success, the NetXplorer Server will be restarted.
4. In case of failure, the NetXplorer Server needs to be reinstalled.

Pre-allocation of additional disk space for DBspaces- STC and LTC databases

Pre-allocating additional disk space is an important way to ensure better performance. This operation prevents fragmentation of database files and time-consuming disk space allocations.

After installation, there should be, for example, the following allocated disk spaces:

STC database - SYSTEM - 100MB; PRELOAD_DB - 100MB; SEC_STAT_DB - 2GB; MIN_STAT_DB - 2GB; HRS_STAT_DB - 2GB; INDX_RULE_DB - 100MB

LTC database - SYSTEM -100MB; STAT_DB -2GB; HRS_STAT_DB - 2GB

The criteria used to pre-allocated size are the number of devices assigned to STC or LTC and the device type (Enterprise or SP).

Recommended for STC - SYSTEM - 1GB

- PRELOAD_DB - 100MB-400MB per device
- SEC_STAT_DB - 1GB-4GB per device
- MIN_STAT_DB - 2GB-4GB per device
- HRS_STAT_DB - 2GB-6GB per device
- INDX_RULE_DB - 100MB-400MB per device

Recommended for LTC - SYSTEM - 1GB;

- HRS_STAT_DB - 1.3GB-9.2GB per device
- STAT_DB - 1GB-7GB per device

The deployment for Windows:

- In directory %ALLOT_HOME%\bin, db_allocation.vbs; run_db_allocation.bat
- In directory %ALLOT_HOME%\conf, dbspaces_stc.txt; dbspaces_ltc.txt

The deployment for Linux:

- In directory $ALLOT_HOME/bin, post_install_stc.sh
- In directory $ALLOT_HOME/conf, dbspaces_stc.txt

Usage: Edit the dbspace size definition file dbspaces_stc(ltc).txt - set required size for pre-allocation per each dbspace in megabytes (**MB**) or gigabytes (**GB**).

For Windows:

- Open MSDOS command window (cmd.exe).
- Run from the command-line - **%ALLOT_HOME%\bin\ run_db_allocation.bat stc | ltc**

The message, which appears after the command is finished, looks like: See dbspace allocation log in – %ALLOT_HOME%\tmp\install\ db_allocation_stc(ltc).log

After finishing, it is recommended to defragment the disk.

- Use Programs->Accessories-> System Tools->Disk Defragmenter program

For Linux:

- Run - $ALLOT_HOME/bin/ post_install_stc.sh

The messages, which appears while the script runs is:

“alter dbspace ${space_name} add ${space_size}”

Reduction Profile Update

This will change the **reduction.cfg** file for the LTreducer application. The installation copies “enterprise normal profile” file into directory %ALLOT_HOME%\conf enabling the mentioned profile to become active. The file name is reduction.cfg.

All the reduction profile files are located in %ALLOT_HOME%\conf\Reduction directory. This utility will copy active reduction profile file in %ALLOT_HOME%\conf from %ALLOT_HOME%\conf\Reduction directory.

Possible reduction profile types are: ent_normal; ent_accuracy; ent_history; isp_normal; isp_accuracy; isp_history (ent - enterprise; isp – internet service provider).

1. Open MSDOS command window (cmd.exe). Run from the command-line - **%ALLOT_HOME%\bin\ reduction_profile_upd.bat <profile type>**.
2. Profile types - ent_normal; ent_accuracy; ent_history; isp_normal; isp_accuracy; isp_history.

- Example: %ALLOT_HOME%\bin\ reduction_profile_upd.bat isp_accuracy

STC (LTC) Profile Update

This will change data aging parameters in the STC or LTC database PARAM table for second, minute, hour, day and month statistic data and delay between aggregation and truncate tables for ISP model.

1. Open MSDOS command window (cmd.exe). Run from the command-line –

   %ALLOT_HOME%\bin\ stc_profile_upd.bat <'profile type'>

   OR

   %ALLOT_HOME%\bin\ ltc_profile_upd.bat <'profile type'>

Profile types - ent_normal; ent_accuracy; ent_history; isp_normal; isp_accuracy; isp_history.

'NetXplorer Server' service (or STC | LTC database) should be restarted.

- Example: %ALLOT_HOME%\bin\ stc_profile_upd.bat **'**isp_accuracy'

Command Line Interface (CLI)

The CLI enables you to modify the NetEnforcer database from a command line. The CLI supplies a set of commands to add, change, rename and remove NetEnforcer entities, such as, Pipes, Virtual Channels or other Catalog entries and change the configuration of NetEnforcer. You can also use the CLI to set system parameters and device settings.

Scripts

Scripts can contain CLI commands in order to automate the data entry process.

Provisioning CLI

To use the provisioning CLI:

1. Unzip the file \<**VERSION NUMBER**>**RnD****WSCli.zip** on the NetXplorer Software CD to a folder on the computer from which you wish to access the statistics.
2. The newly created folder contains 3 batch files: **topologyCLI.bat**, **policyCLI.bat** and **catalogsCLI.bat**. Each of these files needs to be edited. Open a .bat file using a text editor. Look for the **-Dserver** parameter. It is set by default to the local host, 127.0.0.1. Change the value to the IP Address of the NetXplorer Server you wish to work with.
3. The NetXplorer server must be configured to allow your computer to use its web services. On the NetXplorer server machine go to: <allot home>\netxplorer\jboss-4.0.2\server\allot\conf. Open the file **allowedHosts.properties** with a text editor. Add the IP of the machine the CLI is going to be run on in the following format: **<IP>=<IP>.**
4. Open cmd and go to the folder to which you extracted the files, run the batch files you require and enter CLI commands.

Topology

The Topology CLI syntax is:

topologyCLI <action> <option> <value> [<value>] [<option> <value> [<value>]] …

The following actions are possible:
1. addDevice
2. importDevice
3. deleteDevice
4. help

Add Device

topologyCLI – addDevice

- options:
  - -uiName <value: name>
  - -netAddress <value: ip>
  - -password <value: password>

Import Device

topologyCLI – importDevice

- options:
  - -uiName <value: name>
  - -netAddress <value: ip>
  - -password <value: password>

Delete Device

topologyCLI –deleteDevice

- options:
  - -uiName <value: device name>

Policy

The Policy CLI Syntax is:
policyCLI <action> <option> <value> [<value>] [<option> <value> [<value>]] …

- Actions
  - help
  - addTube
  - addFilter
  - addAlarm
  - listTube
  - listPolicy
  - deleteTube
  - deleteFilter
  - deleteAlarm
  - updateTube

- Options

Argument Name	Option	Remarks
tubeDeviceName	Device Name	Only active devices
tubeType	Tube Type	line, pipe, VC
tubeName	Tube Name	
tubeOffset	Tube Offset (location)	First filter is offset 0
tubeLineName	Tube Line Name	
tubePipeName	Tube Pipe Name	
tubeId	Tube ID	
tubeVcName	Tube VC Name	
tubePolicyId	Policy ID	Currently all options work with active
filterId	Filter ID	
filterDirection	Direction	0-Bi, 1-Int. to Ext.,2- Ext to Int
filterService	Service ID	
filterServiceGroup	Service Group ID	
filterExternalHost	External Host ID	
filterExternalHostGroup	External Host Group ID	
filterInternalHost	Internal Host ID	
filterInternalHostGroup	Internal Host Group ID	
filterTime	Time Catalog ID	
filterTos	Filter Tos ID	
filterVlan	Vlan ID	
actionQos	Qos ID	

Argument Name	Option	Remarks
actionDos	Dos ID	
actionTos	Action Tos ID	
actionAccess	Action Access	
actionId	Action ID	
alarmed	alarm ID	
alarmActionId	alarms' action ID	
alarmAlertId	Alarms' Alert ID	
alarmParams	Alarm Params	

Add Tube

policyCLI - addTube

- Required Arguments:
  - -tubeDeviceName Device Name
  - -tubeType Tube Type (line, pipe, VC)
  - -tubeName Tube Name (unique in its level)
  - -tubeOffset Tube Offset (starting at 0)
  - -tubeLineName required for pipe and VC only
  - -tubePipeName required for VC only
- Optional Arguments (if not specified, defaults apply):
  - All filter options except filterId
  - All action options except actionId
  - All alarm options except alarmed

An example of Add Tube

-addTube -tubeDeviceName 73 -tubeType line -tubeOffset 11 -tubeName newLine

Add Filter

policyCLI - addFilter

- Required Arguments:
  - -tubeDeviceName
  - -tubeType
  - - tubeLineName
  - - tubePipeName - Required for pipe and VC
  - - tubeVcName – Required for VC only
- Optional Arguments:
  - All filter options except filterId

Add Alarm

policyCLI - addAlarm

- Required Arguments:
  - -tubeDeviceName
  - -tubeType
  - - tubeLineName
  - - tubePipeName - Required for pipe and VC
  - - tubeVcName – Required for VC only
  - - alarmActionId
  - - alarmAlertId
- Optional Arguments:
  - alarmParams

List Tube

policyCLI - listTube

- Required Arguments:
  - -tubeDeviceName
  - -tubeType
  - - tubeLineName
  - - tubePipeName - Required for pipe and VC
  - - tubeVcName – Required for VC only

List Policy

policyCLI - listPolicy

- Required Arguments:
  - -deviceId

Delete Tube/Filter/Alarm

PolicyCLI -deleteTube/-deleteFilter/-deleteAlarm

- Required Arguments:
  - -tubeDeviceName
  - -tubeType
  - - tubeLineName
  - - tubePipeName - Required for pipe and VC
  - - tubeVcName – Required for VC only
  - -filterId - For delete Filter only
  - -alarmId - For delete Alarm only

An example of Delete Tube

-deleteTube -tubeType vc -tubeDeviceName 73 -tubeLineName Fallback -tubePipeName Fallback -tubeVcName vv1

Update Tube

policyCLI - updateTube

- Required Arguments:
  - -tubeDeviceName
  - - tubeType
  - - tubeLineName
  - - tubePipeName - Required for pipe and VC
  - - tubeVcName – Required for VC only
  - -filterId – If filter fields were modified
  - -alarmId – if alarm fields were modified
- Optional Arguments:
  - tubeName
  - All filter options
  - All alarm options
- All action options

An example of Update Tube

-updateTube -tubeDeviceName 73 -tubeType vc -tubeLineName newLine -tubePipeName newPipe -tubeVcName newVc -actionTos "Best Effort"

Catalogs

The Catalog CLI Syntax is:
catalogCLI -<action> -<catalog> [<-option> <value>]

- Catalogs

- tos
- dos
- qos
- vlan
- alert
- action
- time
- host
- host group
- service
- service group

- Actions
  - help
  - list_all
  - get
  - add
  - delete
  - update
- Options
- Global

Argument Name	Option	Remarks
name	Catalog name	
access_right	Access right	0-read only 1-provisioned user 2-super user 3-super provisioned user

Argument Name	Option	Remarks
admin	Desirable source status	0-unknown 1-enabled 2-disabled 3–deleted
description	Catalog description	

- Dos

Argument Name	Option	Remarks
max_connections	Connections limitation	
max_CER	Connection establishment rate limitation	
violation_action	Violation action	2 – drop 3 - reject

- Vlan

Argument Name	Option	Remarks
vlan_type	Vlan type	0-Do not ignore 1-Ignore Vlan id 2-Ignore priority bits 3–Ignore Vlan id and priority bits
vlan_tag	Vlan value	

- Tos

Argument Name	Option	Remarks
tos_type		0-Ignore Tos bytes 1-Differentiated services 2-Free format
tos_byte	Tos value	

- Alert

Argument Name	Option	Remarks
alert_type	Event Name	From EVENT_DEF_CORE table
oid	OID of the corresponding MIB counter	From ALERT_COUNTER table
is_alarm	Alert is an alarm	0-not an alarm 1-is an alarm
mode	Alert mode	0-regular 1-applies to every template instance
severity		0-unknown 1-cleared 2-indeterminate 3-critical 4-major 5-minor 6-warning
relation		0-equal 1-greater 2-less 3-not equal
threshold	Bad value	
normal	Normal value	
register	% time in the sample to start the event (start barrier)	
unregister	% time in the sample to stop the event(stop_barrier)	

- Qos

Argument Name	Option	Remarks
qos_type		1-ignore 2-each VC 3-both VC 4-each pipe

Argument Name	Option	Remarks
		5-both pipe 6-half duplex pipe 7-each line 8-both line 9-half duplex line 10-PCMM
qos_action		
direction		0-for both direction 1-for internal (outbound) 2-for external (inbound)
mode		
is_reserved	Minimum reserved bandwidth on use	Only for pipe
min_bw		
max_bw		
min_bw_conn		
max_bw_conn		
mode		0-burst 1- CBR (constant bit rate)
delay		if mode=CBR, then max time in microsecond for the package to be in the system (box)
burst		for all flows of this VC
bw_type	bandwidth type measure	0-absolute value 1- percent from max
priority		

- Action

Argument Name	Option	Remarks
location	Action source	0 –Application server 1-device
action_type	action type	1-script

Argument Name	Option	Remarks
		2-email 3-sms 4-stored procedure
actor	Script, stored procedure name ; e-mail address	

- Host

Argument Name	Option	Remarks
host_type	Host type	0 - regular (entries) 1 - data source (queries) 2 - NE for the compression (entries)
device_id	host device	For common host – device ID is null
add_entry	New host-entries	Syntax: TYPE:value[,…] TYPE values are: Name / ip_address / subnet / range / Mac_address / all_address
remove_entry	Entries to remove	

- Host - Group

Argument Name	Option	Remarks
add_host	Host list that will be added to the host group	Syntax hostname[,…]
remove_host	Host list that will be removed from the host group	

- Service

Argument Name	Option	Remarks
service_type	Service type	0 - secondary service - content definition 1-primary service - ports characteristics
application	An existing application name	Null for all.
add_port		Protocol:port_type:from-port:[to-port] [,…] Protocols {TCP,UDP,IP,NON_IP}. Port types: {SIGNATURE,DEFAULT,PORT_BASED}
remove_port		
parent	Parent service	For service content only.
add_content_item		For service content use. Syntax: content_key:content_value
remove_content_item		

- Service - Group

Argument Name	Option	Remarks
add_service	service list that will be added to the service group	Syntax service-name[,…]
Remove_service	service list that will be removed from the service group	

- Time

Argument Name	Option	Remarks
add_item	Time items that will be added time catalog	Syntax service-TYPE:DAY[:TIME] [,…]

Argument Name	Option	Remarks
Remove_item	Time items that will be removed from the time catatlog	while Type is {DAILY,WEEKLY,MONTHLY,ANUALLY}, DAY is the day number in week/month/year, Time format: hh:mm-hh:mm

List All

catalogCLI –list_all – catalog name

- No required arguments

Get catalog

catalogCLI –get – catalog name

- Required arguments:
  - -name –existing name of the required catalog

Delete catalog

catalogCLI –delete –catalog name

- Required arguments:
  - -name – existing name of the required catalog

Add catalog

catalogCLI –add –catalog name

- Required arguments:
  - –name - existing name of the required catalog
- Arguments:
  - See Options for the specific catalog and global options.

Update catalog

catalogCLI – update –catalog name

- Required arguments:
  - -name – existing catalog name
- Arguments:
  - See Options for the specific catalog and global options.

Examples

-add -vlan –name vlan_name – description “vlan description” –vlan_type 3 -tag 128

-update –vlan –name vlan_name –tag 256

-delete –vlan –name vlan_name

-list_all –vlan

-add -time -name time_name -add_item DAILY:10:00-11:00,WEEKLY:2:10:00-11:00

-update –host –add_item ip_address:1.1.1.1,name:hostname

-update -host_group -name group1 -remove_host host1,host2 -add_host host3

-add -alert -name "new-alert" –alert_type 1 -relation 1 -is_alarm 0 -mode 0 -normal 70 -register 90 -threshold 80 -unregister 50 -sevirity 2 -oid "1.3.6.1.4.1.2603.5.5.5.0"

-add -service -service_type PRIMARY -name service1 -type 1 -application "Citrix ICA" -add_port TCP:PORT_BASED:1000:1000,UDP:DEFAULT:1100:1111

-add -service –service_type CONTENT -name "lilach by CLI" -description "added by CLI" -parent "100BAO" -add_item Direction:Upload

Monitoring CLI

To enable the monitoring CLI:

1. Unzip the file \<**VERSION NUMBER**>**RnD****monitorCLI.zip** on the NetXplorer Software CD to a folder on the computer from which you wish to access the statistics.
2. In the newly created folder, open **monitorCLI.bat** with a text editor and change the value of the parameter **SERVER_URL** to the IP address or domain name of the NetXplorer server.
3. Open a DOS window, run **MonitoringCLI.bat** and enter a command requesting monitoring CLI command. The command is sent to the NetXplorer server. Any monitoring data returned by the NetXplorer server is stored in a .csv file.

The Monitoring CLI Syntax is:

monitorCLI <option> [<value>] [<option> <value> [<value>]] …

-dayDefinitionArray <DayDefinitionList>	Day Definition List in UTC used by Typical (50): [Day(1-sun,2-mon,7-sat,0-all),startHour0,endHour0,startHour1,endHour1,,startHourn,endHourn] [Day,startHour0,endHour0,startHour1,endHour1,startHourn,endHourn]
-allSubjectsInScope	Regular req All Subjects in scope.
-inputFile <file>	Input request file

-help Provides usage and help information.

-longTermRequest Long Term Reporting.

-mostActive Most Active Request.

-relativeTimeUnit <relativeTimeId> Relative Time (default 1) :

[RelativeTimeUnit[Seconds=7],
RelativeTimeUnit[Minutes=6],
RelativeTimeUnit[Hours=1],
RelativeTimeUnit[Days=2],
RelativeTimeUnit[Weeks=3],
RelativeTimeUnit[Months=4],
RelativeTimeUnit[Years=5]]

-typicalType <TypicalTypeId> Request Typical Type :

[TypicalType [Day=1],
TypicalType[Week=2]]

-subject <subjectId> Request Subject (default 0) :

[SubjectType[Enterprise=0],
SubjectType[NetEnforcer=1],
SubjectType[Line=2],
SubjectType[Pipe=3],
SubjectType[Virtual Channel=4],
SubjectType[Host=5],
SubjectType[Internal Host=6],
SubjectType[External Host=7],
SubjectType[Protocol=8],
SubjectType[Conversation=9],
SubjectType[Subscriber=10]]

-time <fromDate/Time toDate/Time> Request Date & Time {dd/MM/yyyy,HH:mm:ss}.

-relativeTimeCount <relativeTimeCount> Relative Time count (default 0) : 1..50.

-allAsOne Regular req All as one.

-sortingCriteria <statisticId> Most Active req Sort Based On (default 1) :

[StatisticType[TotalBandwidth=1],
StatisticType[BandwidthIn=2],
StatisticType[BandwidthOut=3],
StatisticType[LiveConnections=4],
StatisticType[DroppedConnections=6],
StatisticType[NewConnections=5],
StatisticType[PacketsIn=7],
StatisticType[PacketsOut=8],
StatisticType[HostCount=9],
StatisticType[BurstIn1=20],
StatisticType[BurstIn2=21],
StatisticType[BurstIn3=22],
StatisticType[BurstIn4=23],
StatisticType[BurstIn5=24],
StatisticType[BurstOut1=25],
StatisticType[BurstOut2=26],
StatisticType[BurstOut3=27],
StatisticType[BurstOut4=28],
StatisticType[BurstOut5=29]]

-subjectCapacity <capacity> Most Active req Subject capacity (default 5) : 1..50.

-distributor <distributorId> Most Active req Stack result by element:

[DistributorType[NetEnforcer=1],
DistributorType[Line=2],
DistributorType[Pipe=3],
DistributorType[Virtual Channel=4],
DistributorType[Host=5],
DistributorType[Protocol=6],
DistributorType[Subscriber=7]]

-outputFile <file> Output file result

-hostFilerArray <hostFilterList> Host Filter List(50): [hostIp or hostName] ... [hostIp or hostName]

-subjectArray <subjectDefinerList> Regular req Subject Definer List Inluded in Graph(50) :

[NE,Line,Pipe,Vc]
[NE,Line,Pipe,Vc] or [hostIp or hostName]
[hostIp or hostName] or [serviceId]
[serviceId] or [hostIpIn,hostIpOut]
[hostIpIn,hostIpOut]

-scopeLimiterType <ScopeLimiterId> Request Scope Limiter (Most active default 0) :

[ScopeLimiterType[Enterprise=0],
ScopeLimiterType[NetEnforcer=1],
ScopeLimiterType[Line=2],
ScopeLimiterType[Pipe=3],
ScopeLimiterType[Virtual Channel=4]]

-scopeLimiterArray <ScopeLimiterList> Scope Limiter List(50): [NE,Line,Pipe,Vc] ... [NE,Line,Pipe,Vc]

-isAllOthers Most Active req All Others

-splitter <splitterId> Most Active req Display Separately for each element:

[SplitterType[Host=1],
SplitterType[Protocol=2],
SplitterType[Subscriber=7],
SplitterType[NetEnforcer=3],
SplitterType[Line=4],
SplitterType[Pipe=5],
SplitterType[Virtual Channel=6]]

-resolution <resolutionId>	Request Resolution (default 1) : [AggregationResType[Level 0=1], AggregationResType[Level 1=2], AggregationResType[Hour=3], AggregationResType[Day=4], AggregationResType[Month=5]]
-serviceFilerArray <serviceFilterList>	Service Filter List(50): [serviceId] [serviceId]
-adjustTime	Adjust Time

Links Format

[NE,Line,Pipe,Vc] / [NE,Line,Pipe,Vc,Template] /

[NE,Line,Pipe,Vc,InstanceType,instanceValue]:

1) [NE,Line,Pipe,Vc] simple VC = 1,2,3,4 ; simple Line = 1,2,0,0

2) [NE,Line,Pipe,Vc,Template] VC Template = 1,2,3,4,T ; Pipe Template = 1,2,3,0,T

3) [NE,Line,Pipe,Vc,InstanceType,instanceValue] VC Instance = 1,2,3,4,2,9999 ; Pipe Instance = 1,2,3,0,1,9999 [InstanceType[Pipe=1], InstanceType[Virtual Channel=2]]

Examples

5 Most Active NEs on Level0 resolution :

monitorCLI -mostActive -subject 1 -resolution 1 -time 22/11/2005,11:20:00

5 Most Active Hosts on Days resolution scope limited to NE #32 & #37 :

monitorCLI -mostActive -subject 5 -longTermRequest -resolution 4 –time 20/11/2005,00:00:00 23/11/2005,23:59:59 -scopeLimiterType 1 -scopeLimiterArray 32,0,0,0 37,0,0,0

10 Most Active VCs on Level0 resolution scope limited to NE #32 stack result by Protocol

monitorCLI -subjectCapacity 10 -mostActive -subject 4 -resolution 1 -time 22/11/2005,11:20:00 22/11/2005,11:25:00 -scopeLimiterArray 32,0,0,0 -distributor 6

Statistics on NE #37, last 5Min on Level0 resolution :

monitorCLI -subject 1 -resolution 1 -time 22/11/2005,11:20:00 22/11/2005,11:25:00 -subjectArray 37,0,0,0

Pipes Distribution on Network, last 5Min on Level0 resolution :

monitorCLI -subject 3 -resolution 1 -time 22/11/2005,11:20:00 22/11/2005,11:25:00 -scopeLimiterType 0 -scopeLimiterArray 0,0,0,0

Statistics on VC Instance #37,1,1,1,2,42 last 5Min on Level0 resolution :

monitorCLI -subject 4 -resolution 1 -time 22/11/2005,11:20:00 -relativeTimeUnit 2 -subjectArray 37,1,1,1,2,42

Use regular monitor request file & create monitor result file (csv format) :

monitorCLI -inputFile c:\monitor_cli\monitor42060.req -outputFile c:\monitor_cli\monitor42060.csv

Use most active monitor request file & create monitor result file (csv format) :

monitorCLI -inputFile c:\monitor_cli\monitor42061.req -outputFile c:\monitor_cli\monitor42061.csv

Events

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,

All event types available in the NetXplorer are listed in the EVENT_DEF_CORE table in the CFG database.

Currently NetXplorer does not support any automatic action on Alarms/Event. “Send E-mail” action is available only for TCA alarms.

- Rising TCA ("Threshold Crossing Alarm")
- Falling TCA ("Threshold Crossing Alarm")
- Device configuration change in $1R new value is $2V'
- Line Policy Change
- Pipe Policy Change
- Virtual Channel Policy Change
- Catalog Entry Change
- Suspected DoS Attack Started
- Suspected DoS Attack Stopped
- External Data Source Down
- External Data Source Up
- Software Problem (Software problem in $1V, message details: $2V)
- NetEnforcer Access Violation (Access violation has occurred on the NetEnforcer: $1V)
- Link Down ('Link $1V is down: admin status is $2V and operational state is $3V')
- Link Up (Link $1V is up: admin status is $2V and operational state is $3V')

- Cold Start
- Warm Start
- Authentication Failure (Authentication failure. Login attempt to the NetEnforcer failed)
- NetEnforcer IP Address Change (A NetEnforcer IP address property change has occurred for IP $2V')
- Connection routing has changed
- Device Status Down
- Device Status Up
- Collector Down
- Collector Up
- Device Unreachable
- Device Reachable
- User Forced Clear Alarm
- Device Hardware Change (New serial number detected for $1V')
- User Force Cleared All Alarms
- User Logged In (User $1V has logged in to the system)
- User Logged Out (User $1V has logged out of the system)
- High Catalog Counter Detected (High Catalog counter detected on <NE>. Invalid synchronization state')
- Catalog Rejected by NetEnforcer
- Automatic Alarm Purge (Automatic Alarm purge performed by the system. Removed on device $1V')
- Policy and Catalogs Export
- NetEnforcer Configuration Import
- Server Management Ownership Taken from Device (Server management ownership on device $2V was taken from the following NetXplorer Server: $1V')

- Server Management Ownership of Device Taken (Server management ownership of Device $2V was taken by another NetXplorer Server: $1V')
- Missing Events Were not Found on Device Trap Table During Synchronization
- Collector Reported Device Unreachable
- Collector Reported Device Reachable
- Invalid Bucket Time in Collector (Collector $1V reported invalid bucket time on device $2V. Time difference is $3V seconds')
- Valid Bucket Time in Collector (Collector $1V reported that invalid bucket time on device $2V is resolved)
- Invalid Bucket in Collector (Collector $1V reported bucket out-of-sync on device $2V')
- Real Time Bucket Overload in Collector
- Short-term Bucket Overload in Collector
- Bucket Validated in Collector (Collector $1V reported that bucket-out-of-sync condition on device $2V is fixed'
- Invalid Bucket Time in Collector (Collector $1V reported invalid bucket time on device $2V. Time difference is $3V seconds')
- Valid Bucket Time in Collector (Collector $1V reported that invalid bucket time on device $2V is resolved'
- Real Time + Short-term Bucket Overload in Collector
- Bucket Overload in Collector Finished
- Long Term Collector Reported Short Term Collector Unreachable
- Long Term Collector Reported Short Term Collector Reachable

- Invalid Bucket Time in Collector (Long Term Collector $1V reported invalid Short Term bucket time on device $2V. Time difference is $3V seconds)
- Valid Bucket Time in Collector (Long Term Collector $1V reported that invalid Short Term bucket time on device $2V is resolved')
- License expiration warning (Server license is about to expire in $1V days')
- License is expired (Server license of NetXplorer has expired)
- Server license registered
- Clear license expiration warning
- Device policy replaced with rescue policy
- Policy data is not synchronized on device
- Collector Reported Disk Space Problem
- Collector Reported Disk Space Problem Fixed
- Long Term Collector Reported Disk Space Problem
- Long Term Collector Reported Disk Space Problem Fixed
- AS does not support device software version
- Over subscription has occurred
- Device was deleted from system
- Collector was deleted from system
- Catalog action failed
- Configuration Database Incremental Backup failed
- Configuration Database Full Backup failed
- Short Term Collector Reported Database Full Backup failed
- Long Term Collector Reported Database Full Backup failed