Using NATKit 3

This section introduces you to the functions found in the Network Analysis Toolkit drawer in Network Analysis Toolkit (NATKit) 3.

Browser Requirements

Before logging in to NATKit, make sure your web browser is one of the versions listed below:

- Netscape Navigator 4.77, 4.78, and 4.79 (Windows, AIX 4.3.3, HP-UX 11.0)
- Netscape Navigator 4.76 for Solaris 2.6, 2.7 and 2.8

⚠ **Caution** For Solaris, use Netscape Navigator downloaded from the Sun web site only.

- Microsoft Internet Explorer 5.5 with Service Pack 2 and Internet Explorer 6, Java Virtual Machine (JVM) version 5.0.0.3802 for IE 5.5 and version 5.0.0.3805 for IE 6.0 To verify the JVM, select **View > Java Console** from Internet Explorer and **Tools > Server > Java Console** from Netscape Navigator.
- JAVA Plugin 1.3.1

Accessing the Server

When you access the NATKit Server, the NATKit 3 CiscoWorks 2000 screen appears with the Login Manager displayed. To access the server from a client system, enter the URL of the server in your web browser as follows:

- If NATKit 3 has been installed on the server, and if SSL is disabled enter:
  `HTTP://server_name:1741`
- If SSL is enabled, enter:
  `HTTPs://server_name:1742`
- If an alternative port has been configured to access the NATKit server, enter:
  `HTTP://server_name:port_number`

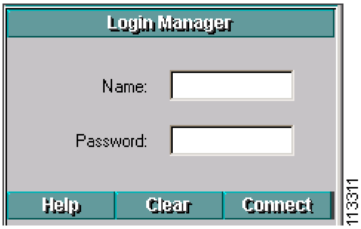
where **`server_name`** is the name of the server on which NATKit 3 has been installed and **`port_number`** is the port number assigned to access the GUI interface of the server.

Logging In

To perform server setup tasks, you must log in as the system administrator by following these steps:

Procedure

Step 1 Enter the administrator username and password in the Login Manager dialog box.



Please contact your Advanced Services engineer if you need GUI access to the NATKit server.

Step 2 Click **Connect**. The Login Manager dialog box is replaced by the navigation tree.

Browser Problems

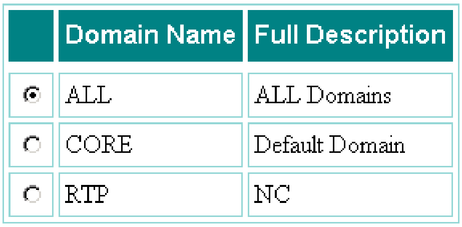
If the desktop buttons do not work, Java and JavaScript are not enabled. Make sure you enable Java and JavaScript.

Make sure the browser cache is not set to zero.

Do not resize the browser window while the desktop main page is loading. This can cause a Java error.

Change Domain

This function allows you to view all (default) devices or just the members of a single domain. This allows you to reduce the number of devices in each view to only members of a single group.



	Domain Name	Full Description
●	ALL	ALL Domains
○	CORE	Default Domain
○	RTP	NC

60443

See Domains for more information on domain set up and use.

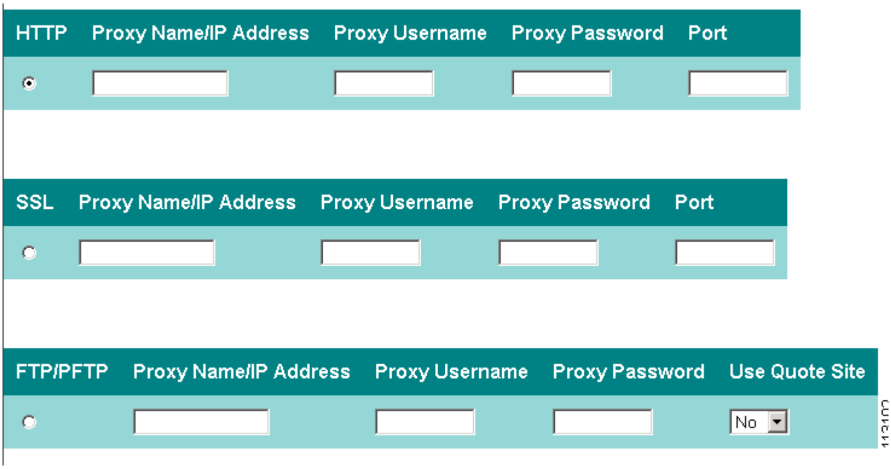
Setup

The following sections describe NATKit setup functions.

Transport

This function allows you to provide access information to a proxy server if NATKit needs to connect to a proxy server in order to do data uploads to natkit-upload.cisco.com via HTTP, SSL, and PFTP/FTP. By default, NATKit uploads data directly to natkit-upload.cisco.com.

NATKit enables SSL download with key-based data transfer. Every NATKit client has a public/private key. Data transfer is initiated only after proper key exchange is achieved with the backend server at Cisco.



HTTP	Proxy Name/IP Address	Proxy Username	Proxy Password	Port
●				

SSL	Proxy Name/IP Address	Proxy Username	Proxy Password	Port
○				

FTP/PFTP	Proxy Name/IP Address	Proxy Username	Proxy Password	Use Quote Site
○				No

Procedure

For HTTP:

Step 1 Select **Network Analysis Toolkit** > **Setup** > **Transport**.

Step 2 Select **HTTP**.

Step 3 Enter the IP Address/hostname in the Proxy Name/IP Address field.

Step 4 Enter a user name in the Proxy Username field.

Step 5 Enter a password in the Proxy Password field.

Step 6 Enter the port which the proxy HTTP server is running on in the Port field.

Step 7 Click **Submit**.

For SSL:

Step 1 Select **Network Analysis Toolkit** > **Setup** > **Transport**.

Step 2 Select **SSL**.

Step 3 Enter the IP Address/hostname in the Proxy Name/IP Address field.

Step 4 Enter a user name in the Proxy Username field.

Step 5 Enter a password in the Proxy Password field.

Step 6 Enter the port on which the proxy HTTP server is running on in the Port field.

Step 7 Click **Submit**.

For FTP/PFTP:

Step 1 Select **Network Analysis Toolkit** > **Setup** > **Transport**.

Step 2 Select **FTP/PFTP**.

Step 3 Enter the IP Address/hostname in the Proxy Name/IP Address field.

Step 4 Enter a user name in the Proxy Username field.

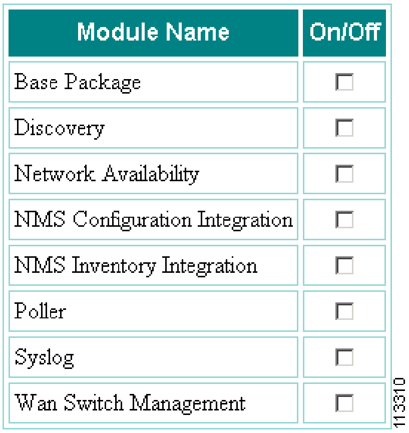
Step 5 Enter a password in the Proxy Password field.

Step 6 Check the **Use Quote Site** box if you are using a proxy server to FTP to the Internet which requires you to do Use Quote.

Step 7 Click **Submit**.

Downloads

This function allows you to specify which modules to include in the daily upload. In NATKit, if the package to upload is greater than the maximum configurable size selected, the download module splits the file into packets (each packet can be up to the maximum configurable size) and then downloads each packet. These packets are reassembled and processed on the backend at Cisco.



Module Name	On/Off
Base Package	□
Discovery	□
Network Availability	□
NMS Configuration Integration	□
NMS Inventory Integration	□
Poller	□
Syslog	□
Wan Switch Management	□

Procedure

Step 1 Select **Network Analysis Toolkit** > **Setup** > **Download.** The Download dialog box is displayed.

Step 2 Click in the check box next to any or all of the following to include them in the daily download:

- Base Package
- Discover
- Network Availability
- NMS Configuration Integration

- NMS Inventory Integration
- Poller
- Syslog
- Wan Switch Management

Step 3 Click **Save**.

Distributed NATKit

If you have multiple NATKit servers residing on your network, a NATKit can be configured to act as a slave and transmit the data to download to another NATKit to send back to Cisco. Slave NATKits use HTTP to transmit the data to download to the master NATKit. The master NATKit downloads the data received by the slave NATKit to Cisco using HTTP, FTP, or PFTP/FTP but not SSL. Please contact your Advanced Services Engineer to learn more about this feature and configure NATKit as a slave.

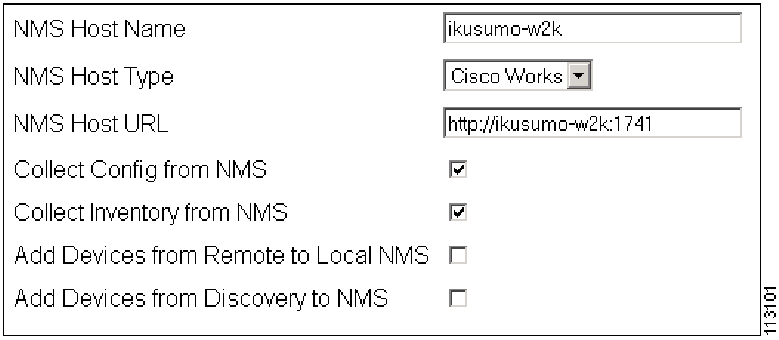
Remote NMS

Remote NMS Integration allows you to slave the NATKit to a remote NMS system. This helps reduce the effort required to keep the NATKit system updated with changes to the devices and device access information.

You can also select to slave NATKit to the remote system for Inventory, Configurations or both. This cuts the traffic to the customer network by NATKit to just about zero. The NATKit administrator can define the NMS for synchronization. Any Remote NMS that needs to be integrated must run a software client that constantly communicates with NATKit. Changes in device attributes and the addition/deletion of devices in NMS are communicated to NATKit immediately.

NATKit initiates a full compare sync operation every few hours to take care of unmanaged devices that don't get published in CiscoWork's Event Distribution System.

Note Currently, this feature is supported on remote NMS systems running RME 3.3, 3.4, and 3.5 on the Solaris and Windows platform. To enable this functionality a separate NATKit remote integration package must be installed as root/admin user on the remote NMS system.



NMS Host Name	ikusumo-w2k
NMS Host Type	Cisco Works ▾
NMS Host URL	http://ikusumo-w2k:1741
Collect Config from NMS	☑
Collect Inventory from NMS	☑
Add Devices from Remote to Local NMS	□
Add Devices from Discovery to NMS	□

Procedure

Step 1 Select **Network Analysis Toolkit > Setup > Remote NMS.** The Setup NMS for Integration dialog box is displayed.

Step 2 Enter a name of an NMS Host in the NMS Host Name field.

Step 3 Select an NMS Host type from the NMS Host Type pull-down menu.

Step 4 Enter the URL of the host NMS in the NMS Host URL field.

Step 5 Click in the **Collect Config from NMS** check box to collect configuration information from NMS.

Step 6 Click in the **Collect Inventory from NMS** check box to collect inventory information from NMS.

Step 7 Click in the **Add Devices from Remote to Local NMS** check box to have NATKit add devices to NATKit's local CiscoWorks. This option initiates separate inventory and configuration polling than that which is already collected from the remote NMS server.

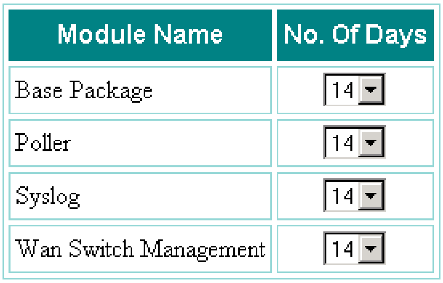
Note If this item is checked, you cannot select option Collect Config from NMS and Collect Inventory from NMS as NATKit's local RME is used to collect the inventory and configurations from the devices and transport them back to Cisco.

Step 8 Click in the **Add Devices from Discovery to NMS** check box to add devices to NMS that have been discovered by NATKit.

Step 9 Click **Save**. The NMS Integration Client software can now be installed on the remote NMS.

Purger

The Purge Data Configuration form allows you to specify the number of days worth of data stored in NATKit each time the data is purged. For example, if the Syslog Module is set to 14 days, all Syslog data stored in NATKit is removed every 24 hours for two weeks *except for the prior 14 days*.



Module Name	No. Of Days
Base Package	14
Poller	14
Syslog	14
Wan Switch Management	14

A purge time can be set for:

- Syslog
- Poller
- Wan switches
- Daily Report
- Download

Domains

A Domain is a group of devices that share a common characteristic or group of characteristics. The administrator of an RME system can keep all devices in a single domain (default) or use the function Create Domain (**Network Analysis Toolkit** > **Setup** > **Domains**) to define the characteristics of the members of a Domain.

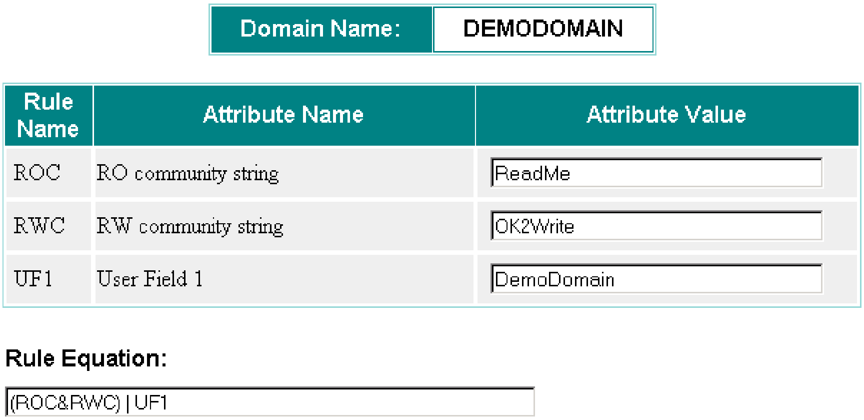
Creating a Domain

This function is used to create new domains. A domain allows you to group devices for viewing purposes.

The characteristics that define a domain can be based on one or more of the following criteria:

- All or part of the device name
- Device Class ID
- sysObjectID
- Any part of the information in the seedfile (user fields, access IDs or passwords/ community strings).

The logical operators at & (and) and | (or). Parentheses can also be used to group items.



Domain Name: DEMODOMAIN

Rule Name	Attribute Name	Attribute Value
ROC	RO community string	ReadMe
RWC	RW community string	OK2Write
UF1	User Field 1	DemoDomain

Rule Equation:

(ROC&RWC) | UF1

60463

In the illustration above, the user has selected three fields (SNMP Read Only, SNMP Read Write community strings and User Field 1) as the characteristics that define members of the domain “DEMODOMAIN”. Note that in the Rule Equation the exact text of the items in the “Rule Name” column have been used along with the logical operators “&”, “|” and the grouping function of the parentheses. Members of the domain DEMODOMAIN are devices with the SNMP R/O community string of “ReadMe” **AND** the SNMP R/W community string set to “OK2Write“**OR** User Field 1* contains the string “DemoDomain”. In other words, any device with DemoDomain in User Field 1 is a member, regardless of the SNMP community strings, and any device whose community strings match the values in the attribute field for SNMP R/O and R/W is a member even if User Field 1 is blank or set to something besides DemoDomain.

Note Domains are tested in the order they are added and once a device meets the criteria for a domain it is not tested for other domains unless you reapply the domain rules. As a result, a device can only be a member of one domain.

*See the RME 3.4 User's Guide for more information about the User Fields of the devices.

Procedure

Step 1 Select **Network Analysis Toolkit > Setup > Domains > Create Domains.** The Create New Domain dialog box is displayed.

Step 2 Type the name of the domain to create in the **Domain Name** field using ALL CAPITALIZED LETTERS. Use only alphanumeric characters and spaces.

Note An error message appears if a name that is used by Resource Manager Essential's View tool is selected.

Step 3 Type the description for the domain in the **Full Description** field. Use only A-Z, a-z, 0-9 and the following characters: _ . ' -

Step 4 Click **Next**.

Step 5 Select a Rule Attribute.

Step 6 Click **Next**.

Step 7 Define the rules for the domain as described in Applying Domain Rules.

Step 8 Click **Save**. Select **Network Analysis Toolkit > Change Domain** to change to the domain just created.

Managing Domains

These functions are used to define what devices are included in a particular domain, or to delete a domain.

Procedures

Modifying a Domain

Step 1 Select **Network Analysis Toolkit > Setup > Domains > Domain Rules.** The View/Modify Domain Details dialog box is displayed.

Step 2 Click in the radio button next to the domain to add devices to or modify.

Step 3 Click **Select Domain Rules**.

Deleting a Domain

Step 1 Select **Network Analysis Toolkit > Setup > Domains > Domain Rules.** The View/Modify Domain Details dialog box is displayed.

Step 2 Click in the radio button next to the domain to delete.

Step 3 Click **Delete Domain**. The domain name is deleted, and the device domain is reset to “core”.

Applying Domain Rules

This screen is used to begin the processing of the attribute rules selected from the Select Domain Rules page and attribute values entered on the Define Rules for Domain page.

All devices are processed against all domains. The first domain that satisfies the equation (entered in the Define Rules for Domain page) is assigned to the device. Devices that do not fit into any domain rule are assigned to a domain labeled “CORE”. Device information for all devices are fetched from the local NMS (CiscoWorks), and a remote NMS if one is used.

Procedure

Step 1 Select **Network Analysis Toolkit > Setup > Domains > Apply Domain Rules**. The Apply Domain Rules dialog box is displayed listing all known domains.

Step 2 Click **Finish** to begin the process.

Step 3 Select **Network Analysis Toolkit > Setup > Domains > Domain Rule Process Status** to check the status of the process.

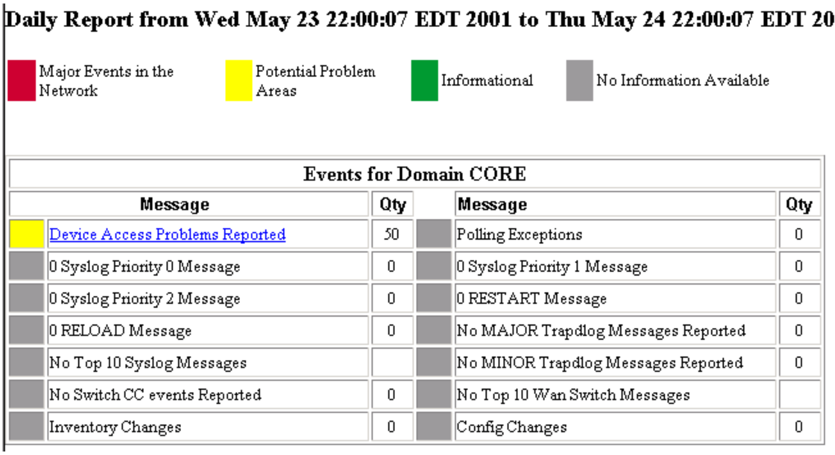
⚠

Caution Be sure that the domain name you choose is not being used by Resource Manager Essential's View tool.

Alerts

Daily Report

The Daily Report is a condensed overview of network activities from the previous day. The Daily Report is automatically produced each morning; no action is required to configure the report. If Domains are created, a Daily Report is created for each domain. Below is an illustration of a Daily Report and a detailed look at reading the report.



Daily Report from Wed May 23 22:00:07 EDT 2001 to Thu May 24 22:00:07 EDT 2001

🟥 Major Events in the Network 🟨 Potential Problem Areas 🟩 Informational ▨ No Information Available

	Events for Domain CORE				
	Message	**Qty**		**Message**	**Qty**
🟨	Device Access Problems Reported	50	▨	Polling Exceptions	0
▨	0 Syslog Priority 0 Message	0	▨	0 Syslog Priority 1 Message	0
▨	0 Syslog Priority 2 Message	0	▨	0 RESTART Message	0
▨	0 RELOAD Message	0	▨	No MAJOR Trapdlog Messages Reported	0
▨	No Top 10 Syslog Messages		▨	No MINOR Trapdlog Messages Reported	0
▨	No Switch CC events Reported	0	▨	No Top 10 Wan Switch Messages	
▨	Inventory Changes	0	▨	Config Changes	0

60425

Reading the Daily Report

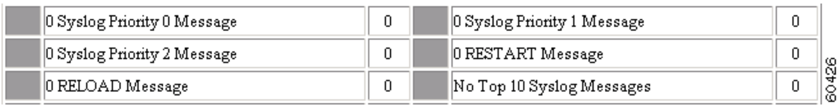
The Daily Report is broken down into sections to simplify understanding the report. Each section of the Daily Report forms a hyperlink to more detail if data in that category has been recorded during the period covered. Click on the hyperlink to read more detailed information about the event.

Procedure

- Select **Network Analysis Toolkit >Alerts >24 Hour Report**.

Syslog Messages

This section consists of six classes of syslog messages. The first three are based on the priority of the messages; levels 0, 1, and 2. The next class is based on a simple message count; the 10 most frequently recorded messages are listed. Finally, messages indicating that a device has been forced to reload or restart are listed.



▨	0 Syslog Priority 0 Message	0	▨	0 Syslog Priority 1 Message	0
▨	0 Syslog Priority 2 Message	0	▨	0 RESTART Message	0
▨	0 RELOAD Message	0	▨	No Top 10 Syslog Messages	0

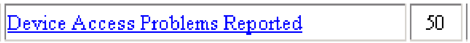
Config Changes

This section covers changes to device configuration. If changes are detected during the period covered, the number of changes is listed and a link to more detailed information is activated. If you select the link, a list of devices that recorded a change is shown. The device name becomes a link to the actual change, the current running configuration, the previous running configuration and a configuration history for that device.

Config Changes	0

Device Access Problems Reported

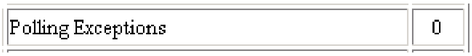
This section focuses on the report from the Device Access Verifier. This tool checks access to each device each night and reports failures recorded. If any of the tests (ping, SNMP R/O and Telnet/SSH) fail, the link becomes active and leads to a report listing the failures, such as: “Failed, reason: Password in login mode is wrong”.



Device Access Problems Reported	50

Polling Exceptions

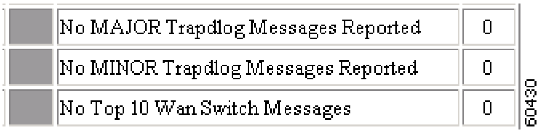
This is a report of exceptions to SNMP poller tasks. This becomes active if a poller task’s threshold is violated. This link leads to a page showing the task recording the violation and the information (if any) collected by the commands selected.



Polling Exceptions	0

Wan Switch Trapd Log Messages

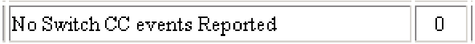
The three Wan Switch Trapd Log messages report on major, minor and the 10 most frequent messages during the period covered by the report.



■	No MAJOR Trapdlog Messages Reported	0
■	No MINOR Trapdlog Messages Reported	0
■	No Top 10 Wan Switch Messages	0

Switch CC Events Reported

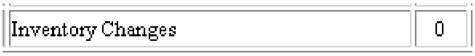
Switch CC Events occur in stratacom devices when the active devices and standby ASC cards are switched. These events are recorded in the trapd log file which NATKit reads periodically and lists here.



No Switch CC events Reported	0

Inventory Changes

Changes recorded for any device in the inventory during the period covered by the report are listed here. If active this link leads to a list of devices recording changes, a list of the changes and the device inventory.



Inventory Changes	0

History

Daily reports that have been completed successfully in the past are available for viewing from the GUI interface. You can click on a particular daily report to view the report in detail.

Procedure

- Select **Network Analysis Toolkit >Alerts >24 Hour Report >History**.

Device Manager

Launch Pad

The Launch Pad provides a way to view device information for a device that has been collected and stored in NATKit. The Launch Pad also provides a way to view multiple data types that have been scheduled for collection.

Once a device type and device have been chosen, the Device Center for that device appears and displays the following information about it:

- **Device Aliases**- Lists all aliases (including IP addresses) that exist for the selected device
- **Device Login Info**- The login info screen is unique to Launch Pad. The information displayed on this screen is collected from the data entered using inventory data. It provides the following information:
  - Domain Name of the specified device
  - Login password
  - Enable password
  - Enable secret
  - TacAcs User
  - TacAcs password
  - Session password
  - Telnet port
  - Read Community String
  - Write Community String

Note Login Info is only available to trusted users.

- **Config Summary Report** - Lists the devices selected and provides the option of viewing the startup, running, or most recently archived configurations, as well as the differences among those configurations.

- **Config Version Report** - Contains the following details of the selected configurations:
  - A link to view the configuration
  - The configuration version number
  - The time the configuration was created
  - What change was made (Change Description)
- **Config Quickview Report** - Lists the devices, configuration version numbers, and configuration details of the device configuration version specified.
- **Telnet -** Launches Telnet client and connects to the specified device.
- **Detail Inventory -** Provides detailed information about NATKit and system the selected device is located on.
- **Daily Syslog -** Shows the syslog events and any correlation data collected by the Syslog profile**.**
- **View Trapd Log -** Shows the contents of the trapd.log file of HP Open View for WAN Switching nodes.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Manager > Launchpad**. The Launchpad dialog box appears displaying the following columns:

Field	Description
Device Type	List of searchable device types.
Devices	List of devices found in the selected device types.

Step 2 Click on a device category from the **Device Type** column. A list of devices found appears in the **Devices** column.

Step 3 Click on a specific device from the **Devices** column.

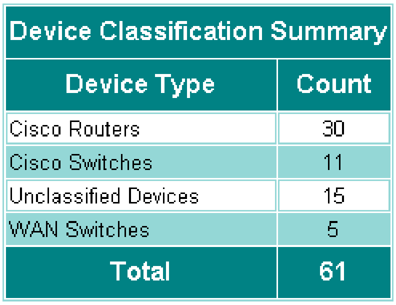
Step 4 Click **Finish**. The Device Center for the chosen device is displayed.

View Current Devices

NATKit only collects data on network devices that have been added to the NATKit database, either by the file method, individually via the GUI or by Device Discovery. The Device Identification Manager (DIM) is used to specify or display those devices. The NATKit Device View screen shows what devices NATKit has in its database, along with additional information such as system object identification and a brief description of the device and its type.

In addition, a summary of all Cisco routers, switches and unclassified devices found are displayed. The Device Name, SysObject ID, Description, and Device Type are listed for each device found.

The Device Name and Device Type of any WAN switch detected is also listed.



Device Classification Summary

Device Type	Count
Cisco Routers	30
Cisco Switches	11
Unclassified Devices	15
WAN Switches	5
Total	61

60441

Procedure

- Select **Network Analysis Toolkit** **Device Manager** **View Current Devices** to display a list of all devices detected by NATKit.

View Access Verifier

NATKit uses the Device Access Verifier tool to determine whether some or all devices are accessible via Telnet, SSH, SNMP and/or Ping at a designated time. This tool provides a way to view the results of a previously scheduled device verification task.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Manager > View Access Verifier.** The Device Access Verifier dialog box is displayed.

Step 2 Select a device (or All) from the Device Type pull-down menu.

Step 3 Select Telnet, Ping, SNMP or All from the Access Method pull-down menu.

Step 4 Chose when to start and stop the Access Verifier, or leave the timer as-is to do an immediate verification.

Step 5 Click **View** to schedule the verification. If an immediate verification was scheduled, the Access Verification Results screen lists the results when the verification process is complete. Each column on the Results screen can be sorted by clicking on **Device Name, Access Method, Time,** or **Access Result.**

Note If a device fails an access verification task, the reason is displayed in Access Result column. Select **Network Analysis Toolkit > Device Manager > Administration > Schedule Access Verification.** Select the device that failed and click on Modify Device Attributes to make changes to the device.

Device Name Mapping

Device Name Mapping (DNM) aliases are used as a quick and easy way to identify and remember devices. Use the Device Name Mappings tool to list the DNM aliases for a particular device.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Manager > Device Name Mappings.** The DNM Aliases dialog box is displayed.

Step 2 Select a device type (or All Devices) from the Device Type window. All devices detected by NATKit for that device type is displayed in the Devices window.

Step 3 Select a device from the Devices window. Use the **Shift** or **CTRL** keys to select more than one device.

Step 4 Click **Finish**. DNM aliases found for any device selected are displayed.

Set Access Methods

The Set Access Methods screen is used to select the preferred method of access (Telnet, SNMP, Ping, or SSH) for a particular device.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Manager** > **Administration** > **Set Access Methods.** The Set Access Methods dialog box is displayed.

Step 2 Select a device type (or All Devices) from the Device Type window. All devices detected by NATKit for that device type is displayed in the Devices window.

Step 3 Select a device from the Devices window. Use the **Shift** or **CTRL** keys to select more than one device.

Step 4 Click **Finish**.

Step 5 Click in the check box under each access method (Telnet, SNMP, Ping) desired for a particular device. If Telnet is selected, SSH access verification is also enabled.

Step 6 Click **Save**.

Classify Devices

NATKit can support devices that are not supported by RME. The Classify Devices feature attempts to classify devices not supported by RME.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Manager** > **Administration** > **Classify Devices.** The Classify Devices dialog box is displayed.

Step 2 Select an unsupported RME device from the Generic SNMP Devices window. Use the **Shift** or **CTRL** keys to select more than one device.

Step 3 Click > to move the selected devices into the Selected Devices window.

Step 4 Select which category to classify the device as from the Assign Class Type pull-down menu.

Step 5 Click **Save**.

Caution NATKit does not support 100% of the devices not supported by RME. It does, however, attempt to classify all that it can.

Set Device Login Type

Class types for classified devices can be reassigned for login (Telnet and SSH) purposes only.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Manager** > **Administration** > **Set Device Login Type.** The Set Device Login Type dialog box is displayed.

Step 2 Select the device(s) to change from the Devices window. Use the **Shift** or **CTRL** keys to select more than one device.

Step 3 Click > to move the selected devices into the Selected Devices window.

Step 4 Select the login type to assign each device from the Assign Login Class Type pull-down menu.

Step 5 Click **Save**.

Note To change a device back to its original login class, move the desired device to the Selected Device window and click **Reset Default**.

Caution It is not possible to assign individual login class types to each device listed in the Selected Devices window. All devices listed in the Selected Devices window is assigned the same login class type chosen from the Assign Login Class Type pull-down menu.

Schedule Access Verification

NATKit uses the Device Access Verifier tool to determine whether some or all devices are accessible via Telnet, SSH, SNMP and Ping at a designated time.

Note If you disabled access verification for Telnet, SSH, SNMP, and/or Ping using the Set Access Methods tool, device access verification on those devices for that particular method does not occur.

The Schedule Access Verification tool is used to schedule a device access verification task for one or more devices. Results of the verification can be viewed using the Device Access Verification.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Manager > Administration > Schedule Access Verification.** The Access Verifier dialog box is displayed listing all devices found along with the results of any previous verification attempts (Pass/Failed/Not Verified).

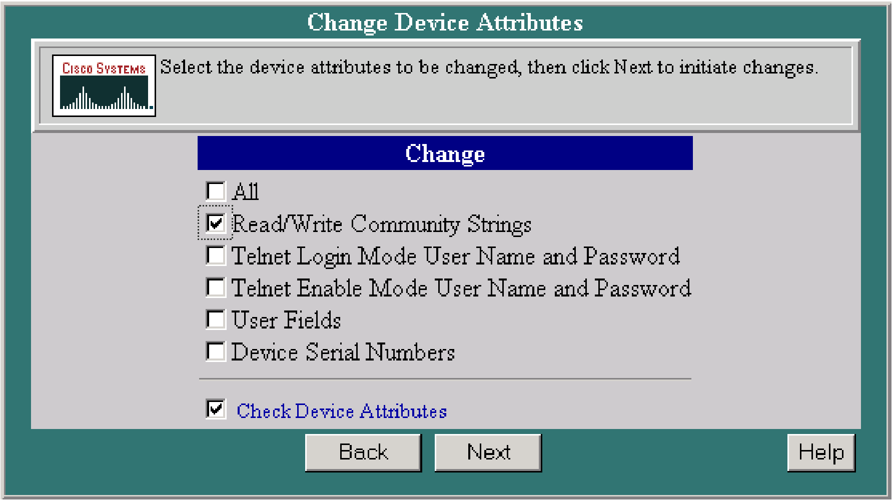
Step 2 Select a device from the Device Name window. Use the **Shift** or **CTRL** keys to select more than one device, or click on **Select All** to select all devices listed in the Device Name window.

Note To select only the devices that have failed previous verification attempts, click on **Select Failed Devices**.

Step 3 Click **Start**. A confirmation screen is displayed along with a Task ID number. The verification request is then sent to the scheduler.

Note To check the status of a verification request, select **Network Analysis Toolkit > Task Manager > View Scheduled Tasks**. Locate the Task ID number of the desired task in the Task # column.

Step 4 To change the passwords, community strings or users IDs for a device Highlight the device or devices and select the Modify Device Attributes option at the lower left. A list of options allows you to select the attributes to change.



Change Device Attributes

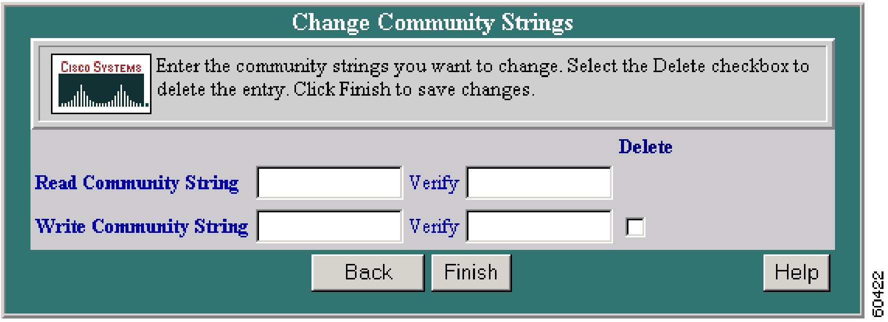
Select the device attributes to be changed, then click Next to initiate changes.

Change

- ☐ All
- ☑ Read/Write Community Strings
- ☐ Telnet Login Mode User Name and Password
- ☐ Telnet Enable Mode User Name and Password
- ☐ User Fields
- ☐ Device Serial Numbers

☑ Check Device Attributes

After selecting **Next,** a screen appears to select new values for the attributes selected. In the illustration below the Read/Write Community Strings option was selected.



Change Community Strings

Enter the community strings you want to change. Select the Delete checkbox to delete the entry. Click Finish to save changes.

				Delete
Read Community String		Verify		
Write Community String		Verify		☐

After making the change return to Step 1 to re-test.

Set Device Domain

This function allows you to force a device into a domain regardless of the rules for that domain.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Manager > Administration > Set Device Domain.** The Select Domain for Device(s) dialog box is displayed.

Step 2 Click in the radio button next to the desired domain.

Step 3 Click **Next**.

Step 4 Click on a device type from the Device Type column to reveal available devices.

Step 5 Select one or more devices from the Devices window. Use the **Shift** or **CTRL** keys to select more than one device.

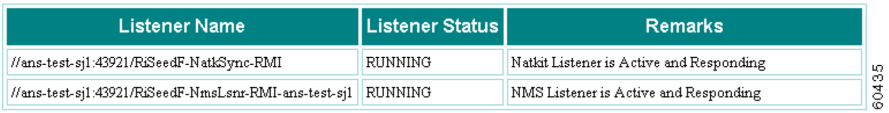
Step 6 Click **Set Domain**.

NMS Server Status

This screen displays the status of all servers required to process seedfile synching. A Local NMS Listener runs on the local machine and listens to the CiscoWorks EDS bus for events on device changes. A Remote NMS Listener is displayed only if Remote NMS is configured. It operates similar to the Local NMS but runs on a remote machine.

NatkSyncServer runs on a local machine and listens for device changes reported by both the Local NMS Listener and any Remote NMS Listener that has been configured.

Once all jobs are running, run the Manual Seedfile Sync to sync up devices.



Listener Name	Listener Status	Remarks
//ans-test-sj1:43921/RiSeedF-NatkSync-RMI	RUNNING	Natkit Listener is Active and Responding
//ans-test-sj1:43921/RiSeedF-NmsLsnr-RMI-ans-test-sj1	RUNNING	NMS Listener is Active and Responding

Manual Seed Files Sync

This tool is used to schedule a task that imports the seedfile from the local CiscoWorks machine or a remote NMS Host into NATKit.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Manager** > **Administration** > **Seed File Integration** > **Manual Seed File Sync.** The Select NMS to Synchronize Seed File dialog box is displayed.

Step 2 Select Local Cisco Works or Remote “NMS Host” (where “NMS Host” is the name of the NMS Host) to import its seedfile into NATKit.

Step 3 Click **Synchronize Seed File**. A task to import the seedfile from the selected source is sent to the scheduler.

Seed File Sync Exceptions

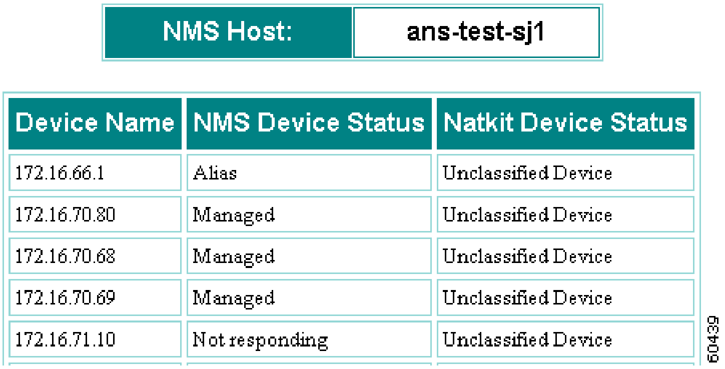
This tool compares the devices in the NMS seedfile to NATKit's device information for inconsistencies. If NATKit isn’t reporting devices known to exist, this tool compares the NMS seedfile to the device information currently in NATKit and report why. More often than not a device is reported as unclassified. Use NATKit's Classify Devices tool to classify them.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Manager** > **Administration** > **Seed File Integration** > **Seed File Sync Exception.** The Select NMS to View Exceptions dialog box is displayed.

Step 2 Select the desired NMS Host from the **NMS Host** pull-down menu.

Step 3 Click **View Exception**. The Seed File Integration Exception Status screen appears listing any inconsistencies.



NMS Host:	ans-test-sj1

Device Name	NMS Device Status	Natkit Device Status
172.16.66.1	Alias	Unclassified Device
172.16.70.80	Managed	Unclassified Device
172.16.70.68	Managed	Unclassified Device
172.16.70.69	Managed	Unclassified Device
172.16.71.10	Not responding	Unclassified Device

Device Discovery

This tool allows you to discover Cisco devices that are accessible via SNMP from NATKit. The discovery consists of a two stage process where you schedule the actual discovery of Cisco devices and then initiates a seedfile to be created by the discovery process.

Discovery View/Administration

This tool displays information about all devices detected by NATKit, and allows for administration and report generation.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 The Device Discovery dialog box displays the status of current (or last) discovery processing, including discovery trending, the discovery method(s), and devices found.

- **Start Time** - The time the last discovery was started. The time is based on the time zone of the server running discovery.

- **End Time** - The time the last discovery ended, or blank if it is currently running. The time is based on the time zone of the server running discovery.

- **Current Status** - Status message indicating whether discovery is currently running or not.

- **Trending** - Displays information on the progress of the discovery process. The table is updated periodically based on the selected refresh frequency rate. You can choose a refresh frequency rate (1 minute, 2 minutes, 10 minutes) by clicking the appropriate button under the table. The table below describes each of the columns:

Field	Description
Time Stamp	Time the discovery information was updated. This may not be the same as the refresh frequency. The time is based on the time zone of the server running discovery.
Managed	Number of devices found that used the configured SNMP read-only string or other configured credential.
Unmanaged	Number of devices found that could not be accessed by any of the configured credentials. This includes all Cisco and non-Cisco devices discovered, but that could not be accessed.
Ping Success	Number of devices that were successfully pinged.
SNMP Success	Number of devices that were successfully accessed by SNMP.

Field	**Description**
CDP	Number of devices found by the CDP discovery method.
Ping	Number of devices found by the Ping discovery method.
Pingsweep	Number of devices found by the Ping Sweep discovery method.
OSPF	Number of devices found by the OSPF discovery method.
BGP	Number of devices found by the BGP discovery method.
ARP	Number of devices found by the ARP discovery method.
Clue IP Address Discovered	Number of Clue IP Addresses discovered that need to be processed.
Completed Clue IP Address	Number of Clue IP Addresses that have been fully processed.
Hop Running	The current hop count.

- **Discovery Method** - Displays information on the methods being used by the current or last discovery process. The table below describes each of the columns:

Field	**Description**
Hop Start Time	Time the hop was started.
Method Name	Discovery method used.
Seed Address	Start IP Address used to discover clues for this method.
Hop/Netmask	The hop count for CDP or netmask used for Ping Sweep.
Status	Indicates whether it is running or completed.

- **Devices Found** - Displays a page where you can view a list of all the devices found during discovery.
- **Export** - Downloads the output from the Trending section to an Excel spreadsheet (xls).

View Discovery Administration

This page allows you to set up and manage your discovery settings, manage profiles, and use the Discovery Wizard.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 Click the **Administration** tab. The Administration page appears.

Defining the Device Discovery Method Using the Wizard

You can use the Wizard to define the Device Discovery method for you. To use the Wizard:

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 Click the **Administration** tab. The Administration page appears.

Step 3 Click **Start/Restart Wizard**.

Step 4 Follow the instructions that appear on the screen to configure your Device Discovery method.

Working with Profiles

After using the Wizard to define the Discovery process, you are given the option to save your information as a profile.

- To save your Profile, click the **Save Profile** button. Give your Profile a name, and click **OK**.
- To load a previously saved Profile, click on the **Load Profile** button.
- To delete selected saved Profiles, click on the **Delete Profiles** button. Select the Profiles you want to delete and click **OK**.

Defining the Device Discovery Method Manually

Use this option to specify the device discovery method for your network. One or more of the following can be selected, with one exception. **CDP** and **CDP, Routing Protocol and ARP** cannot be selected at the same time.

Method	Description
Cisco Discovery Protocol (CDP)	Discovers only CDP-enabled Cisco devices. This method takes the least time to complete and is most useful in networks made up entirely of Cisco devices. Products acquired by Cisco do not support CDP. CDP is found in IOS 10.0 and later, and is not supported by WAN switches. Devices running CDP periodically send out CDP hello messages that are picked up by other CDP-enabled devices and formulate a table of connected devices.
CDP and Routing Table	In addition to CDP-enabled devices, this option also discovers Routing Protocol Cisco devices in your network.

Method	Description
Cisco Discovery Protocol (CDP), Routing Protocol, and ARP	In addition to CDP-enabled devices, this option also discovers Routing Protocol and Address Resolution Protocol (ARP) Cisco devices in your network. ARP allows a host to dynamically discover the MAC-layer address corresponding to a particular IP network layer address.
OSPF	Discovers Cisco devices using the Open Shortest Path First (OSPF) method.
BGP	Discovers Cisco devices using the Border Gateway Protocol (BGP) method.
Ping Sweep Starting IP Address	Discovers all SNMP-enabled Cisco devices in your network. This method takes the longest time to complete but is the most comprehensive. Using this method, device discovery finds all devices connected to the device whose IP address is given. The process is repeated recursively until all devices are reached.
Ping Sweep IP Address Range	Discovers a specific range of SNMP-enabled Cisco devices in your network. This method takes more time to complete than the CDP method but less time than the Pingsweep Starting IP Address method. This method is useful if you know the unique IP subnets in the network. Using this method, device discovery finds all the devices within a range of user-supplied IP addresses. It also provides the ability to find unique IP address ranges from a single device and perform device discovery using the address ranges.
SNMP Communities	Discovery uses community strings to determine whether or not a device supports SNMP. For each community string entered, discovery waits for the SNMP timeout to determine if the device supports that community.

Before Beginning

To include only certain IP address ranges for the device discovery, please refer to the section Include Filters.

To exclude certain IP address ranges from the device discovery, please refer to the section Exclude Filters.

After Selecting the Method

After selecting the method, a second screen appears asking you to provide more information. For CDP and Ping Sweep Starting IP Address, you are asked to provide one or more starting points (IP addresses) and hop counts. The Device discovery starts from the IP addresses selected, discovers devices using the IP address supplied, and stop when all devices within the selected hop count have been discovered.

When the Ping Sweep IP Address Range option is selected, you are asked to provide one or more IP addresses and subnet masks. The discovery program pings all legal addresses (excluding the addresses in the Exclude Filters, within the subnet for each address.

Caveats

Device Discovery discovers only Cisco devices. While non-Cisco devices may be discovered by the ping-based methods, an SNMP request (using the SNMP R/O strings supplied by the user for the sysObjectID) is sent to each device after discovery. If the device fails to respond or the response doesn't include certain fields identifying Cisco equipment, the device is declared unmanaged and not included in further discovery or the seed-file produced by device discovery.

CDP is a Cisco propriety protocol; the user of the router may also disable CDP. Because of this, the NATKit Device Discovery user selecting the CDP option must be certain no Cisco equipment is “behind” (from the NATKit systems point of view) non-Cisco equipment or Cisco devices with CDP disabled. In cases where Cisco devices are behind non-CDP devices, you must provide at least one IP address for each network region behind (from the NATKit systems point of view) these links.

CDP is not completely supported over some wide area links (such as ATM) even on Cisco devices. To ensure successful discovery of all Cisco devices you must provide at least one IP address for each network region behind)these links.

Discovery of any type places a load on the network being tested. It is the your responsibility to use the setting in Advanced Settings and the scheduler function (see Schedule Polling for more information) to minimize the impact of discovery.

Exclude Filters

Use this option to define filters for excluding devices from device discovery. Devices discovered with IP addresses in the Exclude Filters list are not added to inventory.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Exclude Filters**. The Exclude Filters dialog box displays the following fields:

Field	Description
IP Address(es)	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Address(es) window.
Remove Address(es)	Lists deleted IP addresses. To return a deleted entry to the IP Address(es) window, select it, then click **Re-Add**.
Address	Enter a new IP address.
Netmask	Enter a new Netmask.

Step 2 Click **Add** to apply the filter. The new entry appears in the IP Addresses window.

Step 3 Click **Submit** to save your changes.

Include Filters

Use this option to define filters to include devices in device discovery. The discovery process attempts to locate additional devices that are reachable via these devices.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration > Administration > Include Filters**. The Include Filters dialog box displays the following fields:

Field	Description
IP Address(es)	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Address(es) window.
Remove Address(es)	Lists deleted IP addresses. To return a deleted entry to the IP Adress(es) window, select it, then click **Re-Add**.
Add IP Address	Enter a new IP address.
Netmask	Enter a new Netmask

Step 2 Click **Add** to apply the filter. The new entry appears in the IP Addresses window.

Step 3 Click **Submit** to save your changes.

TacAcs Logins

Use this option to set the TacAcs Logins.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration >Administration > TacAcs Logins**. The TacAcs Logins dialog box displays the following fields:

Field	Description
Logins	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Logins window.
Remove Logins	Lists deleted TacAcs Logins. To return a deleted entry to the Logins window, select it, then click **Re-Add**.
Login	Enter a new TacAcs Login.

Step 2 Click **Add**. The new entry is added to the Logins window.

Step 3 Click **Submit** to save your changes.

TacAcs Passwords

Use this option to set the TacAcs passwords.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration > Administration > TacAcs Passwords**. The TacAcs password dialog box displays the following fields:

Field	Description
Passwords	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Passwords window.
Remove Password	Lists deleted TacAcs Passwords. To return a deleted entry to the Passwords Listed, select it, then click **Re-Add**.
Password	Enter a new TacAcs Password.

Step 2 Click **Add**. The new entry is added to the Passwords window.

Step 3 Click **Submit** to save your changes.

Telnet Passwords

Use this option to set the Telnet passwords.

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Discovery View/Administration** > **Administration** > **Telnet Passwords**. The Telnet password dialog box displays the following fields:

Field	Description
Passwords	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Passwords window.
Remove Password	Lists deleted Telnet passwords. To return a deleted entry to the Passwords window, select it, then click **Re-Add**.
Add Password	Enter a new Telnet password.

Step 2 Click **Add**. The new entry is added to the Passwords window.

Step 3 Click **Submit** to save your changes.

Enable Telnet Passwords

These options allow you to set the Telnet passwords you want to enable.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Enable Telnet Passwords**. The Enable Telnet Passwords dialog box displays the following fields:

Field	Description
Passwords	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Passwords window.
Remove Password	Lists deleted Telnet passwords. To return a deleted entry to the Passwords window, select it, then click **Re-Add**.
Add Password	Enter a new Telnet password.

Step 2 Click **Add**. The new entry is added to the Passwords window.

Step 3 Click **Submit** to save your changes.

TacAcs Login Prompts

These options allow you to set the TacAcs login prompts.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **TacAcs Login Prompts**. The TacAcs Login Prompts dialog box displays the following fields:

Field	Description
Prompts	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Prompts window.
Remove Prompts	Lists deleted TacAcs login prompts. To return a deleted entry to the Prompts window, select it, then click **Re-Add**.
Add	Enter a new TacAcs login prompt.

Step 2 Click **Add**. The new entry is added to the Prompts window.

Step 3 Click **Submit** to save your changes.

TacAcs Password Prompts

These options allow you to set the TacAcs password prompts.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Device View/Administration > Administration > TacAcs Password Prompts**. The TacAcs Passwords Prompts dialog box displays the following fields:

Field	Description
Prompts	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Prompts window.
Remove Prompts	Lists deleted TacAcs password prompts. To return a deleted entry to the Prompts window, select it, then click **Re-Add**.
Add	Enter a new TacAcs password prompt.

Step 2 Click **Add**. The new entry is added to the Prompts window.

Step 3 Click Submit to save your changes.

Telnet Login Prompts

These options allow you to set the Telnet login prompts.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Telnet Login Prompts**. The Telnet Login Prompts dialog box displays the following fields:

Field	Description
Prompts	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Prompts window.
Remove Prompts	Lists deleted Telnet login prompts. To return a deleted entry to the Prompts window, select it, then click **Re-Add**.
Add	Enter a new Telnet login prompt.

Step 2 Click **Add**. The new entry is added to the Prompts window.

Step 3 Click Submit to save your changes.

Telnet Prompts

These options allow you to set the Telnet prompts. Upon user exec level login to a device, one of the following defined Telnet Prompts shown is expected. Please add additional Telnet prompts as needed.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Telnet Prompts**. The Telnet Prompts dialog box displays the following fields:

Field	Description
Prompts	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Prompts window.
Remove Prompts	Lists deleted Telnet prompts. To return a deleted entry to the Prompts window, select it, then click **Re-Add**.
Add	Enter a new Telnet prompt.

Step 2 Click **Add**. The new entry is added to the Prompts window.

Step 3 Click Submit to save your changes.

Enable Telnet Login Prompts

These options allow you to set the Telnet login prompts you want to enable.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Enable Telnet Login Prompts**. The Telnet Login Prompts dialog box displays the following fields:

Field	Description
Prompts	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Prompts window.
Remove Prompts	Lists deleted Telnet login prompts. To return a deleted entry to the Prompts window, select it, then click **Re-Add**.
Add	Enter a new Telnet login prompt.

Step 2 Click **Add**. The new entry is added to the Prompts window.

Step 3 Click **Submit** to save your changes.

Enable Telnet Prompts

These options allow you to set the Enable Telnet Prompts you want to enable. Upon privileged level login to a device, one of the following defined Enable Telnet Prompts shown is expected. Please add additional Telnet prompts as needed.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Enable Telnet Prompts**. The Telnet Prompts dialog box displays the following fields:

Field	Description
Prompts	Lists the current settings. To delete an entry, select it, then click **Delete**. The entry is moved to the Remove Prompts window.

Field	Description
Remove Prompts	Lists deleted Telnet prompts. To return a deleted entry to the Prompts window, select it, then click **Re-Add**.
Add	Enter a new Telnet prompt.

Step 2 Click **Add**. The new entry is added to the Prompts window.

Step 3 Click **Submit** to save your changes.

Clear All Visits

This tool clears all selected options.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Discovery View/Administration** > **Administration** > **Clear All Visits**.

Step 2 All visits to optional features are removed.

Remove All Devices

This tool deletes all devices from the discovery database and removes all data in the Summary Report. Information remains in the NATKit database for all discovered devices if you specified to Export Device List on Discovery Completion under Export Settings.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Device View/Administration** > **Administration** > **Remove Devices**. The Remove All Devices window appears.

Step 2 Click **OK**. All devices in the discovery database are removed.

Start/Stop Discovery

Use this option to start or stop the device discovery immediately or to schedule it to start at a predefined time. If more than one person starts, stops, or schedules device discovery at the same time, the system accepts only one request for device discovery, and sends an error message to the other.

Note It is not be possible to schedule a job using **at** if the causer username does not have permission to do so.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Discovery View/Administration** > **Administration** > **Start Discovery**. The Start Discovery dialog box displays the following fields:

Field	Description
Discovery Method	Displays the current setting for the discovery method.
Exclude Filters	Displays the current settings for the device IP addresses to exclude from device discovery.
Include Exclude Filters	Displays the current settings for the device IP addresses to include in device discovery.
Max Bandwidth (per sec.)	The maximum total amount of bandwidth available in the network. The default is 10 Mbits/sec.
SNMP Retry	The number of times to query a device that does not respond. The default is 1.
SNMP Timeout (msec.)	The amount of time before a query to a device times out. The default is 5000 milliseconds.
Max Percent Bandwidth	The maximum percentage of the total network bandwidth to be used for device discovery. The default is 10%.

Field	Description
Ping Retry	The number of times to ping a device that does not respond. The default is 1.
Ping Timeout (msec.)	The amount of time before a ping to a device times out. The default is 1000 milliseconds.

Step 2 To begin discovery immediately, click **Start Discovery**. The Discovery Status dialog box displays the current status of device discovery.

Step 3 To schedule discovery to begin at a later time, click **Schedule Discovery**. The Discovery Job Scheduler dialog box displays the following fields:

Field	Description
Current Server Date-Time	Displays the current date and time on the server.
Start Server Date-Time	Displays the time to start the discovery process.
Set Defaults	Zeros out the time fields and sets 1 for the frequency and the total number of jobs.
View All Jobs	Displays the start date and time for each job.

Step 4 Enter the appropriate scheduling information and click **OK**.

Start Credentials

Discovery Credentials can be run after running a completed Discovery process. Running Discovery Credentials creates a seedfile named **`seedfile.txt`** from the discovered devices. Set the start time to zero days, zero hours and zero minutes to start the process immediately. Otherwise, set the start time relative to the current server time. The seedfile is be located in the ***`/opt/CSCOpx/objects/CSCOad/nsa/natkit/data/`*** of the web server installation root.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration > Administration > Discover Credentials**. The Discovery Credentials dialog box displays the following fields:

Field	Description
TacAcs Logins	Lists all of the TacAcs logins added using the TacAcs Login tool
TacAcs Passwords	Lists all of the TacAcs passwords added using the TacAcs Password tool
Telnet Passwords	Lists all of the Telnet passwords added using the Telnet Password tool
Enable Passwords	Lists all of the Telnet enable passwords added using the Enable Password tool
ReadWrite Community	Lists all of the Read/Write Communities added using the ReadWrite Community tool
Server Date-Time	Displays the current date and time of the server.
Start Date-Time	Specify the day and time from now to start discovery phase two.
Start From	Specify the date from which to start.
SaveConfig	Saves the current configuration parameters

Step 2 Click **Start Credentials** when done. You can click on **Stop** once the collector begins running to cancel.

View Summary Report

Summary report shows all the devices in the Discovery database. Click on the Device count to get the device list and export the data.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/ Administration.**

Step 2 Click the Reports tab.

Step 3 Click **Summary Report**.

The Summary Report displays all the devices in the Discovery database based on discovery method and device family. The top table contains a count of the devices found by each discovery method in addition to the count of managed and unmanaged devices. The bottom table contains the count of managed devices by device family. You can click on the link beside each type in this table to obtain additional information about these devices.

View Delta Report

Delta report shows the devices found in the current and previous run along with new devices added and missing devices from the previous run.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration**

Step 2 Click the Reports tab.

Step 3 **Click Delta Report**.

The Delta Report displays all devices found in the previous discovery run, the current run, and any new devices added or devices missing since the previous run.

- **Export** - Click the Export button to download the list of devices in this report to an Excel spreadsheet (xls).

View Last Completed Run Report

Last Completed Run report shows the devices from the last discovery run.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 Click the Reports tab.

Step 3 Click **Last Completed Run Report**.

This screen displays the list of devices found during the last completed run of discovery and includes the method that was used to find them and other additional collected information.

- **Device Family** - To view the discovered devices, start by clicking on a product family of device in the Device Family box. The IP addresses for all the devices in that family are shown in the Device List window.
- **Device Lis**t - Click on a device from the Device List box to display information about that device in the Device Description box.
- **Device Description** - The Device Description box displays the following information:
  - Method - Discovery method used to find the device.
  - Name - Name of the device as specified by its sysName.
  - Community - SNMP read-only community for device.
  - Type - Device type.
  - Object ID - SNMP sysObjectID of device.
  - IP List - List of IP addresses associated with device.
- **Export** - Click the Export button to download the list of devices to an Excel spreadsheet (xls).

View Debug Log Report

The Debug Log reports displays the Debug Log Viewer.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 Click the Reports tab.

Step 3 Click **Debug Log**.

The Debug Log contains debug messages that support engineers and developers can use to troubleshoot issues during discovery. Enter a search string and/or select any additional filter criteria and click the Retrieve button to view the results in the browser, or use the Export button to export to Excel (xls).

The Debug Log viewer displays the following fields:

Field	Description
Debug Type	Pertains to the function that generated the message.
Debug Level	Verbosity level of the messages.
Search String	String to match against the debug message.
Lines	Use to select how many lines of debug text to view on the page. Chose from 100, 200, 300, 500, 750, 1,000, 2.500, 5,000, or All.

View Alert Log Report

The Alert Log report displays alert information generated during discovery. This includes any issues discovering the layer3 topology.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 Click the Reports tab.

Step 3 Click **Alert Log**.

The Alert Log log contains messages that indicate reasons why certain devices were not discovered. This log is used for troubleshooting problems with discovery not finding all expected devices. Enter a search string and/or select any additional filter criteria and click the Retrieve button to view the results in the browser, or use the Export button to export to Excel (xls).

The Alert Log viewer displays the following fields:

Field	Description
Alert Type	Pertains to the function that generated the message.
Alert Level	Severity level of the messages.
Search String	String to match against the alert message.
Lines	Use to select how many lines of alert text to view on the page. Chose from 100, 200, 300, 500, 750, 1,000, 2.500, 5,000, or All.

Below are some potentially severe error messages that may get generated, indicating a problem during the Discovery process:

Error - DiscoveryAlert: SNMPNotSupported: Seed ip nn.nn.nn.nn does not support SNMP.

Meaning - Seed device could not be reached via SNMP.

Error - DiscoveryAlert: SNMPNotSupported: Seed ip nn.nn.nn.nn does not support CDP.

Meaning - Seed device could not be reached via CDP.

Error - DiscoveryAlert: CDPSNMPNotSupported: Default router(s) does not support SNMP/CDP.

Meaning: Default device could not be reached by either SNMP or CDP.

View Error Log Report

The Error Log report displays errors generated while discovering devices.

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration.**

Step 2 Click the Reports tab.

Step 3 Click **Error Log**.

The Error Log contains error messages pertaining to exceptions that were caught during discovery. If there are lot of error messages that may indicate there was a significant problem during the discovery processing. Enter a search string and/or select any additional filter criteria and click the Retrieve button to view the results in the browser, or use the Export button to export to Excel (xls).

The Error Log viewer displays the following fields:

Field	Description
Error Type	Pertains to the function that generated the message.
Error Level	Severity level of the messages.
Search String	String to match against the error message.
Lines	Use to select how many lines of error text to view on the page. Chose from 100, 200, 300, 500, 750, 1,000, 2.500, 5,000, or All.

Below are some potentially severe error messages that may get generated, indicating a problem during the Discovery process:

Error - DiscMgrService: callCallback got exception.

Meaning - Discovery not able to return the status of a process.

Error - DiscMgrService: runSeedFileCreation got exception.

Meaning: An exception was generated while creating the seedfile.

Error - DiscMgrService:stopSeedFileCreation got exception.

Meaning - When stopping seedfile creation got exception.

Error - DiscMgrService:startDiscovery --got exception detail message.

Meaning - Discovery was not able to start.

VisioDB Creation

This tool generates a VisioDB file that can be opened in Visio 2000 where a network topology diagram can then be generated.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Device Discovery** > **Discovery View/Administration**

Step 2 Click the Reports tab.

Step 3 Click **Create VisioDB**.

Step 4 Click **Create the File**. The file **`visiodevs.vss`** is created and stored in the **`/opt/CSCOpx/objects/CSCOad/`** directory.

Step 5 Download the Visio Shapes.

Step 6 Download the Visio CSV file you require.

Step 7 Place the shapes file and the Visio CSV files in the same directory.

Step 8 Open and modify the first five lines where it refers to shapes.vss to the full path of the saved location of shapes.vss.

Step 9 Start the Visio application.

Step 10 From the menu in Visio Select **File** > **Open**.

Step 11 Browse to the directory of the downloaded files.

Step 12 Select the **`shapes.vss`** file.

Step 13 From the menu in Visio Select **File** > **Open**.

Step 14 Select the file you downloaded. Select “,” as the separator (default).

Step 15 Visio imports and lays out the file.

Find Device

The Find Device tool allows you to find a device based on its IP address, hostname, or a regular expression (XXX.*.*.* or *.*.*.XXX).

Procedure

Step 1 Select **Network Analysis Toolkit > Device Discovery > Discovery View/Administration**

Step 2 Click the Reports tab.

Step 3 Click **Find Device**.

Step 4 Enter the IP address, hostname, or a regular expression (XXX.*.*.* or *.*.*.XXX) to find the device.

Syslog

Viewing Syslog Events

The Syslog Scheduler creates and edits Syslog profiles. The Syslog Viewer allows you to view the syslog events and any correlation data collected by Syslog profiles. You can choose to view a subset of the collected syslog events by using the timer to specify the time interval of syslog manager.

There are four ways to sort syslog events:

- View Per Device
- View Per Error Type
- View Per Severity Level
- View Exception

The syslog events displayed are all the events collected by all the Syslog profiles previously created.

Note Syslog supports long terse messages up to 800 characters.

Procedure

Step 1 Select **Network Analysis Toolkit > Syslog > View Syslog.**

Step 2 Select a sorting option by clicking on the button next to the desired event.

- View Per Device
- View Per Error Type
- View Per Severity Level
- View Exception

Caution If View Exception is selected, there must be devices in the NATKit database (with correct password information) or an error message appears once Step 2 is completed.

Step 3 Select the Syslog Pattern. This option allows you to filter the syslog messages with a pattern. You can use the asterisk (*) as a wildcard.

Step 4 Use the **Hour**, **Min**, **Day**, **Mth** and **Year** pull-down menus to select the period of time to view.

Step 5 Click **Submit**.

Step 6 One of four screens appears, depending on the sorting option selected in Step 1. Click on a **Device Name**, (Error) **Message Type**, or **Severity** from the respective screen to view a detailed listing of the event.

Scheduling Syslog

This screen is used to create or edit a Syslog Filter task. Up to five screens comprise Syslog Filter task creation:

- **Initial Syslog Editor Filter screen** - Specify whether a Filter task is being created or edited.
- **Filter Task Creation screen** - used for:
  - Naming the task
  - Specifying a syslog daemon logfile and spooling frequency
  - Choosing a correlation type
- **Filter Task Editing screen** - Used to add or delete filter correlation settings to a Syslog Filter task.
- **Task Confirmation screen**- Used to confirm Syslog Filter tasks with default correlation or no correlation attributes before submitting the task to the Scheduler.
- **Custom Correlation screen** - Used to create syslog message patterns and specify actions to be executed when a syslog message matching the pattern is received. See Data Collection under SNMP Poller for more information on specifying actions.

Procedure

Step 1 Select **Network Analysis Toolkit > Syslog > Administration >Schedule Syslog**

Step 2 To create a new Syslog Filter task, choose **Create New Filter Specifications** and click **Next**.

Step 3 To edit a previously created Syslog Filter task, choose **Change Filter Specifications of a Scheduled Process** and click **Next**.

Note The syslog file must be present on the NATKit workstation. This must be done via a mount, either simple NFS or via SCP. The NATKit system cannot be used as a syslog server.

SNMP Poller

The SNMP Poller creates polling profiles to collect variable data and optionally perform correlation on the specific devices included in the profile. View Data by Profiles provides a view of the data collected by the SNMP Poller profiles.

View Polled Values

Displays the data collected by a specific SNMP Poller profile. The Select Profile screen allows you to choose a profile to view. View a “slice” of the data collected by the profile by setting the timer's start and end times to some portion of the profile's scheduled collection time.

Procedure

Step 1 Use the pull-down list to select a profile name.

Step 2 Set the timer to the time period the profile polled its devices.

Step 3 Click **Submit** to view the profile.

⚠ **Caution** When setting the timer, be sure it corresponds to the date and time a profile is polling. Check the Scheduler to see the Start Time, End Time, and the interval settings for the profile.

Schedule Polling

The SNMP Poller tool creates polling profiles to filter all of the devices in your network. A polling profile issues SNMP commands to collect device variable data for the devices and variables specified. The simplest SNMP Poller profile polls the specified devices and collects the variable values.

The SNMP Poller allows you to create a polling profile that can be run at a pre-determined time of day for a specific length of time.

Procedure

Step 1 Select **Network Analysis Toolkit > SNMP Poller > Administration > Schedule Polling.** The SNMP Polling Device Search dialog box displays the following fields:

Field	Description
Device Type	Select the device type from the pull-down menu. All types are selected by default.
Device Search String	Enter a search string for a specific device using the following suggestions: • The search string can include multiple patterns separated by spaces, for example: 171* nsa*. • The Search field recognizes exclusive ORs. This example searches for all devices 171* OR nsa*
Select Predefined MIB File(s)	Select a pre-defined MIB (Management Information Base) file from the pull-down menu.

Note Both a Device Type and Predefined MIB File need to be selected in order to proceed. An error message appears if either or neither is selected.

Step 2 Click **Submit**.

Caution The search routine uses an exclusive OR. If more than one search string is entered, each separated by a space, NATKit displays a list of devices found matching the last recognized string.

SNMP Poller: Correlation

This screen becomes available when changing the variable thresholds of a task from the SNMP Poller: Device and MIB Selection screen. The following can be done on this screen:

- Change the thresholds of any variable included in an SNMP Poller profile
- Set correlation options including:
  - Device data collection and analysis commands
  - Correlation Output specification

Device Variable Thresholds

Device variable thresholds are used to establish trigger points for the SNMP Poller to collect exceptions statistics.

A Poller profile polls the specified variables of the selected devices and, if a threshold is exceeded, collects and saves the information requested in NATKit. If you accept the default variable thresholds or create your own thresholds, then, in addition to data collection, your profile also posts exceptions to those thresholds in the Daily Report.

Correlation Setting

Change a selected variable's threshold without performing a correlation, or issue CLI commands to gather additional data about the devices that have returned an exception. This additional data can be sent to an external program, such as a spreadsheet program, for further analysis.

Correlation Rate Limit

When a variable's threshold has been exceeded, it is reported as an exception. While it is every exception should be reported, you may not want the correlation settings to run each time an exception occurs. Using the rate limit default setting specifies that correlation should be run no more than twice for every exception occurring within a one minute period.

The rate limit setting and the periodic timer setting are closely related. For the rate limit to work as a limiting restraint, its period must be greater than that of the periodic timer.

Data Collection

When a threshold violation has occurred, you may want to collect config data for that particular device. By checking **Collect Device Configuration**, the appropriate commands are issued as part of the correlation data collection.

There are four CLI command lines in the Cisco Device Data Gathering Commands section. In addition to config data collection, each command field can be used to specify one CLI command, such as **sh proc CPU**.

The **Output** field next to each command line allows you to specify where to put the incoming data from the CLI command. The output of all four commands can be sent to the same datastream or individual datastreams. The output is viewed using View Data By Profiles whether one or more datastreams are used. The only reason for using separate output datastreams is when sending the output to another external program for further analysis.

The Iterations and Time Interval fields allows you to specify how many times each CLI command should be run. The default is to run each CLI command twice with an interval of ten seconds between command issuance.

Data Analysis

Once device data has been collected by specifying certain CLI commands to be run, the data can be fed to external programs for further analysis. In addition, you can request that an email or pager notification be sent upon completion of the custom correlation.

Note A special pager notification mechanism with command line interface is required to use the pager feature.

There are four commands lines in the Analysis Command Section. The command lines can be used to invoke any program available from within the NATKit server. Each command line has an associated **Input** and **Output** field. The Input list corresponds to the datastream output created when running a CLI command. Use the appropriate output data from a CLI command as input when invoking an external command.

Correlation Output

The output of the commands specified in Data Collection or Data Analysis are stored in their respective Data 1 through Data 4, or Analysis 1 through Analysis 4 boxes. If any of the items in the Correlation output boxes are checked, those buttons are saved so that they can be viewed.

An email address can be entered if you want to be notified if/when polling exceeds specified thresholds.

Procedures

Correlation Setting

Step 1 Click in the **Do Not Correlate Event** radio button to change a selected variable's threshold without performing a correlation.

Step 2 Select **Correlate Event** to issue CLI commands to gather additional data about the devices that have returned an exception.

Correlation Rate Limit

Step 1 Select how many times the correlation should be run for every exception from the **Events** pull-down menu.

Step 2 Select the exception frequency rate from the **Every** pull-down menu.

Threshold Settings

Step 1 Select one of the following comparison values from the **Comp(s)** pull-down menu:

- **GT** = greater than
- **LT** = less than
- **NE** = not equal

Step 2 Enter a variable's threshold by entering a new threshold value in the **Thresh(s)** field.

Data Collection

Step 1 Check the box for **Collect Device Configuration** to collect this data when running an SNMP Poller profile.

Step 2 Enter a CLI command using the standard syntax in a **Command** field. For example, **sh proc CPU**.

Step 3 Choose an output datastream path from the **Output** pull-down menu adjacent to the command field. For example, **dat_out1**.

Step 4 Set the number of times the command should be run by selecting a value in the **Iterations** pull-down menu.

Step 5 Set the amount of time to wait between issuances of the command using the **Time Interval** pull-down menu.

Data Analysis

Step 1 Enter the full path to the external program in a **Command** field. For example, **`c:\programs\spreadsheet.exe`**.

Step 2 Specify the datastream used to capture the system command data from the **Input** pull-down menu. For example, to set **sh proc CPU** in a command field and the output to **`dat_out1`**, specify the input datastream to **`dat_out1`**.

Step 3 Choose a datastream from the **Output** pull-down menu to designate where to put the result of an external analysis.

Correlation Output

Step 1 Click in the desired Data 1 - 4 boxes to save the output specified in Data Collection.

Step 2 Click in the desired Analysis 1 - 4 box to save the output specified in Data Analysis.

Step 3 Enter an email address in the **Email Notifications** field to be notified when polling exceeds specified thresholds.

Step 4 Click **Submit**.

⚠ **Caution** Make sure the **Correlate Event** radio button is checked to run the user-defined custom correlation settings.

Make sure that the **Collect Device Configuration** box is checked to perform Data Collection.

When running custom correlation, make sure a valid threshold value for each variable is included in each profile.

View Scheduled Tasks

Select **Network Analysis Toolkit > SNMP Poller > Administration > View Scheduled Tasks** to view all tasks scheduled using the Schedule Polling tool.

Change Task Status

The Change Task Status tool allows you to run, suspend, or delete a task scheduled using the SNMP Poller scheduler.

Procedure

Step 1 Select **Network Analysis Toolkit > SNMP Poller > Administration > Change Task Status**. The Change SNMP Task Status dialog box is displayed.

Step 2 Select a task from the Select Task Name pull-down menu. Note that the status of the task appears next to the Task name.

Step 3 Select one of the following three options:

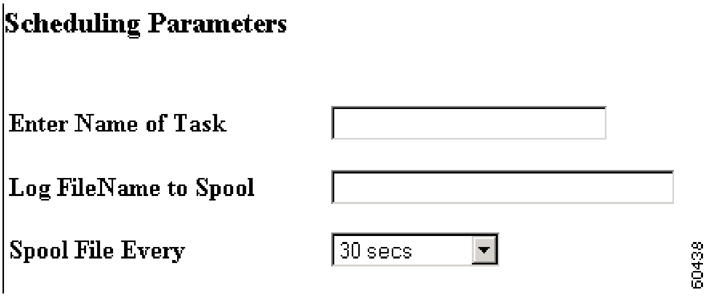
Option	Description
Run	Select to continue a task that has been suspended. Changing a task status from Scheduled to Run is not permitted.
Suspend	Select to temporarily suspend a task that is running or is scheduled to run.
Delete	Forces the task to stop collection and changes the status to Complete.

Step 4 Click **Submit**.

WAN Switches

Schedule Trapd Log

The Trapd Spooler gathers and interprets messages logged in the trapd.log file of HP Open View for WAN Switching nodes based on your input.



Scheduling Parameters

Enter Name of Task

Log FileName to Spool

Spool File Every 30 secs

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > Administration > Schedule Trapd Log.**

Step 2 Enter the name of the Task to schedule.

Step 3 Enter the Filename of the log to spool.

Step 4 Select how often the spooling should occur (every 5 seconds to hourly).

Step 5 Click on **Submit** to display the Scheduler Results.

Caution The Stratacom log task is limited to read only WAN switches in the trapd.log file of HP Open View. The trapd.log file must be accessible (mounted) to the NATKit workstation.

Schedule CLI Collection for BPX/IPG/IPX

The CLI Scheduler is used to schedule the CLI Collection module in NATKit for BPX, IGX, and IPX devices. Specify the start and end times, or periodic time intervals at which this collection program is run.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > Administration > Schedule CLI Collection > BPX/IGX/IPX**. The BPX/IPX/IGX Wan Switches CLI Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Nodes** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select whether or not to continue Command Prompt Processing.

Step 5 Select a Command Profile that contains a pre-defined list of commands, or enter a list of commands separated by a semi-colon. If you are entering a list of commands, be sure to select the appropriate radio button under Select Scheduling Category.

- **Run Selected Profile** - Run the profile selected from the Select Command Profile field.
- **Run the Commands** - Specify a set of commands to run (use a semicolon (;) to separate multiple commands).

Step 6 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 7 Click **Submit** to schedule the task.

Schedule CLI Collection for MGX 8220 (Axis)

This screen is used to schedule a CLI command profile or user-specified commands for MGX 8220 devices. You can specify the start and end times, or periodic time intervals at which this collection program is run on one or more devices selected.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > Administration > Schedule CLI Collection > MGX 8220 (Axis)**. The MGX 8220 (Axis) Wan Switches CLI Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Device(s)** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the number of parallel process you wish to use via the Task Concurrency pull-down menu. Task concurrency can be used to decrease the amount of time it takes the CLI module to complete the task. For example, if you have 10 devices selected with a Task Concurrency of 2, then the CLI module splits the 10 devices into two sets of 5 devices each and processes each set in parallel.

Step 5 Select a Command Profile that contains a pre-defined list of commands, or enter a list of commands separated by a semi-colon. If you are entering a list of commands, be sure to select the appropriate radio button under the Select Scheduling Category section.

- **Run Selected Profile** - Run the profile selected from the Select Command Profile field.
- **Run on all Cards** - Specify a set of commands and run them on all cards (use a semicolon (;) to separate multiple commands).
- **Run on Processor Cards** - Run a set of commands on all active and/or standby processor cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

Step 6 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 7 Click **Submit** to schedule the task.

Schedule CLI Collection for MGX 8230

The CLI Scheduler is used to schedule the CLI Collection module for the MGX 8230 device. The CLI Collection module captures the screen outputs for the commands entered for the profile selected and creates a file in the following format:

```
<task_name>_CLI_<nodename>_<command>.<timestamp>
```

This file is saved in the following directory:

```
/opt/CSCOpx/htdocs/NSA/COMPANIES/<natkid>/out/wansw
```

and can be viewed through the CLI Viewer for MGX 8230 device or by a text editor of your choice.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **Administration** > **Schedule CLI Collection** > **MGX 8230**. The MGX 8230 Wan Switches CLI Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the node(s) by selecting the **All** radio button for all nodes, or the **Device(s)** radio button to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the number of parallel process you wish to use via the Task Concurrency pull-down menu. Task concurrency can be used to decrease the amount of time it takes the CLI module to complete the task. For example, if you have 10 devices selected with a Task Concurrency of 2, then the CLI module splits the 10 devices into two sets of 5 devices each and processes each set in parallel.

Step 5 Select a Command Profile that contains a pre-defined list of commands, or enter a list of commands separated by a semi-colon. If you are entering a list of commands, be sure to select the appropriate radio button under the Select Scheduling Category section.

- **Run Selected Profile** - Run the profile selected from the Select Command Profile field.
- **Run on all Cards** - Specify a set of commands and run them on all cards (use a semicolon (;) to separate multiple commands).
- **Run on Processor Cards** - Run a set of commands on all active and/or standby processor cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

Step 6 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 7 Click **Submit** to schedule the task.

Schedule CLI Collection for MGX 8250/8850 Release 1

This screen is used to schedule a CLI command profile or user-specified commands for MGX 8250/8850 devices. You can specify the start and end times, or periodic time intervals at which this collection program runs on one or more devices selected.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > Administration > Schedule CLI Collection > MGX 8250/8850 Rel1**.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Click in the **Device(s)** radio button and select one or more devices from the Select Device(s) field, or click in the **All** radio button to select all devices listed. Use **CTRL** or **Shift** keys to select multiple devices.

Step 4 Select a profile from the Select Command Profile field. Each command profile has a list of commands associated with it. You can also specify your own commands (see step 6).

Step 5 Select the task concurrency (1-10) from the Task Concurrency pull-down menu. For example, if you schedule a task on 100 devices and select a task concurrency of 10, then 10 threads run in parallel with 10 devices.

Step 6 Select a Command Profile that contains a pre-defined list of commands, or enter a list of commands separated by a semi-colon. If you are entering a list of commands, be sure to select the appropriate radio button under the Select Scheduling Category section.

- **Run Selected Profile** - Run the profile selected from the Select Command Profile field.
- **Run on all Cards** - Specify a set of commands and run them on all cards (use a semicolon (;) to separate multiple commands).
- **Run on Processor Cards** - Run a set of commands on all active and/or standby processor cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

Step 7 Select the desired Start Task, End Task, Periodic Type and Periodic Interval settings, or click **Advanced Timer** for more specific options.

Step 8 Click **Submit**.

⚠ **Caution** This Stratacom CLI interface is designed to work with MGX 8250/8850 Release 1 nodes only.

Schedule CLI Collection for MGX 8850 Release 2

The CLI Scheduler is used to schedule the CLI Collection module for the MGX 8850 Release 2 device. The CLI Collection module captures the screen outputs for the commands entered for the profile selected and creates a file in the following format:

```
<task_name>_CLI_<nodename>_<command>.<timestamp>
```

This file is saved in the following directory:

```
/opt/CSCOpx/htdocs/NSA/COMPANIES/<natkid>/out/wansw
```

and can be viewed through the CLI Viewer for MGX 8850 Release 2 device or by a text editor of your choice.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > Administration > Schedule CLI Collection > MGX 8850 Rel2**. The MGX 8850 Rel 2 Wan Switches CLI Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Nodes** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the number of parallel process you wish to use via the Task Concurrency pull-down menu. Task concurrency can be used to decrease the amount of time it takes the CLI module to complete the task. For example, if you have 10 devices selected with a Task Concurrency of 2, then the CLI module splits the 10 devices into two sets of 5 devices each and processes each set in parallel.

Step 5 Select one of the following:

- **Run on all Cards** - Specify a set of commands and run them on all cards (use a semicolon (;) to separate multiple commands).
- **Run on Processor Cards** - Run a set of commands on all active and/or standby processor cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).
- **Run on AXSM Cards** - Run a set of commands on all AXSM cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

Step 6 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 7 Click **Submit** to schedule the task.

Schedule CLI Collection for MGX 8950

The CLI Scheduler is used to schedule the CLI Collection module for the MGX 8950 device. The CLI Collection module captures the screen outputs for the commands entered for the profile selected and creates a file in the following format:

```
<task_name>_CLI_<nodename>_<command>.<timestamp>
```

This file is saved in the following directory:

```
/opt/CSCOpx/htdocs/NSA/COMPANIES/<natkid>/out/wansw
```

and can be viewed through the CLI Viewer for MGX 8950 device or by a text editor of your choice.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **Administration** > **Schedule CLI Collection** > **MGX 8950**. The MGX 8950 Wan Switches CLI Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Nodes** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the number of parallel process you wish to use via the Task Concurrency pull-down menu. Task concurrency can be used to decrease the amount of time it takes the CLI module to complete the task. For example, if you have 10 devices selected with a Task Concurrency of 2, then the CLI module splits the 10 devices into two sets of 5 devices each and processes each set in parallel.

Step 5 Select one of the following:

- **Run on all Cards** - Specify a set of commands and run them on all cards (use a semicolon (;) to separate multiple commands).
- **Run on Processor Cards** - Run a set of commands on all active and/or standby processor cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

- **Run on AXSM Cards** - Run a set of commands on all AXSM cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

Step 6 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 7 Click **Submit** to schedule the task.

Schedule CLI Collection for BPX-SES

The CLI Scheduler is used to schedule the CLI Collection module for the BPX-SES device. The CLI Collection module captures the screen outputs for the commands entered for the profile selected and creates a file in the following format:

`<task_name>_CLI_<nodename>_<command>.<timestamp>`

`This file is saved in the following directory:`

`/opt/CSCOpx/htdocs/NSA/COMPANIES/<natkid>/out/wansw`

and can be viewed through the CLI Viewer for BPX-SES device or by a text editor of your choice.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **Administration** > **Schedule CLI Collection** > **BPX-SES**. The BPX-SES Wan Switches CLI Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Nodes** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the number of parallel process you wish to use via the Task Concurrency pull-down menu. Task concurrency can be used to decrease the amount of time it takes the CLI module to complete the task. For example, if you have 10 devices selected with a Task Concurrency of 2, then the CLI module splits the 10 devices into two sets of 5 devices each and processes each set in parallel.

Step 5 Select one of the following:

- **Run on all Cards** - Specify a set of commands and run them on all cards (use a semicolon (;) to separate multiple commands).
- **Run on Processor Cards** - Run a set of commands on all active and/or standby processor cards. Select **Active**, **Standby** or **Both** and enter the desired commands, separating each command with a semicolon (;).

Step 6 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 7 Click **Submit** to schedule the task.

Schedule CLI Collection for BPX Report

The BPX Report Scheduler is used to schedule the CLI Collection module and parsing module for the selected BPX report. The CLI Collection module captures the screen outputs for the commands in the selected report and creates a file in the following format:

```
<task_name>_CLI_<nodename>.<timestamp>
```

This file is saved in the following directory:

```
/opt/CSCOpx/htdocs/NSA/COMPANIES/<natkid>/out/wansw
```

Since the reports are a collection of tables that are populated by parsing specific field from the CLI output, you must use the built in viewer and then select the appropriate device category. You can also save the tables in a CSV format to your local machine.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **Administration** > **Schedule Report** > **BPX**. The BPX Wan Switches Report Scheduling frame is displayed.

Step 2 Enter the name of the task to be scheduled in the Enter Name of Task field.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Nodes** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the report profile from the Select Report Profile column.

Step 5 Select the desired Start Task, End Task and Run Task options, or click **Advanced Timer** for more specific Start Task, End Task, and Run Task options.

Step 6 Click **Submit** to schedule the task.

View Trapd Log

The Trapd Viewer allows you to view the contents of the trapd.log file of HP Open View for WAN Switching nodes. Display options include node name, alarm type, and message type.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > View Trapd Log**.

Step 2 Select whether to view nodes, alarm types, or message types.

Step 3 Determine the time range of the Node, Alarm Type or Message Type by setting the Start Time and End Time parameters.

Step 4 Click on **Submit** to display a list of Nodes, Alarm Types, or Message Types.

Step 5 Click on the particular Node, Alarm Type or Message Type to display more information about it.

Caution The Stratacom log task is limited to read only WAN switches in the trapd.log file of HP Open View. The trapd.log file must be accessible (via a file mount) to the machine running NATKit.

View CLI Collection for BPX/IGX/IPX

The CLI viewer displays the output gathered from the CLI commands that capture the switch log, software logs, card and slot errors, CPU utilization, and memory blocks for BPX, IGX, and IPX switching nodes. The viewer displays output per profile, device, and run time.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > View CLI Collection > BPX/IGX/IPX.**

Step 2 Select a profile to view from the pull down window.

Step 3 Click on **Submit** to display a list of WAN switches from the profile selected. Click on the desired WAN switch to display a list of WAN switch times for that switch.

Step 4 Select the WAN switch time desired from the pull-down window and click **Submit**.

Step 5 Output from the CLI Log appears.

Caution The Stratacom CLI interface is designed to work with Stratacom nodes only.

View CLI Collection for MGX 8220 (Axis)

The CLI viewer displays the output gathered from the CLI commands that capture the switch log, software logs, card and slot errors, CPU utilization, and memory blocks for MGX 8220 (Axis) devices only. The viewer displays output per profile, device, and run time.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > View CLI Collection > MGX 8220 (Axis).**

Step 2 Select a profile to view from the Select Profile to View pull-down menu and click **Submit**.

Step 3 Click in the **Device(s)** radio button and select one or more devices from the Select Device(s) field, or click in the **All** radio button to select all devices listed.

Note Use **CTRL** or **Shift** keys to select multiple devices.

Step 4 Click in the **Slot(s)** radio button and select one or more slots from the Select Slots field, or click in the **All** radio button to select all slots listed.

Note Use **CTRL** or **Shift** keys to select multiple slots.

Step 5 Select the time the task was run from the Select Time pull-down menu.

Step 6 Select how the data is sorted by choosing one of the following sort options:

- Device
- Slot Number
- Command

Step 7 Click **Submit.** A list of devices from the profile selected is displayed by name, slot number and command.

Step 8 Click on a hyperlinked device name, slot number or command to view more information about it.

- **Device** - Shows output of all commands that are run on all slots of that device.
- **Slot Number** - Shows output of all commands that are run on that slot of the device in that row.
- **Command** - Shows output of the command that are run on that device and slot on that row.

Caution This Stratacom CLI interface is designed to work with MGX 8220 (Axis) nodes only.

View CLI Collection for MGX 8230

The CLI Viewer is used to view the CLI Collection module for MGX 8230 devices. The CLI viewer displays the raw data output for the various CLI commands in a given task.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **View CLI Collection** > **MGX 8230**. The MGX 8230 Wan Switches CLI Viewer frame is displayed.

Step 2 Select a profile from the Select Profile to View pull-down menu and click **Submit**.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Device(s)** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the desired slot(s) by selecting the All radio button for all slots, or Slot(s) to select one or more slots in the list.

Note Use the **Shift** or **CTRL** keys to select more than one slot.

Step 5 Select the time of the run that you want to view from the Select Time pull-down menu.

Step 6 Select how you want to sort the output.

Step 7 Click **Submit** to view the list of devices, slots, and commands.

Step 8 Click on a device name to view the output of all commands for that device. Click on the slot number to view the output for all commands for that device/slot. Click on a command to view the output for just that command.

View CLI Collection for MGX 8250/8850 Release 1

The CLI viewer displays the output gathered from the CLI commands that capture the switch log, software logs, card and slot errors, CPU utilization, and memory blocks for MGX 8250/8850 Release 1 devices only. The viewer displays output per profile, device, and run time.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > View CLI Collection > MGX 8250/8850 Rel1.**

Step 2 Select a profile to view from the Select Profile to View pull-down menu and click **Submit**.

Step 3 Click in the **Device(s)** radio button and select one or more devices from the Select Device(s) field, or click in the **All** radio button to select all devices listed.

Note Use **CTRL** or **Shift** keys to select multiple devices.

Step 4 Click in the **Slot(s)** radio button and select one or more slots from the Select Slots field, or click in the **All** radio button to select all slots listed.

Note Use **CTRL** or **Shift** keys to select multiple slots.

Step 5 Select the time the task was run from the Select Time pull-down menu.

Step 6 Select how the data is sorted by choosing one of the following sort options:

- Device
- Slot Number
- Command

Step 7 Click **Submit.** A list of devices from the profile selected is displayed by name, slot number and command.

Step 8 Click on a hyperlinked device name, slot number or command to view more information about it.

- **Device** - Shows output of all commands that are run on all slots of that device.
- **Slot Number** - Shows output of all commands that are run on that slot of the device in that row.
- **Command** - Shows output of the command that are run on that device and slot on that row.

Caution This Stratacom CLI interface is designed to work with MGX 8250/8850 Release 1 nodes only.

VIew CLI Collection for MGX 8850 Release 2

The CLI Viewer is used to view the CLI Collection module for MGX 8850 Rel2 devices. The CLI viewer displays the raw data output for the various CLI commands in a given task.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **View CLI Collection** > **MGX 8850 Rel2**. The MGX 8850 Rel2 Wan Switches CLI Viewer frame is displayed.

Step 2 Select the profile from the Select Profile to View pull-down menu and click **Submit**.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Device(s)** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the desired slot(s) by selecting the **All** radio button for all slots, or **Slot(s)** to select one or more slots in the list.

Note Use the **Shift** or **CTRL** keys to select more than one slot.

Step 5 Select the time of the run that you want to view from the Select Time pull-down menu.

Step 6 Select how you want to sort the output.

Step 7 Click **Submit** to view the list of devices, slots, and commands.

Step 8 Click on a device name to view the output of all commands for that device. Click on the slot number to view the output for all commands for that device/slot. Click on a command to view the output for just that command.

View CLI Collection for MGX 8950

The CLI Viewer is used to view the CLI Collection module for MGX 8950 devices. The CLI viewer displays the raw data output for the various CLI commands in a given task.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > View CLI Collection > MGX 8950**. The MGX 8950 Wan Switches CLI Viewer frame is displayed.

Step 2 Select the profile from the Select Profile to View pull-down menu and click **Submit**.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Device(s)** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the desired slot(s) by selecting the **All** radio button for all slots, or **Slot(s)** to select one or more slots in the list.

Note Use the **Shift** or **CTRL** keys to select more than one slot.

Step 5 Select the time of the run that you want to view from the Select Time pull-down menu.

Step 6 Select how you want to sort the output.

Step 7 Click **Submit** to view the list of devices, slots, and commands.

Step 8 Click on a device name to view the output of all commands for that device. Click on the slot number to view the output for all commands for that device/slot. Click on a command to view the output for just that command.

View CLI Collection for BPX-SES

The CLI Viewer is used to view the CLI Collection module for BPX-SES devices. The CLI viewer displays the raw data output for the various CLI commands in a given task.

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > View CLI Collection > BPX-SES**. The BPX-SES Wan Switches CLI Viewer frame is displayed.

Step 2 Select the profile from the Select Profile to View pull-down menu and click **Submit**.

Step 3 Select the desired node(s) by selecting the **All** radio button for all nodes, or **Device(s)** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 4 Select the desired slot(s) by selecting the **All** radio button for all slots, or **Slot(s)** to select one or more slots in the list.

Note Use the **Shift** or **CTRL** keys to select more than one slot.

Step 5 Select the time of the run that you want to view from the Select Time pull-down menu.

Step 6 Select how you want to sort the output.

Step 7 Click **Submit** to view the list of devices, slots, and commands.

Step 8 Click on a device name to view the output of all commands for that device. Click on the slot number to view the output for all commands for that device/slot. Click on a command to view the output for just that command.

View Scheduled Reports for BPX Devices

The Report Viewer is used to view the scheduled reports for BPX devices. The Report viewer displays the parsed data in various tables as defined by the specific report selected.

Procedure

Step 1 Select **Network Analysis Toolkit** > **WAN Switches** > **View Report** > **BPX**. The BPX Wan Switches Report Viewer frame is displayed.

Step 2 Select the desired Node(s) by selecting the **All** radio button for all nodes, or **Device(s)** to select one or more nodes in the list.

Note Use the **Shift** or **CTRL** keys to select more than one node.

Step 3 Select the report profile from the Select Report Profile field and click **Submit**.

Step 4 Select the time of the run that you want to view from the Select Report Run Time to View pull-down menu.

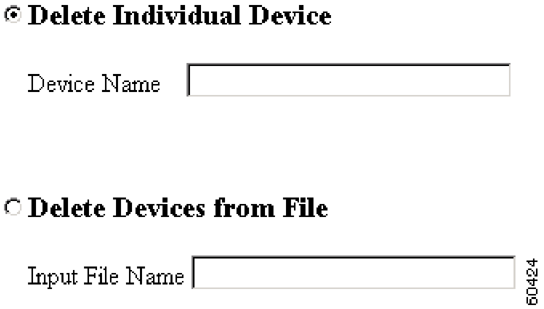
Step 5 Click **Submit** to view the report.

Step 6 Click **Download CSV File** to save the report for that node to a comma-separated-value file for importing into a spreadsheet.

Step 7 Click **View Report Output File** to view the raw CLI data used to create the tables in the report.

Delete WAN Switches

This screen allows you to delete an individual device or devices located in a file.



● **Delete Individual Device**

Device Name

○ **Delete Devices from File**

Input File Name

Procedure

Step 1 Select **Network Analysis Toolkit > WAN Switches > Administration > Delete WAN Switches.**

Step 2 To delete an individual device, select **Delete Individual Device** and enter the name of the device in the Device Name field.

Step 3 To delete the devices in a file, select **Delete Devices from File** and enter the name of the file in the Input File Name field.

Step 4 Click on **Submit**.

Task Manager

View Scheduled Tasks

The NATKit Scheduler schedules new tasks, starts and ends tasks on time, and deletes the task context when instructed to do so. The scheduler is responsible for checking resource availability before starting a task. It also maintains statistics for how many times the task got started and ended, and its success or failure.

A Note About Tasks and Profiles

The terms *task* and *profile* are used somewhat interchangeably. A task such as an inventory task, or availability task may be scheduled. A *profile* is a configurable task. Currently only Syslog tasks (called Syslog Reporter files) are configurable.

NATKit System Tasks

In addition to scheduled tasks and profiles such as inventory, config, availability, syslog, and poller, Scheduler also maintains NATKit system tasks. These include:

- **Daily Access Verifier** - Verifies device SNMP read-only/read-write community strings and log in strings (password, enable password, TacAcs user name, etc.).
- **Garbage Collector** - Periodically clears temporary files from directories.
- **Database Backup** - Periodically backs up critical NATKit information from the database.
- **Daily Health Download** - Downloads health information of the NATKit box to Cisco.
- **Daily Download** - Schedules the Download Manager to send data back to Cisco.
- **NMS Device Import** - Extracts device names from RME and imports them into the NATKit database.
- **Daily Reporter** - Creates a report summarizing all activities in the last 24 hours.
- **Daily Purger** - Purges data dependencies on purge configs.

- **Device Scheduler** -Schedules Access Verifier, DNM, and Wan Node Discovery for every device added and modified in RME. Device Scheduler runs every 10 minutes and checks whether any device has been added or device attribute modified in the last 10 minutes. If an addition or modification is found, the Device Scheduler schedules the access verifier, DNM and Wan Node discovery for the devices that have changed.
- **Daily DNM** - Searches NATKit looking for all the aliases for the device. This program runs once every 24 hours and collects the various alias names for that device.

The Scheduler Layout

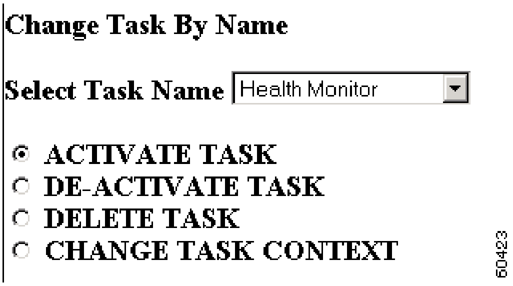
Each row in the Scheduler represents a task and its properties.

- **Task #** - Task id number assigned by the Scheduler.
- **Task Name** - Name of the task. If the task or profile has been scheduled, it is the name that was assigned the task. Click on a Task Name to view detailed information it.
- **Task Module** - Type of task. For example, poller or system task.
- **Creator** - Creator of the task.
- **Status** - Either ON (Activated) or OFF (De-activated).
- **Start Time** - The starting time for this task.
- **End Time** - The ending time for this task.
- **Last Execute Time** - The last ending time for this task.
- **Next Start Time** - The next time the task is scheduled for execution.
- **Periodic Interval** - The task execution frequency.

Change Task Settings

Changing the status of a task affects how a task is handled by the Scheduler. There are four ways to change the status of a task:

- **Activate Task** - Sets the status of a task or profile to ON in the Scheduler.
- **De-Activate Task** - Sets the status of a task or profile to OFF in the Scheduler. If the task or profile is currently running, it runs to its scheduled completion, but is not scheduled again.
- **Delete Task** - Deletes the task or profile from the scheduler. If the task or profile is currently running, it runs to its scheduled completion, but is not scheduled again.
- **Change Task Context** - Reschedules a task in the Scheduler. If rescheduling a task that has been de-activated, use this option to re-activate the task.



Change Task By Name

Select Task Name Health Monitor ▾

● ACTIVATE TASK
○ DE-ACTIVATE TASK
○ DELETE TASK
○ CHANGE TASK CONTEXT

Procedures

Activating, De-Activating, and Deleting Tasks

Step 1 Select **Network Analysis Toolkit > Scheduler > Administration > Change Task Settings**.

Step 2 Select a task to activate, de-activate, or delete from the pull-down menu.

Step 3 Check the desired option, Activate, De-Activate, or Delete Task.

Step 4 Click **Submit** to make the status change.

Changing the Context of a Task

Step 1 Select **Network Analysis Toolkit** > **Scheduler** > **Administration** > **Change Task Settings**.

Step 2 Select the task to change from the pull-down menu.

Step 3 Check the Change Task Context option.

Step 4 Click **Submit** to proceed to the scheduling screen.

Step 5 Change the Start, End and Periodic times to what you want.

Step 6 Click **Submit** to send all changes to the Scheduler.

Caution Currently, Syslog profiles cannot be edited using Change Task Context. SNMP poller tasks do not appear in the general scheduler, and may be modified using the Change Task Status option from **Network Analysis Toolkit** > **SNMP Poller** > **Administration** > **Change Task Status**.

Download

The tools in this folder allow you to view the contents of all downloaded .tar files for each module on NATKit, as well as to schedule an on-demand download.

Show Download Files

All files in the downloaded .tar file for each module are expanded and displayed on this screen.

Procedure

Step 1 Select **Network Analysis Toolkit > Download > Show Download Files**. All downloaded .tar files and the modules in each are displayed. All files contained in each module are listed and hyperlinked.

Step 2 Click a hyperlinked file under the **File** column to view its contents.

Step 3 Click on the hyperlinked .tar file to download it to your local computer.

Download Now

Use this screen to schedule an on-demand download.

Procedure

Step 1 Select **Network Analysis Toolkit > Download > Download Now**.

Step 2 Click **Start** to confirm the schedule on demand download. A confirmation screen appears if the download was successfully scheduled.

Step 3 Click View Scheduled Tasks to view the contents of the scheduler.

Logs and Errors

NATKit creates error reports and message logs for all the tasks carried out by NATKit. Each tool, SNMP Poller, Syslog, System Logs, Scheduler, Inventory, Configs, Seedfile Manager, Domain Manager, Integration Manager, GUI, Access Verifier, Downloader, Event Statistics, and Transient has a corresponding error report and message log.

The error reports list any problems encountered while trying to perform data collection. The message logs track various data collection events, depending on which tool's log is being viewed.

In addition to each tool, there is an error report and message log for NATKit's system processes that collects similar information. System error reports and messages logs have static and dynamic views.

Logging, Error Rotation and Reporting Levels

In order to conserve disk space, NATKit controls the size of log and error files by using two mechanisms:

- **Logging and Error Rotation**- When a message log or error report file reaches a configurable size, newer data is collected and older data is rotated out of the file. The default size for log and error files is configured by NATKit support personnel. Contact them (NATKit-support@cisco.com) for specific information.
- **Reporting Levels** - There are five levels of message and error reporting, from level 1 (Catastrophic) to level 5 (Debugging). As the reporting level increases (level 1 is lowest), the amount of information collected and saved for each error or log message grows. The level of data collection for each error report and message log is configured by NATKit support personnel. In order to maintain the greatest number of events in each error report and message log, the default level is 2 (critical events and status events) for message logs and 3 (catastrophic, critical, and operational events) for error reports.

Error Report and Message Log Format

Each message log and error report follows a similar, tabular format. Information for each recorded event includes:

- **PRI** - A reporting (priority) level (see Reporting Levels above)
- **Timestamp** - The date the event was recorded
- **Message** - The event message
- **Task ID** - The task ID number

Procedure

Log and Error messages can be viewed in one of the following four ways:

- By Process ID
- By Priority Level
- By Time
- View all Messages

Viewing by Process ID

Step 1 Select **Network Analysis Toolkit > Logs and Errors.**

Step 2 Choose the task to check.

Step 3 Click on **Logs** or **Errors**.

Step 4 Select **View by Process ID** from the Select Viewing Category field.

Step 5 Select the Task ID from the Select Task ID pull-down menu.

Step 6 Click **Submit**.

Viewing by Priority Level

Step 1 Select **Network Analysis Toolkit > Logs and Errors.**

Step 2 Choose the task to check.

Step 3 Click on **Logs** or **Errors**.

Step 4 Select **View by Priority Level** from the Select Viewing Category field.

Step 5 Select the Priority Level (1-5) to view from the Select Priority Level pull-down menu.

Step 6 Click **Submit**.

Viewing by Time

Step 1 Select **Network Analysis Toolkit > Logs and Errors.**

Step 2 Choose the task to check.

Step 3 Click on **Logs** or **Errors**.

Step 4 Select **View Messages During a Time Period** from the Select Viewing Category field.

Step 5 Use the Select Time Interval Tool to choose the start and end time of the time period to search for Log/Error messages.

Step 6 Click **Submit**.

Viewing All Messages

Step 1 Select **Network Analysis Toolkit > Logs and Errors.**

Step 2 Choose the task to check.

Step 3 Click on **Logs** or **Errors**.

Step 4 Select **View All Messages** from the Select Viewing Category field.

Step 5 Click **Submit**.

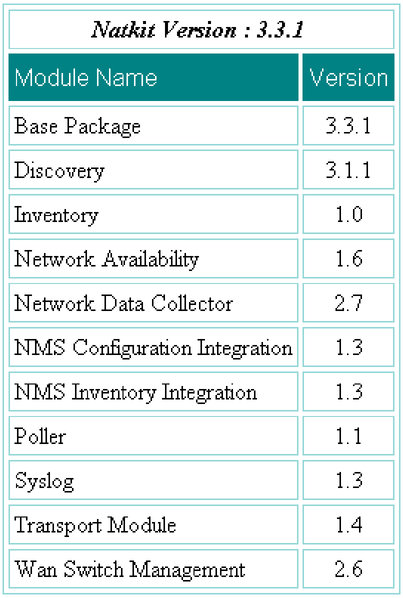
About NATKit

This function allows you to check the version number of the NATKit system and the modules installed in the system.

Procedure

Step 1 Select **Network Analysis Toolkit > About NATKit> Modules Installed.** The NATKit Version dialog box is displayed.

Step 2 Check the version number of the NATKit system and the installed modules.



Natkit Version : 3.3.1

Module Name	Version
Base Package	3.3.1
Discovery	3.1.1
Inventory	1.0
Network Availability	1.6
Network Data Collector	2.7
NMS Configuration Integration	1.3
NMS Inventory Integration	1.3
Poller	1.1
Syslog	1.3
Transport Module	1.4
Wan Switch Management	2.6

Net Audit

Timesaver You should read and understand "Running an Audit from Start to Finish" before continuing with this section.

The Net Audit folder consists of tools used to collect data for Net Audits, define and verify access for devices, and monitor data collection with real-time statuses.

Register Audit

An authentication key is provided by the Cisco NATKit Support Engineer. Please contact your Advanced Services Engineer for details on registering your audit.

Net Audit Settings

The initialization phase of setting up an audit is done here. The screen shows Audit ID and the Audit Type depending upon the authentication key assigned by Cisco and entered by the Cisco NATKit support engineer at the time of audit scheduling. The following information can be verified and entered on this screen:

Method	Description
Audit ID #	A distinct number assigned for each audit that is being scheduled on the Network Analysis Toolkit.
Audit Type	Shown from nine different audits: • Cisco Snapshot Audit for WAN Switched Networks 3.0 • Cisco Snapshot Net Audit for LAN Switched Networks • Cisco Snapshot Net Audit for Routed Networks • Cisco Snapshot Net Audit for Routed and LAN Switched Networks • Cisco Stability Net Audit for Cisco 12000 Series Internet Routed Networks • Cisco Stability Net Audit for IP Telephony Networks • Cisco Stability Net Audit for LAN Switched Networks • Cisco Stability Net Audit for OSPF Networks • Cisco Stability Net Audit for Routed Networks
Company	This is the name of the customer the audit is being performed for. This field is mandatory.
Data Collector	The means of collecting the data. This field is mandatory.
Auditor Email	This is the email address of the contact person at the company the audit is being performed for. This field is mandatory.
Comments	Any information deemed pertinent by the customer in regards to the audit being performed should be included here. This field is mandatory.

Note The Audit ID and Audit Type fields are automatically filled.

Procedure

Step 1 Select **Network Analysis Toolkit > Net Audit > Net Audit Settings**. The Net Audit Settings dialog box appears.

Note Audit key must be registered by Cisco NATKit Support Engineer before you can access Net Audit Settings. If not, you will see the following error ***Authentication Key Not Registered, please contact Net Audit Support <mailto:netaudit-support@cisco.com?subject=Authentication Key> for further help.*** when accessing the Net Audit Settings dialog box.

Step 2 Ensure the name of the company the audit is being performed for in the Company field is accurate.

Step 3 Enter the data collector that will be scheduling the audit.

Step 4 Enter the email address of the contact person in the Auditor Email field.

Step 5 Enter any information deemed pertinent in regards to the audit being performed in the Comment field.

Step 6 Click **Submit**.

Device Selection

All eligible routers and/or switches added or imported appear in their respective Switch or Router screen. Select one or more of each to include in the audit. The devices selected are tested using the Access Verifier as explained in the Schedule Access Verification section. Devices on the Switch and Router screens appear in one of the following two columns:

- **Device List** - Devices available to be audited, but have not yet been selected to be included in the audit.
- **Selected Devices for Audit** - Devices that have been selected to be included in the audit.

Note Router and switch device types will be used as examples below, illustrating how to select devices for the audit. Other device types are also supported. Please contact your Advanced Services Engineer to get details on which devices are supported by each of our audits.

Procedure

Step 1 Select **Network Analysis Toolkit** > **Net Audit** > **Device Selection**. The Select Devices for Net Audit screen appears with the Routers or Switches tab displayed.

Step 2 Highlight the router (or routers) in the Device List column to be included in the audit.

Step 3 Click on **Select**. The highlighted router(s) are moved to the Selected Devices for Audit column (or click on **Select All** to move all routers to the Selected Devices for Audit column).

Note To remove a selected router listed in the Selected Devices for Audit column, highlight it and click **Deselect** to return it to the Device List column.

Step 4 Click **Next** to proceed to the Switch List window.

Step 5 Highlight the switch (or switches) in the Device List column to be included in the audit.

Step 6 Click **Select**. The highlighted switch(es) are moved to the Selected Devices for Audit column (or click on Select All to move all switches to the Selected Devices for Audit column).

Note To remove a selected switch listed in the Selected Devices for Audit column, highlight it and click **Deselect** to return it to the Device List column.

Step 7 Click **Next** to proceed to Access Verification.

Access Verification

Refer to Schedule Access Verification located earlier in this chapter for more information on scheduling access verification.

Data Collection

You can start the data collection immediately or use the scheduler to set a time within in the next five years to begin data collection. You can stop data collection or change the schedule at any time. When scheduling a data collection, the following parameters can be set:

- Month
- Day
- Year
- Hour
- Minute

Start a Data Collection

Step 1 Select **Network Analysis Toolkit** > **Net Audit** > **Data Collection**. The Data Collection dialog box appears.

Step 2 Select **Start Collection**.

Step 3 Click **Next** to immediately start the data collection.

Note Once a data collection has started, it can be stopped by clicking **Stop Collection**.

Schedule a Data Collection

Step 1 Select **Network Analysis Toolkit > Net Audit > Data Collection**. The Data Collection dialog box appears.

Step 2 Select the month to begin the data collection from the Month pull-down menu.

Step 3 Select the day to begin the data collection from the Day pull-down menu.

Step 4 Select the year to begin the data collection from the Year pull-down menu.

Step 5 Select the hour to begin the data collection from the Hour pull-down menu

Step 6 Select the minute to begin the data collection from the Minute pull-down menu.

Step 7 Select **Schedule Collection**.

Note Once Schedule Collection has been selected, the **Change Schedule** option becomes active. Click on it to change any of the previously selected settings.

Step 8 Click **Next**.

Note Once a data collection has started, it can be halted by clicking **Stop Collection**.

Data Collection Status

The Data Collection Status screen allows you to monitor the status of the current data collection process. The information displayed on this page reflects cumulative data for all routers and switches from the beginning of the collection up to the time the Data Collection Status screen was accessed. The Net Audit Success Rate is used to determine the success/failure of the audit. The success rate must be 80% or higher for the audit to pass.

The node status can be in one of three states:

- Passed
- Failed
- Contingent

Note Telnet 2 information is not collected until the final day of collection.

Procedure

Step 1 Select **Network Analysis Toolkit > Net Audit > Data Collection Status**. The Data Collection Status screen appears.

Step 2 Select **Stop Collection** to end the current data collection process if needed.

Step 3 Click **Node Status** to advance to the Node Status screen.

Note Click **Refresh** to updated the information on the Data Collection Status screen.