Net Insight – Nimbra Vision Training

Nimbra Vision 5.6 and NimOS GX4.6

November 2010

Workbook

This page is intentionally blank.

Contents

Lab. 1 Element Manager

Goal

In this exercise you get acquainted with the web browser and Net Insight's products.

Management network setup for the exercises

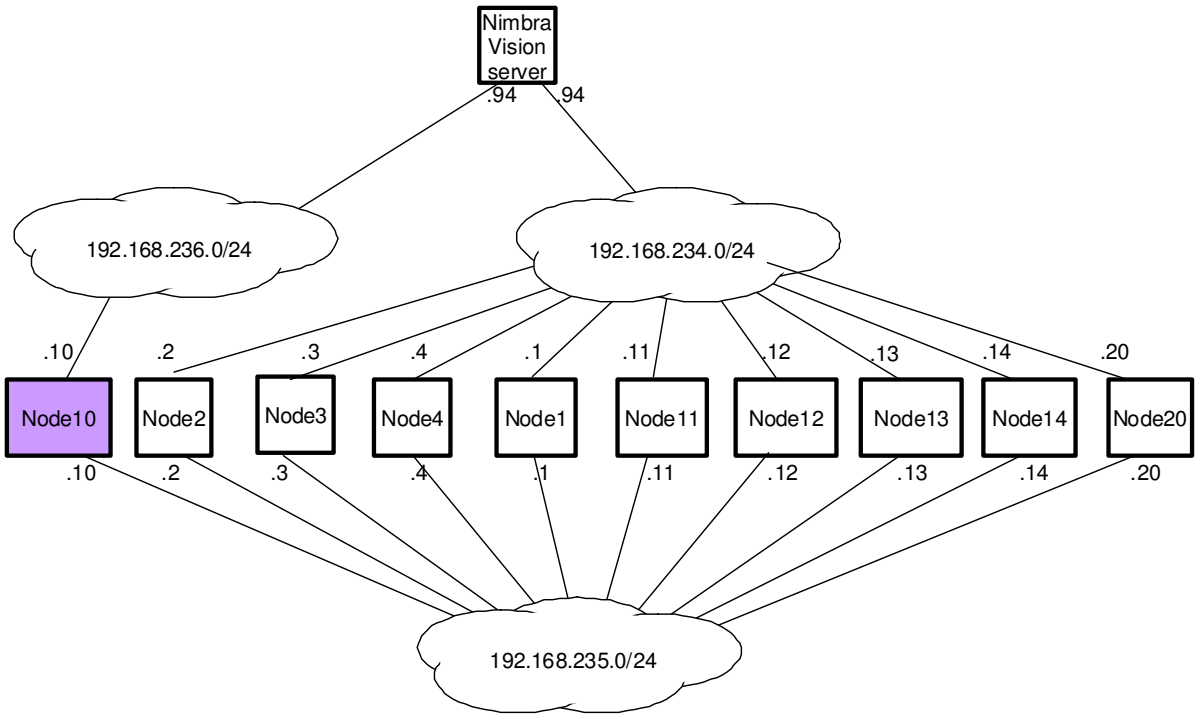


Figure 1. Redundant management networks. Node10 is gateway and DLE server

Start of PC/Login to Nimbra nodes

Log in to the PC with user name administrator and password 4neti. Start a web browser and log in to the various nodes from the web browser. To log in, enter the node names in the URL field (IP address 192.168.234.xxx, where xxx is the node number).

The Nimbra nodes all have user name root and password neti.

Lab 2 Preliminaries in Network Elements

Preliminary actions to before launching Nimbra Vision:

Define SNMP notification receivers. The nodes must send SNMP notifications to the IP address of the Nimbra Vision server. In cases of server failover or load balancing, notifications (traps) must be sent to all possible servers. The used SNMP port (UDP port) is the port Nimbra Vision uses to listen to SNMP notifications. This port is 162 by default.

The nodes must be configured properly for SNMP v2c or SNMP v3 actions, whichever is used.

Nimbra Vision uses host name lookup to match the IP addresses of the nodes to host names and host names to the IP address of the nodes. For this reason, the hosts file must be correct on all possible Nimbra Vision servers (By default, the hosts file is located in the C:\WINDOWS\system32\drivers\etc folder).

The eventlog in all network elements should be large enough to hold events for at least a couple of minutes. A rule-of-thumb is 2.5 times the number of expected connections originating or terminating on the node, but not less than 50. Nimbra vision uses the eventlog to fetch earlier events that have been lost. If the eventlog does not contain the missed event, Nimbra Vision has to refresh the complete network element in the database. This is an operation that is more time consuming.

Goal

In this exercise you will learn how to configure the trap receivers and SNMPv3 access settings in the network element. You will also learn how to increase the event log.

Configuration of SNMP Parameters

Nimbra Vision uses SNMPv1 and/or SNMPv2c when monitoring the nodes and SNMPv2c or SNMPv3 when it writes to the nodes. You have to define a user with a password that shall be used by Nimbra Vision when it writes to the nodes.

The procedure is to create a user for SNMPv3 access using security level AuthNoPriv with full user rights, which means that the user can both read from and write to the nodes.

The nodes should be configured to send SNMP notifications to Nimbra Vision. The notifications are sent when an alarm status or a configuration has changed.

To configure SNMP parameters, open a web browser and connect to the node. Write the IP address in the URL window and login with user/password combination root/neti. Follow the Control Network → SNMP link to configure SNMP v3 access and set SNMP trap receivers.

Configuration of SNMP access

On the SNMP configuration page, set the read-only community name in the box intended for this. The default value is ‘public. This community allows SNMPv1/v2c read operations, but not write operations. Leave this blank if you want to use the same community name for read and write.

Set a read-write community name in the box intended for this. This community will allow both read and write operations using SNMPv1/v2c. If this field is left blank, write operations are disabled.

Set an SNMPv3 user name in the intended box, for example root, use authNoPriv as security level and set the password to ‘passwd’. Click ‘OK’ to confirm the setting.

Configuration of SNMP notification (trap) receiver

Set the SNMP Notification Receivers. Select the button ‘Add SNMP Notification Receiver…’ to add a new notification receiver, or select an existing from the table if you want to modify it. Enter the IP address(es) to Nimbra Vision server(s), and UDP port number (default is 162). Click ‘OK’ to confirm the selection. Save the configuration when all the necessary changes have been made. (You can do this after the next exercise, lab 2c).

Configuration of the Eventlog Size

The eventlog in the node should be large enough to hold event for at least a couple of minutes. Nimbra Vision uses this event log to fetch events that has been lost. If the log does not contain a missed event, Nimbra Vision needs to refresh the complete node. This is an operation that is more expensive. A good rule of thumb is that the event log size should be at about 2.5 times the number of expected connections, but not less than 50. Follow the link Maintenance → System and set the event log size to 50 in the appropriate box. Confirm with the ‘OK’ button.

Definition of the hosts text file

When Nimbra Vision discovers a new network element, or makes a refresh of a network element, it gives the element a name based on its IP address. Nimbra Vision names the element after the host name in the hosts file. For correct function, the name lookup must report the same result each time. If no name is returned by the hostname function, its IP address is used as a name. If another name is returned when the object is (re)discovered, a new object is created in the database. In this manner, the database has two entries for the same physical element.

The normal operation of host name lookup is that the local host database of the Nimbra Vision server is used. If no match is found in the file, the DNS server is asked. This step, of course, requires that a DNS server is used.

For Windows NT4/2000, the file is named `C:\WINNT\system32\drivers\etc\hosts` and for Windows XP, the file is named `C:\WINDOWS\system32\drivers\etc\hosts`.

If you don't have a (reliable) DNS server, it is a good idea to enter hostnames for the IP addresses of the network elements in the hosts file. If you use redundant management networks, i.e. multiple IP addresses for a single node, then you must use the local hosts file. Note that the information in the hosts file is used by all the applications on your server, not only by
Nimbra Vision.

The hosts file contains mappings of IP addresses to host names. Each entry should be kept on a separate line. The IP address should be placed in the first column followed by the corresponding host name. The IP address and the host name should be separated by at least one space. Additionally, comments may be inserted on individual lines or following the host name denoted by a number sign (#).

For redundant networks, each node has two or more IP addresses. Each of the IP address to a host name relationship is entered in the file. An earlier entry has higher priority than a later entry for the same hostname.

Example for the network used in the exercises:

```
127.0.0.1       localhost

# outband
192.168.234.1   node01 # primary address
192.168.236.1   node01 # Management net
192.168.234.2   node02 # primary address
192.168.234.3   node03 # primary address
192.168.234.4   node04 # primary address
192.168.234.10  node10 # primary address

192.168.234.11  node11 # primary address
192.168.234.12  node12 # primary address
192.168.234.13  node13 # primary address
192.168.234.14  node14 # primary address
192.168.234.20  node20 # primary address

# inband
192.168.235.1   node01 # secondary address
192.168.235.2   node02 # secondary address
192.168.235.3   node03 # secondary address
192.168.235.4   node04 # secondary address
192.168.235.10  node10 # secondary address

192.168.235.11  node11 # secondary address
192.168.235.12  node12 # secondary address
192.168.235.13  node13 # secondary address
192.168.235.14  node14 # secondary address
192.168.235.20  node20 # secondary address
```

Lab. 3 Starting Nimbra Vision

Goal

In this exercise, you'll learn how to start Nimbra Vision server and client.

Start the Nimbra Vision Server

Double click on the icon 'Start Nimbra Vision Server 5.5.1'. Some DOS command prompts are opened automatically. The must be kept open for Nimbra Vision to work properly. Wait for all processes to start and a request to start Nimbra Vision Client.

Start the Nimbra Vision Client

Double click on the icon 'Start Nimbra Vision Client 5.5.1'. Wait for the java client to open in a separate window. The default user/password combination for Nimbra Vision is root/public. If not on the Nimbra Vision server, click on the 'Advanced' button and enter the IP address or host name of the Nimbra Vision server. After all connection settings have been made, confirm with the 'Connect' button

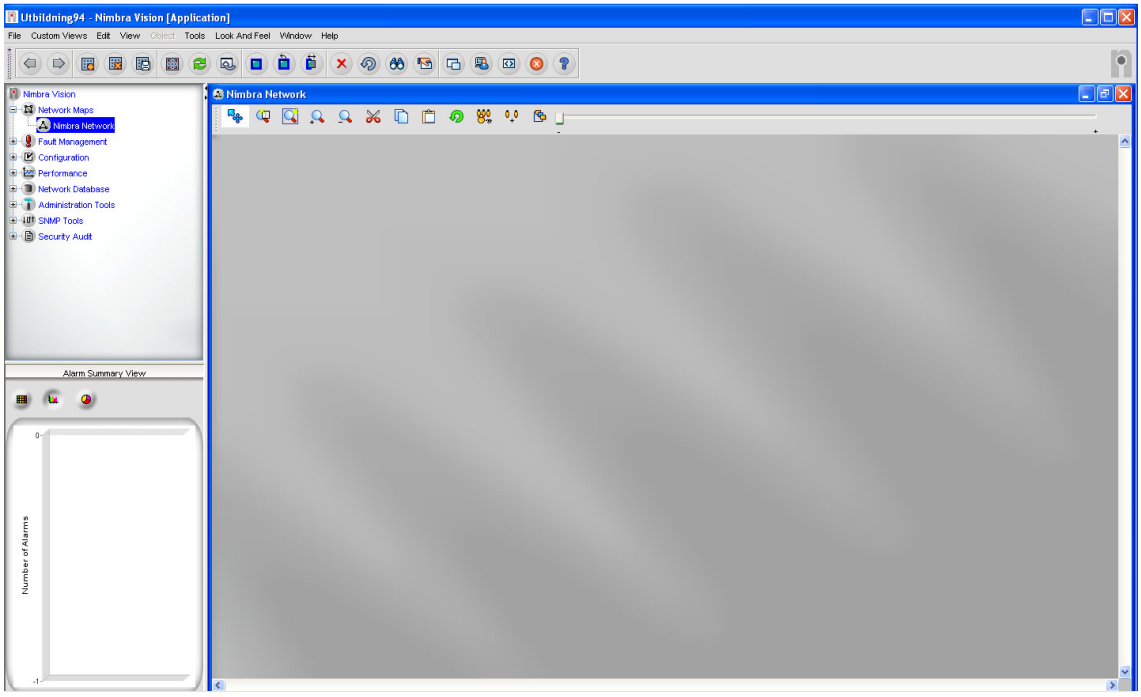


Figure 2. Nimbra Vision Client (5.5.1).

Lab. 4 Configuring the Discovery Engine

Nimbra Vision must be configured for discovery of the network elements in the network(s). This configuration is a set of rules and seeds used by Nimbra Vision to discover network elements that you want Nimbra Vision to monitor.

Tabs for Topology Discovery Configurator:

- General - general settings for the discovery engine
- Protocol - configuration of general but protocol specific parameters
- Network Discovery - configuration of IP networks or address ranges to discover
- Node Discovery - add individual nodes as seeds prior discovering networks or ranges
- Criteria - limit discovery to only include nodes having specified characteristics, e.g. only Nimbra nodes

Discovery Configurator

The Discovery Configurator is started from Nimbra Vision client. Select menu Tools - Runtime Administration and there select Topology - Discovery Configurator.

Most of the parameter settings are already adequate for most Nimbra networks.

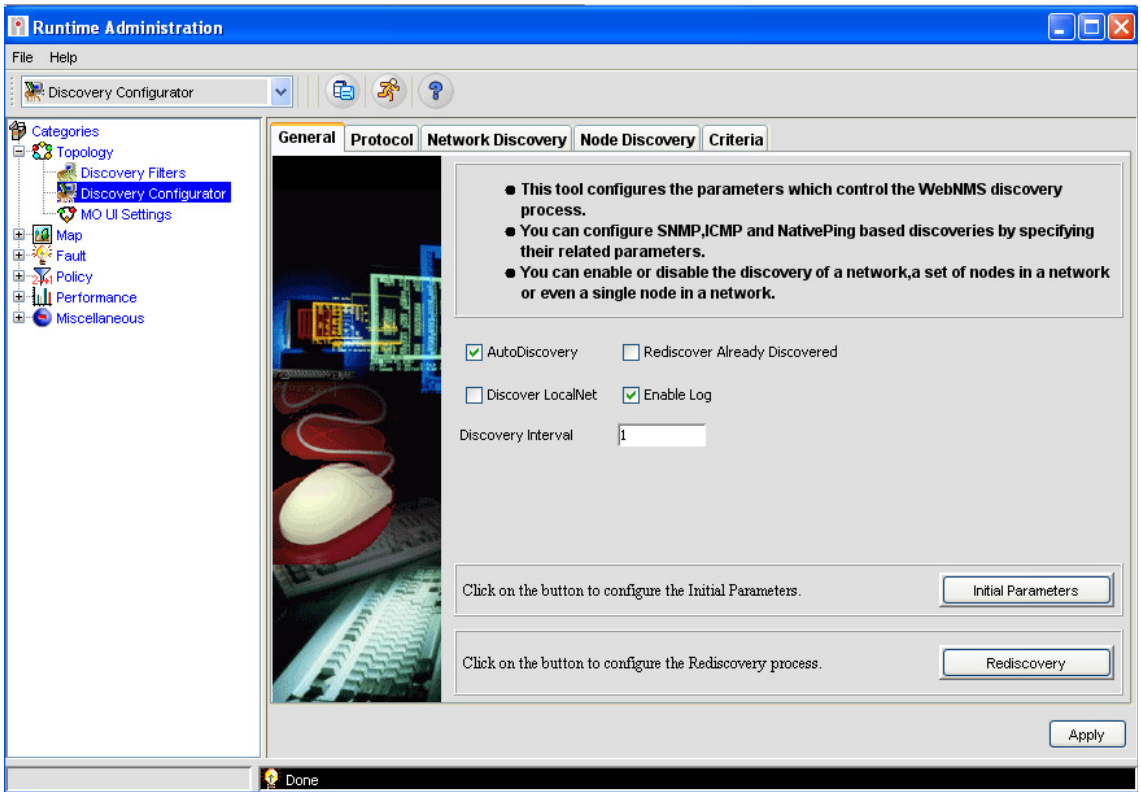


Figure 3. Discovery Configurator for Nimbra Vision.

General settings

Under the General tab, the following settings can be made:

Discover LocalNet. This setting should be disabled. The server could be located outside the management network, in which case it is not interesting to discover and manage the local net using Nimbra Vision. Also, SNMPv3 parameters need to be configured for discovery, which cannot be done here.

Rediscover Already Discovered. There is no need to rediscover already discovered nodes. This setting should be disabled.

Discovery Interval. The Discovery Interval is not used during the first discovery after the server has started, only during later discoveries. To set the interval for the first discovery, open the Initial Parameters form.

Configure the **rediscovery scheduler** from the Rediscovery. The rediscovery process discovers new nodes. The default setting of 24 hours is normally kept.

Protocol settings

SNMP Discovery must be enabled. These settings are used as default settings when discovering nodes.

SNMPv3 Discovery should be enabled when SNMPv3 discovery is done. You should not set any value in the User Names and Context Name boxes.

Network Discovery settings

The network could be discovered with SNMPv1, SNMPv2c or SNMPv3. If SNMPv3 is used you need to enable the SNMP checkbox and add SNMPv3 Properties. SNMPv3 discovery is necessary to be able to configure the node from Nimbra Vision.

Select the Network Discovery tab and enter IP address 192.168.234.0 and net mask 255.255.255.0. The host range should be 192.168.234.1 to 192.168.234.20.
Configure correct netmask at all time!
Prevent IP addresses to be discovered to prevent alarms on unreachable addresses

Enable SNMP and click on SNMP Properties. These settings are used as default settings when discovering nodes. Click on Add and enter:

User name: *root*
Context name: (default context, empty string).
Agent Port: 161

Select Security tab and enter

Security level: AutNoPriv
Auth Protocol: MD5
Auth Passwd: *passwd* and then click OK twice. Click on Add and Apply.

Node Discovery settings

Use this tab to add individual nodes for the discovery process.

You can specify nodes that should be added before other nodes are discovered. These nodes are used as seed, and their knowledge of the network is used for further discovery. You would normally not have to enter anything here, but if you like to discover a newly added node entering its IP address and discover a single node is faster than discovery of an entire network. In most cases, when adding a node under this tab, you don't want to automatically discovery its parent network as you would not have SMMPv3 parameters configured for the parent network.

The node shall be added using SNMPv2c, or SNMPv3. If you want to add individual nodes, make sure the Discover Parent Net is disabled. This restricts the discovery engine to add the node only and prevents the complete IP subnetwork to be discovered.

Node Criteria settings

If you need to further add constrains on the discovered network elements use this tab to setup constraints for individual nodes.

It is strongly recommended to setup the Discovery Engine to do SNMPv3 discovery with the SNMPv3 access parameters for networks or individual nodes. Nimbra Vision adds and updates SNMPv3 parameters for the nodes in its database based on the result from the network/node discovery.

Limit the discovery process to only include nodes having specified characteristics, e.g. only Nimbra nodes.

If you only want to monitor Nimbra nodes, check the Allow criteria box and select in the drop down list:

	Drop down list	Criteria
Property name	name	Node*
Property name	type	Nimbra*

Click Apply to make the changes valid to the Discovery Configurator.

Lab. 5 Maps

Goal

Nimbra Vision is an application for managing Nimbra networks. It consists of maps, a network database, an event and alarm database and a number of applications for managing the nodes and the network itself. In this exercise you will get introduced to Nimbra Vision client window and how to work with maps.

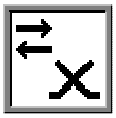
DTM Network

The DTM Network map is a graphical representation of the Nimbra network. The map shows the Nimbra network elements, and their topology with the DTM links. The map does not show the same information as IP maps, although it may show the same network elements. The IP map shows the network from an IP network view.

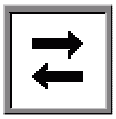
In the tree, navigate to Nimbra Vision - Network Maps and click on DTM Network – DTM Network: The DTM Map contains all the Nimbra network elements and their link connections.

Symbol

Look at the different symbols and their colors. The DTM Network shows all discovered DTM network elements and their links. The elements are represented by symbols and different symbols represent different types of network elements.

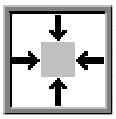


Nimbra One



Nimbra 340, Nimbra 340HD, Nimbra 360

Nimbra 680



Unknown Nimbra

The color of the symbol represents the status of the network element. This is the highest severity of an active alarm in the node or a color (grey) representing unknown if the network element is unmanaged.

Link

Rearrange the symbols on the map so that you have a good view of the network. Notice how the links are like rubber bands when you move the symbols. (Use right mouse button to move multiple selected symbols) An arrow on the link shows the direction of the link. The color of the link reflects the link utilization or status. The thickness of the

link represents the maximum transmit capacity of the link interface. It is possible to show an administrative name for the link in the map. The administrative name is a text sting that you can supply for easy identification of the link.

Background picture, zoom, refresh etc

Change the background picture from `graybg.png` to `worldmap.gif` with menu **View | Symbol properties**. Change the Image name.

Save the changes to the server so that the changes are available to others or to you next time you log in. Menu: **Custom Views | Save** or the save icon.

Try some other functions:

- Try the zoom and refresh .Try the Zoom Window
- Try the group and ungroup.
- Try to detach and attach the map window; use the toolbar button or menu **File**.
- Examine the object and symbol properties, by right clicking on the symbols and links. Notice the Object menu that changes depending on what object that is selected.

Right click on of the symbols in the map. (Or select the DTM network element in the map, or in the network database.)

Click on Symbol properties. It will open a dialog to modify the properties for the map symbol.

Click OK to apply the changes and close the dialog, or click Close to close the dialog without applying any changes.

Adding a DTM Map

Invoke the Add Map Property pop-up menu from **Custom View | Add New Map (DTM Map)**, or the **Add Map** toolbar button.

Figure 4. Add map toolbar button.

Fill in the Map Properties,

- The **Name** is name of the map in the database. The **name** has to be **unique**. Nimbra Vision will automatically add ***.netmap*** to the name.
- The **Label** is the name that will be displayed in the Tree.

Specify the match criteria to select what managed objects that will be included in the map.

- Check **Create custom** map if you want the map to automatically be populated with symbols and links according to match criteria. Or uncheck Create custom map if you want to create an empty map. You will in this case have to add symbols and links to this map manually. You can do this by cut-and-paste from other maps.

- **Name** is the match criterion for selecting which managed objects that will populate the map. Knowing that the names of links are based on the node's names makes it easy to specify a criterion. E.g. *Node1** or *NY1**

- **Type** is a match criterion for the type of managed object.
  E.g. *Nimbra3** and *DtmLink.*

Create a map that will match all the DTM nodes and links.

- For the single criterion, the property has to match any of its rules. The rules can be specified in a **comma-separated** list. You can use the **asterisk** (*) as a wild card, both in the beginning, within or at the end of a match rule. **Exclamation** (**!**) can be used to negate. If the property does not exist for a managed object, it is not considered as a match.

Click **Save** to add the map. A node is added under the Network Maps node in the Tree.

After the map has been created, you can modify the Criteria Properties to add additional criteria. To do this, open the Custom View properties for the map and add additional criteria. To open the Custom View properties, click the **Properties** toolbar button without having any symbol selected.

Figure 5. The Properties toolbar button.

Add a map for Node1 and Node 2 include the link between them

To put these two nodes on a customer specific map, proceed as follows:

1. Navigate to the **Network Maps | Nimbra Network**. Right click and select the menu C**ustom View**. Click on Add New Map.

2. Enter:
   Name: N1-2 (name in **db**)
   Label: Node1-Node2 (name in **tree**)
   Name: node1, node2,*_node* (the name of the nodes and its link)
   Type: Nimbra*, DtmLink

Add a Hierarchical Map using Map Group

By having a symbol in the map representing another map, e.g. a sub-map, you can open the sub-map from the parent map. The opened map is displayed in a separate window. Because the sub-map is created separately the parent map, it can be referenced from

other maps as well as from the Tree. The map properties for the sub-map are used by sub-map, and are not affected by the parent map's properties. This means that your sub-map can have its own background image, topology, reindeers, criteria properties etc. However, you will have to create all the links to/from the sub-map symbols in the parent map manually. The color of the symbol is not affected by the severity of the objects in the map. Using map symbols, you can create hierarchies with any depth.

1. Open the map

2. Select the symbols and links that shall be part of the group.

3. Select the **Group Selected Symbols** tool in the map toolbar. The group is created. Right click and look at the symbol properties. Note the name of the group.

Figure 6. Group selected symbols button.

4. Right click on the group symbol and select Ungroup. Include additional nodes as you like and form a new group with additional elements.

Failed systems

Navigate to **Application | Network Maps** and click on **Failed System**.
Failed Systems is the Failed Systems map includes all failed network elements, defined as network elements with status severity *Critical* or *Major*.

Lab. 6 Network Database

Goal

In this exercise you will familiarize yourself with the network database, and the properties for the different types of managed objects.

Network Database

The Network Database maintains the properties of all Managed objects of a network. These managed objects (nodes, links, networks etc) and their object properties are listed under the Network Database in the tree structure to the left. The properties of the various Managed Objects can be found through the menu specific for the selected object. Select the object type under Network database in the tree structure and select the object in the list produced. Right click on the object and select ‘managed Object Properties’.

By default, sets of **Custom Views** are defined for the Network Database.

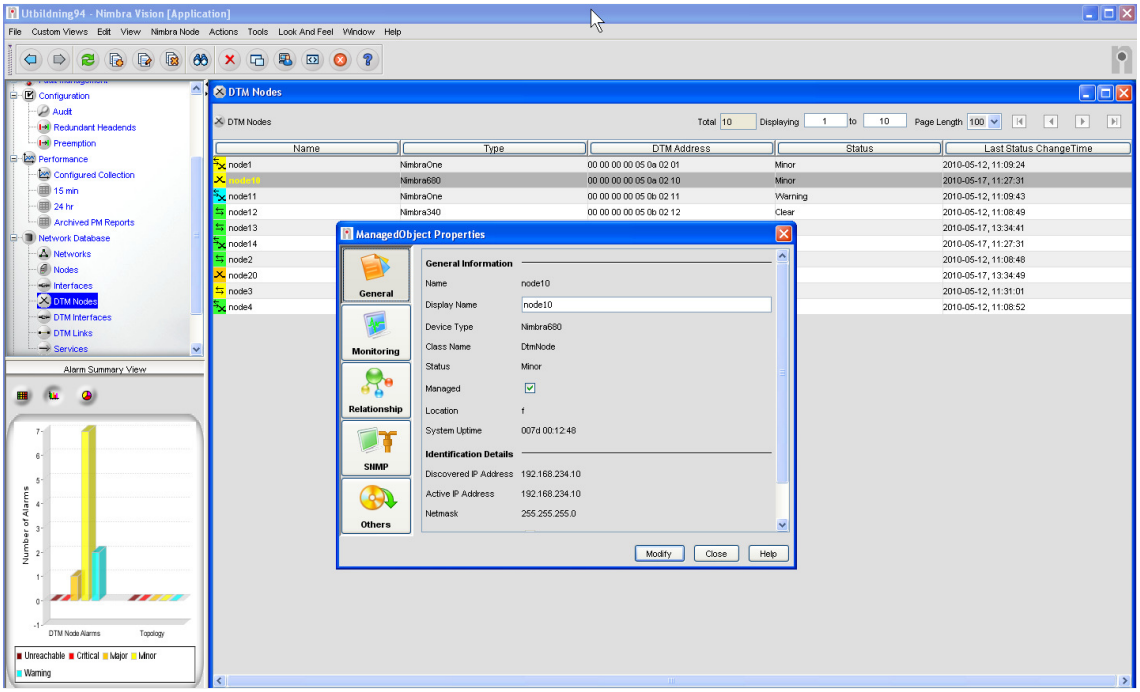


Figure 7. Managed object properties.

The dialog **Managed Object Properties** is a generic function that displays all the properties about a managed object in the database. The dialog is a generic and its function is the same for all the managed objects regardless of their type or class, although its content depends on the actual managed object. If the properties of the managed object are modified, the database is updated but the changes are not forwarded to the network element itself. Generally, the dialog is not used for changing node information and for that reason access to save edited data should be disabled for most users.

Note! *The property names are case sensitive, and start with a lower case letter. In the property form, a more descriptive label replaces all property names. Use the on-line help to view the available properties for an MO, or the context-sensitive help button on the dialog.*

Nimbra Node Properties

The Managed Object **DTM Node** contains properties for DTM network elements. To open the Managed Object Properties dialog, select the object in the database (**Network Database | DTM Nodes**) and select menu **Nimbra Node | Managed Object Properties**, right click on the object to get menu as a pop-up or double-click on the object itself.

Look at the properties. Look at all the pages to get an idea of what type of information that available.

Nimbra Interface Properties

The Managed Object **DTM Interface** contains properties for DTM interface.

Open the Managed Object Properties dialog; select a managed object in the **Network Database | DTM Interfaces** custom view. Look at the properties. Look at all the pages to get an idea of what type of information that available. The available operations depend on your permissions, as defined by the administrator.

Nimbra Link Properties

The Managed Object **DTM Link** contains properties for DTM link connecting two Nimbra interfaces in two Nimbra nodes.

Select a managed object in the DTM Links custom view, and select the menu **Managed Object Properties** by right clicking on the link. Look at the properties. Look at all the pages to get an idea of what type of information that available.

IP Network Properties

The Managed Object **Network** contains properties for IP networks. Select a managed object in the Networks custom view, and select the menu **Network | Managed Object Properties**. Look at the properties. Look at all the pages to get an idea of what type of information that available.

Example - Custom View for specific nodes

Create a custom view for all nodes except Node 10 and Node 20.

In order to create a custom view, navigate to the Network Database | DTM Nodes, right click and select the menu Add custom View. Enter ‘Filter View name’ and ‘Parent Name’ (DTM Database). Under ‘name’ filtering is made on node names, i.e. all nodes satisfying the stated condition are included on the map. Under ‘type’ filtering is made on node type (example nimbra* includes all nimbra nodes). To include all nimbra nodes

except nodes 10 and 20, let ‘type’ be nimbra* and name = !*0 (not ending with 0).

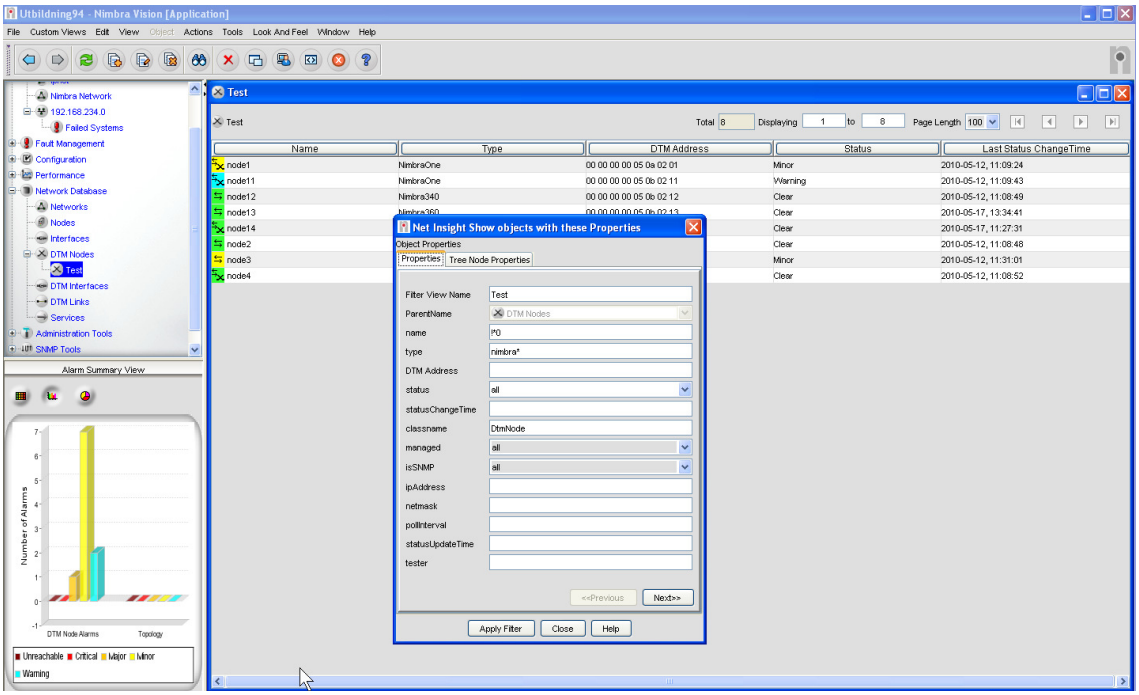


Figure 8. Custom view without nodes 10 and 20.

Create one custom view excluding all Nimbra 680s and the node ‘node 1’

Enter properties:

Filter View name: Nimbra
ParentName: DTM Database
name: !node1
type: !Nimbra680

Custom View for Node11 and for its interfaces

Enter properties:
Filter name: DTM Interfaces
ParentName: DTM Interfaces
Node name: node11
classname: DtmInterface

Lab. 7 Manage/Unmanage

Managing a network element means that you are making Nimbra Vision monitor it. Unmanaging a network element stops Nimbra Vision from monitoring the element. When a node is unmanaged, Nimbra Vision does not periodically poll the element for its status. Nimbra Vision ignores SNMP notifications from the node that otherwise would result in some kind of status update, including alarm updates.

When the status is changed from unmanaged to managed, Nimbra Vision will immediately update the status of the node, which in turn typically results in a refresh operation.

You can perform the **Manage/Unmanage** operation on an individual network element, or on a complete IP network. On an IP network, all the included network elements are affected.

Note! A node might be connected to multiple IP networks!

When a network element is unmanaged, its status becomes unknown, which is indicated with gray color.

1. Select a DTM Node in the Network Database or the map.

2. Select menu **DTM Node | Manage/UnManage** to toggle the status

3. At the end of the exercise, restore the status to Manage.

Lab. 8 Delete and Add Nodes

Goal

In this exercise you will learn how to delete a managed object, such as a node, link or interface, from the database. You will also learn how to add a node or network to the database without using the discovery function.

Select a node in the Network Database and delete it using **DTM Node | Delete Object and Traces**. Confirm in the pop up window. The node with all its links, interfaces, alarm, events and collected data is deleted from the database.

Add the node again from the Discovery Configurator or from the Network Database. To add from the database directly, use **Edit | Add Node**. In the opened window, add the node (use the node name as configured in the *hosts* database or the IP address).

Note! The node shall not enable SNMPv3 discovery here! If the Discovery Configurator is setup with the node as part of an IP subnet configured for SNMPv3 discovery, or as a node with SNMPv3 discovery, then the node will be SNMPv3 discovered.

Lab. 9 Start/Stop Discovery

Goal

In this exercise you will learn how to restart the discovery process to quickly find new nodes in an already existing IP network.

1. Select e.g. node4 and delete the node, as you learned in previous exercise.

2. Select the network in the Network Database, and select menu **Network | Start Discovery** by right clicking on the network.

3. The node is re-discovered.

Lab. 10 Centralized Inventory

General

Nimbra Vision supports centralized inventory of all network elements in a Nimbra network. Inventory data is automatically discovered and stored in the Nimbra Vision database. The data includes all Field Replaceable Units (FRU) from all network elements, such as hardware modules, application packages, software, etc.

Inventory data is searchable with the result presented in a sortable table. Using this search function it is possible to find where a certain type of FRU is installed. It is possible to configure what information (columns) to be displayed in the resulting table. Inventory objects and their relationship may also be browsed per network element in a tree structure, where nodes may be expanded and collapsed.
The following topics describe the function in more details:

- Search/Browse Inventory Database
- Inventory Search Result
- Inventory Properties

Goal

In this exercise you will learn how to search the inventory. It could be done from the database or from the map.

Search inventory database

To search the inventory database, select a network map or an item like a network in the network database. Go to the menu **View | Inventory Search**… . With this function, you can enter criteria for any inventory property.

Example with following search criteria: **Node**: node*, **Type**: sfp. One entry (row) is selected and the ‘Details’ button is chosen. In the picture below, both windows are shown. **Display column**, if ticked, then the column is displayed in the tabular search result.

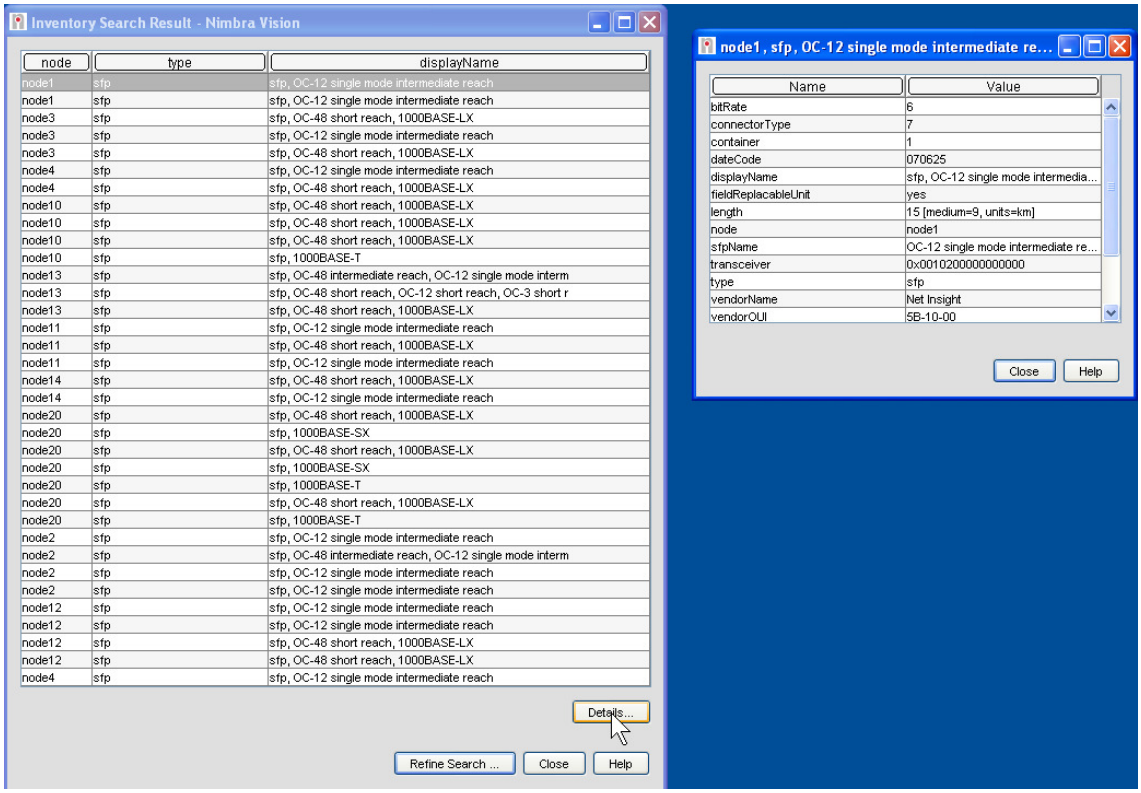


Figure 9. Inventory search with details.

Inventory browse is similar, but the database output is shown in a different way:

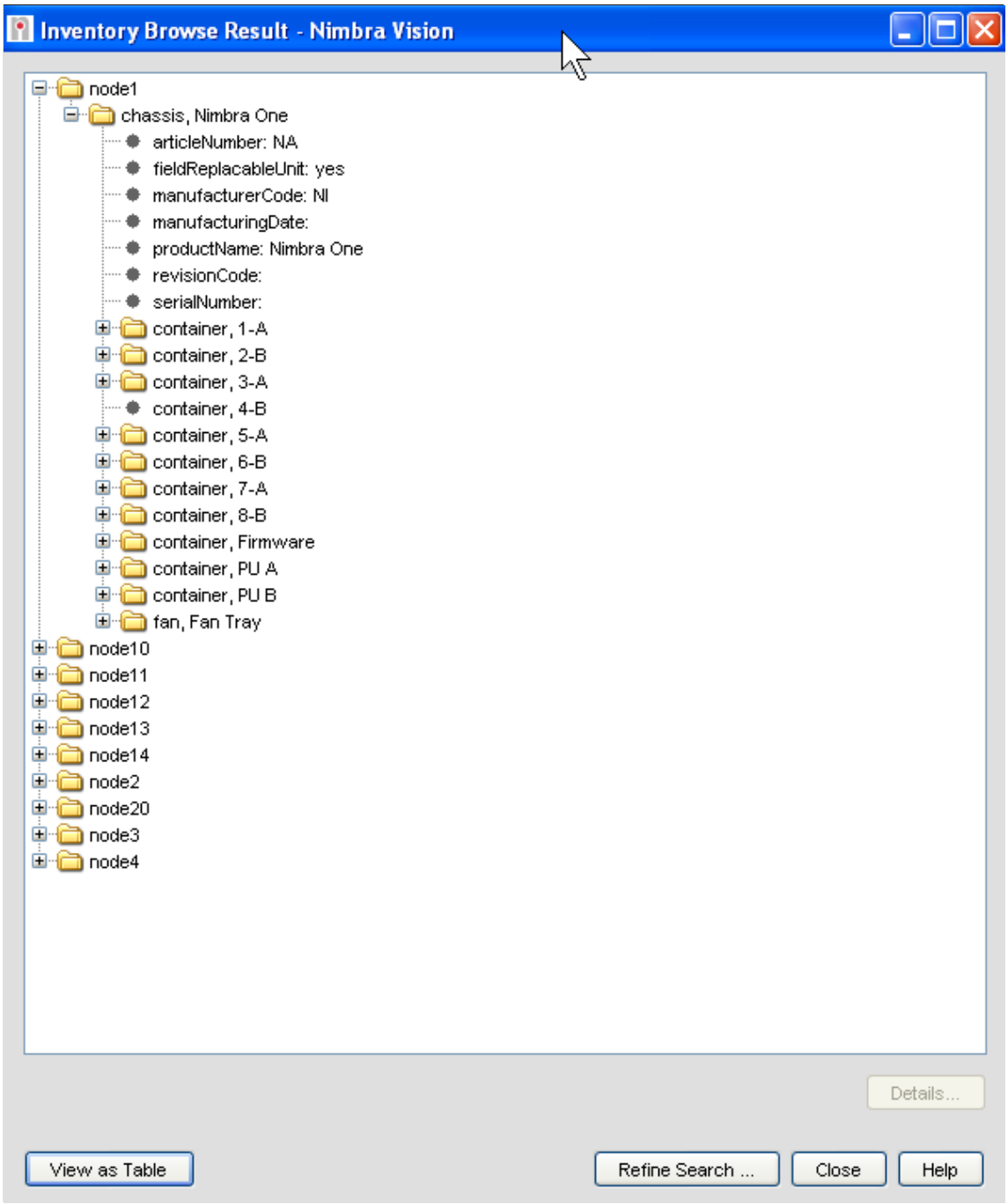


Figure 10. Inventory browse

Lab. 11 Operations on Nodes

Goal

In this exercise you will familiarize yourself with the different operations that you can do on the nodes.

Exploration of possible actions

In a network map or the network database, select a node and right-click on the mouse. The available choices are presented below:

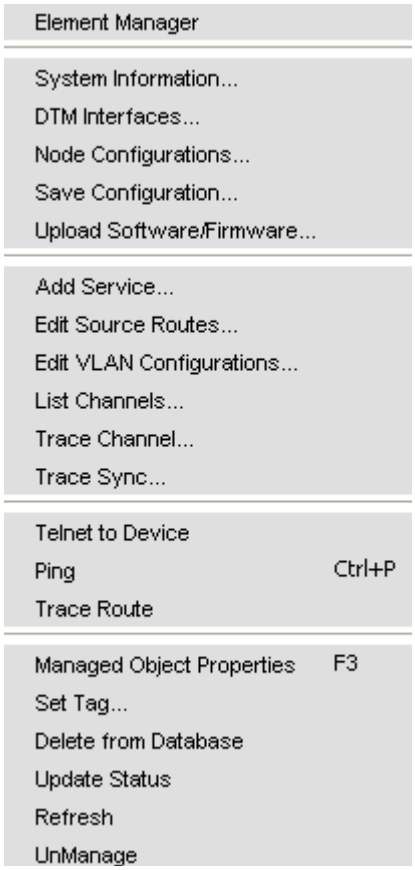


Figure 11. Node menu is available with a selected node and a right-click on the mouse.

Element manager opens the graphical web interface to the selected node.

System Information opens a dialog window, with three parameters to enter. They are

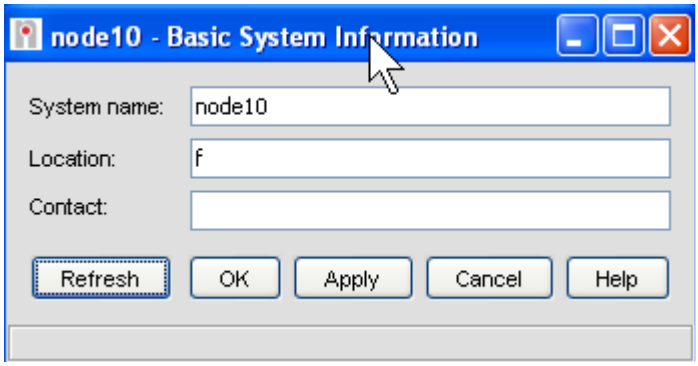


Figure 12. Basic System Information

system name, location and contact. All parameters are character strings stored in the node. The strings typically contain information about the node. A simple way to check the SNMP write settings is to add a nonsense string (like the 'f' for location in the illustration).

DTM Interfaces lists all DTM interfaces on the node and some of their properties.

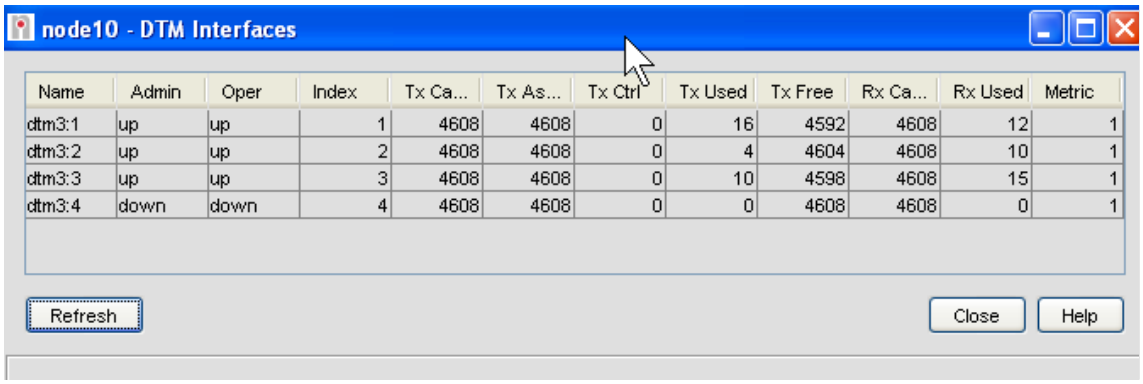


Figure 13. DTM Interfaces

Node Configurations lists all available node configurations. It is possible to select one or more configuration(s) and enable/disable the selection, delete configurations in the node or save the configurations on the node.

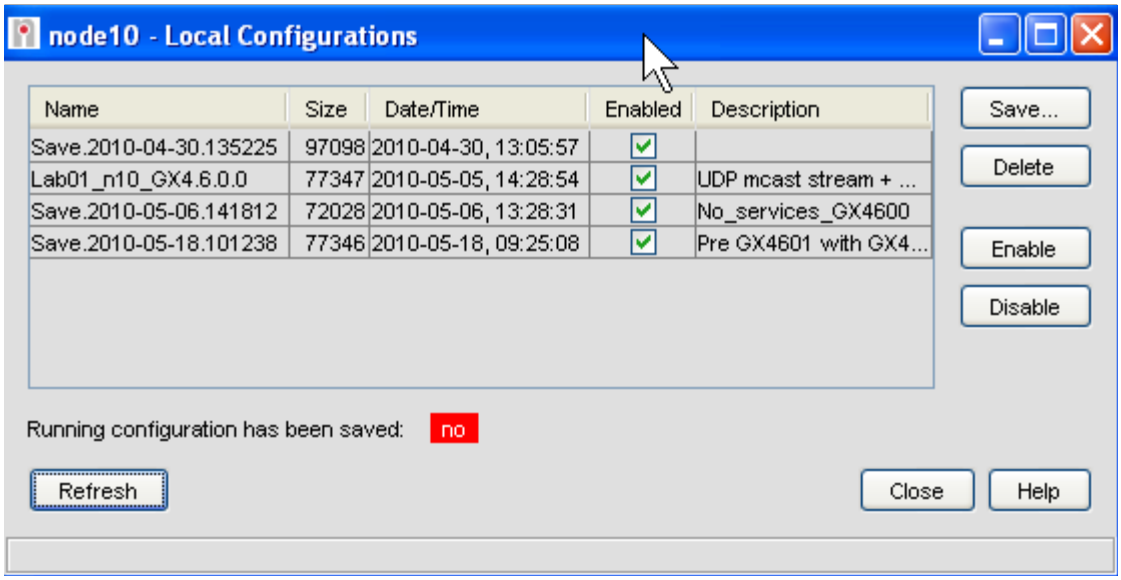


Figure 14. Node configurations

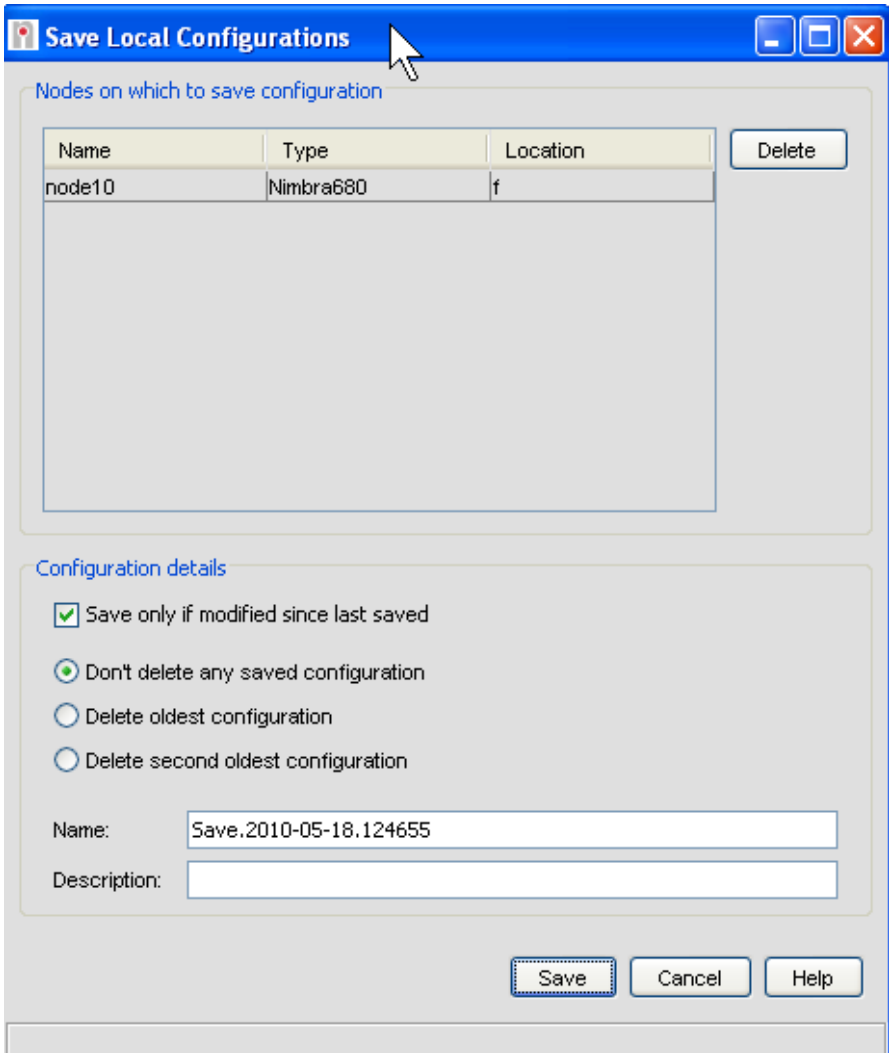


Figure 15. Save configuration

Save configuration gives the user an opportunity to save the configuration file to the node. A configuration name and description can be entered here. Here, it is also possible to remove an old configuration to ensure that the save operation is allowed.

Software/Firmware upload gives the user a quick way to upload new system release software to the node. A repository of the version of the system release software must be available from the node. The repository is defined under

1. Look at: **Boards:** Present a list of boards on the network element. The window shows a table with data about the network element's boards:

    - **Pos**. The shelf position where the board is mounted.
    - **Description**. The description of the board.
    - **Software rev**. The software revision of the board or entity, if it can be determined.
    - **Hardware rev**. The hardware revision of the board or entity, if it can be determined.
    - **Firmware rev**. The revision of the board's firmware, if it can be determined

2. Look at:: This will be explored more in a later lab (Lab. 13 Local Configuration Files). Manage configuration files on the network element.

3. Look at: **Save Configurations**: This will be explored more in a later lab (Lab. 13 Local Configuration Files). Save the current configuration on a network element on a local file. You can select multiple network elements to perform the operation on multiple network elements.

4. Look at: **Originating Connections**: Present a list of all the connections that originate on the network element.

5. Look at: **Terminating Connections**: Present a list of all the connections that terminate on the network element.

6. Try: **Element Manger**: Opens the web browser and loads the network element's element manager. The web browser is opened on you local client PC, but the server will provide a valid IP address.

7. Try: **Telnet**: Opens a telnet session to the network element for Command Line Interface (CLI) access. The telnet session is opened from the Nimbra Vision server; only the display is on the local client PC.

8. Try: **Ping**. Sends ICMP ECHO_REQUEST packets to the network element using the management network. The **Ping** operation sends ICMP ECHO_REQUEST packets to the network element, and displays the result in a window. **Ping** can be used to check connectivity to a remote network element on the IP network.

9. Try: **Trace Route**: The **Trace Route** operation print the route packets take to a network element on the IP management network. The information is displayed in a window. **Trace Route** can be used for trouble shooting problems in the management network.

Note! ***Ping*** *and* ***Trace Route*** *are using the IP network, not the DTM network. It does not operate on the DTM network level, and is not directly affected by the status of the DTM network. However, if DLE in-band management network is used, the DTM network and the status of the DLE service affect the IP network.*

10. Try: **Refresh**: Reads all the information from the network element and updates the database and maps.

11. Don't try: **Delete Object and Traces**: This was already explored in earlier exercise (Lab. 8 Delete and Add Nodes). Deletes the network element from the database, including its DTM interfaces and DTM by-pass link connections.

12. Try: **UnMange/Mange**: The network element is ignored when it is unmanaged.

Lab. 12 Operations on Links and Interfaces

Use the **DTM Link** menu to access the operations on the link.

Operations on DTM interfaces are accomplished from the link symbol in the map using the **DTM Link** menu, or from the interface object in the network database. This was explored in earlier lab (Lab. 6 Network Database) using the **DTM Interface** menu.

Goal

In this exercise you will familiarize with operations that you can do on interfaces and links.

1. Look at: **DTM Interface** configuration dialog allows you to enable or disable a single DTM interface on the network element. A DTM interface is responsible for the allocation of capacity on a link that is originating from the interface.

   Warning! *Changing the configuration of an interface affects the services that use the interface. It could also affect the in-band management network, resulting in that you could potentially loose contact with the network element.*

   - **Interface name**. The name of the DTM interface, local to the node. The format of the name is normally the prefix *dtm* followed by the equivalence to the physical board position and the port position on the board, e.g. *dtm6:1* for port #1 on board in position #6. The interface name is normally analogue to the trunk interface naming.
   - **First slot**. The first slot of the slot range that shall be used by the by-pass chain that is originating on the interface. Note that the first slot (i.e. slot 0) is always used by the system and cannot be allocated by the user.
   - **Last slot**. The last slot of the slot range that shall be used by the link originating on the interface.
   - **Number of ctrl slots**. The number of slots allocated for a control channel. The control channel is allocated from the slot range configured for the interface.
   - **Used slots**. The number of slots that are currently used by the link originating on the interface. This includes slots for the control channel and the services.
   - **Max slots**. The maximum number of slots that the interface is capable of.

   The receive area contains status parameters for the receive part of the interface.

   - **Used slots**. The number of slots that are currently used on the interface. This includes slots for the control channel and the services.
   - **Max slots**. The maximum number of slots that the interface is capable of.

DTM Link

The DTM Links window shows data about a DTM link. The links is actually the *DTM by-pass link connections*, which is the part of the *DTM by-pass chain* that connects two adjacent nodes. When a DTM interface corresponds to exactly one trunk interface, the

DTM link represents the physical connection between two adjacent nodes. The color of the link describes its status as:

- **Green** – the link is up. This means that a connection exists between the two DTM interfaces.
- **Aqua** – the link status cannot be determined because the originating node is unreachable.
- **Red** – the link is down. This means that an earlier detected DTM link cannot be detected anymore. (Links are not automatically removed from the map.)

The thickness of the link represents the maximum transmit capacity of the DTM by-pass link's originating interface. The default value is dashed (indicated as zero pixel width) for capacity below 85 slots, one pixel up to 1940 slots, and three pixels for higher capacity.

2. Look at: **Dtm Link**:

- **Admin name**. This is an administrative name for the link. When the link is created, the system assigns an administrative name to the link. This is a property of the DTM Link managed object, which can be changed by the user.
- **Originating interface**. The name of the originating interface.
- **Terminating interface**. The name of the terminating interface
- **Used capacity**. The capacity that is used by the originating interface for connections that originates on its node.
- **Configured capacity**. The capacity that is available to the node of the originating interface. This is the capacity that has been configured on the interface and that can be used by the originating node. On a point-to-point connection, this would be the full interface capacity. On a bus or ring, the total interface capacity would be distributed among the nodes in the by-pass chain.
- **Usage bar**. The usage bar shows the ratio of used capacity compared to the configured capacity. This is the load of the link.

Delete Link

3. The **Delete Object and Traces** operation deletes the DTM by-pass link connection from all maps, and its object from the database

If a link cannot be detected, it is because the link either is removed or because it is down. Nimbra Vision does not automatically remove links from its database when they cannot be detected any longer. Instead, the links gets their valid status changed from *true* to *false*. You can use the **Delete Object and Traces** command to remove the links that should not be managed any longer.

If a removed link is detected again, it will re-appear in the DTM Network map, and in the Network database. A link is detected when its status is changed, or when the managed object is refreshed.

Lab. 13 Local Configuration Files

The Local Configurations window allows you to manage local configuration files in the node. A configuration file contains the complete configuration of the node. This includes the configuration of any services. When the node is booting, it reads the newest configuration file that is ***enabled***, and configures itself accordingly.

A node may have multiple configuration files. The maximum number of saved configurations on a node is nine.

Goal

In this exercise you will learn to manage and save configurations in the network elements.

Managing Local Configuration Files

1. Open the window, select a node in the DTM Network map or in the Network Database, and select the object menu **DTM nodes | Node configurations…**. The window shows a table with all the configuration files and their attributes:

   - **Name**. A name of the file. The name must be unique among the node's configuration files.
   - **Description**. A textual description of the configuration.
   - **Created**. A time stamps when the configuration file was created. The node creates the time stamp when it saves its configuration. The node uses its local real-time clock.
   - **Size**. The configuration file's size in bytes.
   - **Status.** The status of the configuration file. A configuration file may be ***enabled*** or *disabled*. When the node boots, it is reading the newest configuration file with status *enabled*.
   - **Running configuration has been modified since it was saved:** This indicates that the node's configuration has been changed, and that it has not been saved to a configuration file. Note that this does not indicate that a saved configuration exists matching the running configuration.

2. Click **Save**… to save the node's current configuration into a new configurations file and giv it a name. The file will have the status *enabled*. This means that the node will use this configuration file next time it is booting.

3. Verify that the configuration is in the list.

4. Click **Delete** to delete the configuration file that is currently selected in the table.

5. Click **Disable** to disable the configuration file that is currently selected. The node ignores a disabled configuration file.

6. Click **Refresh** to update the window. The information is retrieved directly from the node. Use Refresh if you suspects that someone else has modified the table since the window was opened.

Save Local Configuration on Multiple Nodes

The dialog Save configurations on multiple nodes allows you to save the current configuration of multiple nodes to local files.

For each node, its current configuration will be saved in a local file stored on the node. Note that there is a limit of the number of configurations that can be saved on a node.

1. To open the window, in the DTM Network map or the Network Database, select all the nodes for which the configuration shall be saved, and select the object menu **DTM Node | Save configurations…**.

   A list is shown. The list contains all nodes for which the configuration shall be saved. The list contains all the nodes that were selected in the DTM Network map or the Network Database when the window was opened.

   - **Name**. The name of the configuration file. The name must be unique within the node. The field will contain a suggested name that should be unique. The same name will be used on all nodes.

   - **Description**. A textual description of the configuration.

2. Click **Delete** to remove a selected entry from the table. This could be used if you, when you opened the window, selected a node for which you don't want to save the configuration.

- **Save running configuration only if it has been modified** since it was last saved. The function checks if the current configuration in the node has changed since it was last saved. If it has changed, the configuration will be saved. If it has not changed, the configuration is not saved.

- **Do not delete any saved configuration**. The existing configurations on the node are untouched.

- **Delete the second oldest saved configuration**. The second oldest configuration is removed instead of the oldest. This can be used to keep one configuration (the oldest) as a fall-back configuration that is always available.

3. Click **Save** to save the current configuration on all the nodes in the list.

Lab. 14 Alarms

An alarm is generated when a fault or failure is detected. Most of the alarms in a Nimbra network is detected and reported by the network element and then forwarded to Nimbra Vision. The alarm database does thus become a collection of all the alarms from all the managed network elements.

In addition to the alarms generated by the network elements, Nimbra Vision can generate alarms when it detects failures. This would typically be Typology failure that is generated when Nimbra Vision fails to connect to a managed object. It is also possible to monitor individual SNMP objects, and generate an event when its value crosses a threshold.

Alarms are built up from events. An event is generated as a result of that something is happening in the network or in the management system. An SNMP notification is normally converted to an event. If the event represents an alarm, the event will result in creation of an alarm.

From an alarm, you can see all the events that have affected the status of the alarm. Some types of events that are logged are:

- Generation and clearing of alarms
- Switching of sync source
- Modifications of node configurations (Object modified, created or deleted)
- Modification of DTM topology
- Detection of lost traps
- Node refresh
- Network or node added to or deleted from the database

Alarm Manager

The alarm manger displays alarms (also known as alerts). Alarms are correlated network events. You can view events in much the same way as you can view the alarms.

1. Explore the alarm manager, open the **Fault Manage | Alarms**.
2. Examine the window, sort alarms by selecting a column. You cannot sort on all columns.
3. Look at the “Alarm Summary View” at the bottom left of the client window. Clicking on different items in the “Alarm Summary View” opens the alarm list with related alarms.
    - Look at “Totals”, look at different views (Table, Bar chart, Pier chart)

- Open the alarms with specific category by selecting the category.
- View alarms by severity by selecting the severity Critical/Major/Minor/Warning/Clear.

4. Open the alarm manager of a set of nodes by selecting some nodes in the "DTM Map", and use menu **View | Alarms**.
5. View alarm details by opening an alarm: select an alarm and choose **View | Details** (or double-click).
6. **View | Events** to se which events that build an alarm.
7. Generate some alarms: Shut down a node; pull a fiber etc. (Ensure that the configuration on the node is has been saved before shutting down the node). Notice the received alarms, and that the links to the node is becoming red. Also note that after a while, a Topology alarm is raised and the node is turned red.
8. Re-start the node again. The alarms shall be cleared, the links turned green again and the Topology alarm cleared.

Some alarms can be suppressed in the node. Alarms on trunk interfaces can be suppressed. You will still receive alarms in the DTM interface.

9. To suppress alarms from the trunk interface, using the node's element manager, navigate to a trunk interface and check suppress alarms.
10. Disconnect the fiber terminating on the interface. Notice the differences between the alarms when "Suppress alarms" are enabled or not.

Source:
Severity
message
failure object

Additional criteria:

Property Name	**Match criteria**
type	communication equipment
purpose	SDI* customerX
cause	ReplaceableUnitMiss LossOfSignal ServiceUnavailable PowerProblem

Property Name	Match criteria
objectName	ets* Itsi* Sonet/sdh*

Alarms, Custom views: Node Name

In this exercise you will create a custom view, which will only match alarms for the node type Nimbra One. The filer should select only node Node1, node4, Node11and node14.

1. Navigate to **Fault Manage | Alarms**. Right click and select Add Custom Views.

2. Enter:
   Filter View Name: Nimbra One alarms
   Select type of **severity** to: Critical
   Failure object: (1.4.1.2928.6.2.16.1.1.2.1.2.11/1/29)
   Source: node1, node11, node4, node14

3. Select all the alarms regardless date. Click on *Apply filter*.

4. Verify the custom view.

Create also a custom view, which will only match alarms for the Nimbra 680.

1. Navigate to **Fault Manage | Alarms**. Right click and select Add Custom Views.

2. Enter:
   Filter View Name: Nimbra 680 alarm
   Select type of **severity** to: Critical
   Source to: node10, node20

5. Select all the alarms regardless date, *Apply filter* and verify it.

Alarms, Custom views: Specific Alarm type

In this exercise you will create a custom view, which will only match a specific type of alarms, and for all nodes, type: Node*.

1. Navigate to **Fault Manage | Alarms**. Right click and select Add Custom Views.

2. Enter:
   Filter View Name: Critical alarms
   Select type of **severity** to: major
   Source to: node*

3. Specify a 10-minute long period for the alarm.

4. Verify the custom view.

Alarms, Custom views: Match criteria for PM data on a specific interface

In this exercise you will create a custom view, which will only match PM data a specific interface. PM on interface sonnet/sdh-2:1

1. Navigate to **Fault Manager | Alarms**. Right click and select Add Custom Views.

2. Enter:
   Filter Name: major alarms
   Select type of **severity** to: *
   Source to: node1*

   Click on additional criteria:

Property name	**Match criteria**
cause	ServiceUnavailable
objectName	sonnet/sdh-2:1

3. Verify the custom view.

Lab. 15 Alarm Actions

Goal

In this exercise you will learn how to trigger actions on receiving alarms (and events).

When an alarm is raised or cleared, Nimbra Vision can execute an action. It is possible to define the criteria for selecting the alarms that will trigger the action. It is possible to define multiple actions for one set of criteria.

In this exercise, you will create an action that will show a message on the screen. The action will be executed for all major and critical alarms form any of the nodes *node01*, *node03*, *node04* and *node05*.

The data for the alarm action can include any property from the alarm. To designate a property, use its name perpended with a dollar sign (**$**). To find out what properties that exist, see the help chapter "Working with Alarms" in the Nimbra Vision Guide.

Creating a simple Alarm Action

1. Open the **Alarms** panel from the tree.

2. Open the Alert Filters using menu **Edit | Configure | Alarm Filters**.

3. Create a new filter with the button **Add** from the **Alert Filter** sub-panel

4. Enter **filter name**.

5. Enter **Match Criteria** for the filter.
   The criterion **Source**: *node1** to match the network elements
   Severity: *critical,major*.
   (Generally, if you want to include a property not listed in the criteria, use the **Advanced** button and add the property.) See the *Web NMS User's Guide*, *Appendix F: Custom View Properties*, *Tips and Tricks* for details on how to write rules.

6. Add a filter action with the button **Add** from the **Add action** panel.

7. Select the type as **Run Command Action** press **New**.

8. Configure the action. As command, set the string as below. This will show a pop-up message. (For this to work, the Windows must allow message pop-ups.)

   ```
   msg * Alarm from $source: $message
   ```

9. Click **Apply**.

10. Try the filter by generating some alarms.

You can do the same type of filtering on events!

Creating a simple Alarm Action, Trap action

1. Open the **Alarms** panel from the tree.

2. Open the Alert Filters using menu **Edit | Configure | Alarm Filters**.

3. Create a new filter with the button **Add** from the **Alert Filter** sub-panel

4. Enter **filter name**.

5. Enter **Match Criteria** for the filter.
   The criterion **Source**: *node1** to match the network elements
   Severity: *critical,major*.
   (Generally, if you want to include a property not listed in the criteria, use the **Advanced** button and add the property.) See the *Web NMS User's Guide*, *Appendix F: Custom View Properties*, *Tips and Tricks* for details on how to write rules.

6. Add a filter action with the button **Add** from the **Add action** panel.

7. Select the type as **Send Trap Action** press **New**.

8. Notification Name:
   Trap destination:
   Destination port:
   Trap Community:
   V2Csettings: Trap OID

Creating a simple Alarm Action, Send sms

1. Open the **Alarms** panel from the tree.

2. Open the Alert Filters using menu **Edit | Configure | Alarm Filters**.

3. Create a new filter with the button **Add** from the **Alert Filter** sub-panel

4. Enter **filter name**.

5. Enter **Match Criteria** for the filter.
   The criterion **Source**: *node1* to match the network elements
   Severity: *critical*.

6. Add a filter action with the button **Add** from the **Add action** panel.

7. Select the type as **XXX** press **New**.

Lab. 16 Software and Firmware Upload

General Software/Firmware Upload

It is possible to download a complete software and firmware package to multiple specified network elements in a single command. The network elements are selected from the Nimbra Vision map or the network database. The software to be downloaded is stored in a repository, which is given a name and a URL describing its location. Multiple repositories may be defined for different software and firmware distributions. A distribution typically contains all the software and firmware for all types of Nimbra network elements.

When software and firmware upload is complete, the nodes may either be restarted automatically or manually restarted at a convenient time. The following topics described the function in more detail:

- Installing the Repository
- Manage Software/Firmware Upload Repositories
- Uploading Software/Firmware
- Functional Description of Software/Firmware Upload
- Configure Software/Firmware Upload

Goal

In this exercise you will learn how to upgrade the software of the nodes in the networks.

Prior to uploading, you must install the repository on a HTTP server or server FTP. The network elements must have access to this HTTP or FTP server. To install, unpack and extract the compressed tar file on the FTP server or HTTP server. This will create a folder with the same name as the system release, e.g. GX4.1.2.0. You can use the Nimbra Vision server as a repository server. To do that:

1. Create a sub-folder in the Nimbra Vision home folder (e.g. <NMS_Home>/repos). **http://server:9090/repos/GX4.1.2.2**
   This folder will hold all the repositories.

2. Extract the single file repository to the folder. This creates a sub-folder that contains all the images. You will need to get the file uncompressed and to do this you will need a software such as WinZip. Windows does include software for extracting tar files.

3. Done. The URL to the repository is then http://server:9090/repos/**GX4.1.2.2**.
   http://192.168.234.94:9090/repos/GX4.1.2.2

Nimbra Vision

Navigate to **Tools | Manage Software/Firmware Upload Repositories**…. This opens the dialog to add, edit and delete definitions of repositories.

4. Click on multiple nodes in the map.

5. Disconnect the network cable to one of the nodes in the network that are not acting as gateway. Notice the generated alarms of category *Topology*. How has the **activeIpAddress** been changed? You can still reach the node -- try it with an operation! Generate an alarm by pulling a fiber; you should still receive the alarm!

Lab. 17 Redundant Networks

Goal

In this exercise you will learn how to monitor redundant management networks.

1. Look at the **IPnet** map: Notice the IP subnets and the nodes that are routers. Compare with the map in Figure 1 on page 6. What is similar? What is different?

2. Disconnect the network cable to one of the nodes in the network that are not acting as gateway. Notice the generated alarms of category *Topology*. How has the **activeIpAddress** been changed? You can still reach the node -- try it with an operation! Try generating an alarm, you should still get it!

3. Now, reconnect the cable. Disconnect the cable to one of the routers for the in-band network. Once again, look at the generated alarms, and on the IP map. How has the **activeIpAddress** changed? Can you still reach the node?

4. Reconnect the cables.

Lab. 18 Filter and Search

Goal

In this exercise you will learn how to search for data.

1. Open a view into the Network Database.
2. Open the search dialog with **Edit | Search**.
3. Try some different search operations. Note that the properties displayed in the panel from where the search dialog was opened can be used in the criterion.
4. Try the search function form the Events and Alarms panels, and from a map.

Lab. 19 Performance Monitoring

Goal

In this exercise you will learn how to look at monitored data.

Performance Reports from the network element (G.826)

The reports are generated by the network element, and are after each measurement period sent to Nimbra Vision as an event. The reports are displayed in a Custom View. For the network element to send these periodic reports, you must enable the function in the network element.

1. Enable the sending of periodic reports in the network element for e.g. the trunk interfaces. Also, ensure that events of the type *performance* are generated.

2. Examine the reports, found in the tree as **15 min** and **24 hrs** in the **Performance** node (you will not have any 24hr reports before a new day has started).

Collected Statistics

By default, the used capacity of each DTM interface is collected periodically. This information can be plotted as an on-the-fly generated reports:

1. Open the **Configured Collections** node in the **Performance** node. A panel with all the nodes, and their collections will be displayed. You can limit the list by selecting nodes in a map or network database, and open the panel with the menu **View | Statistics**.

2. Select a node, and select a statistics collection.

3. Plot collected statistics, menu **View | Plot | Collected Statistics**. A window will plot statistics for all interfaces on the selected network element.

Pre-formatted DTM Interface Reports

Using policies, daily, weekly and monthly reports can be created. You will learn how to use the policie Lab. Searching For and Filtering Data

Goal

In this exercise you will learn how to create custom views that filters the information according to your own specification. A custom view can be applied to a list view or to a map view.

By default, sets of Custom Views are defined for the Network Database. You can easily define other Custom Views, or modify the exiting ones. The predefined Custom Views displays the properties that you are most likely interested in for the type of Custom View.

The table below describes the default Custom Views for the Database, from the **Network Database** node in the Tree.

Name	Description
Networks	IP networks. These are also displayed in the **ipnet** map. See IP Network Properties.
Nodes	All network elements, i.e. the managed objects with the property **isNode** set to *true*.
Interfaces	All interfaces, i.e. the managed objects with the property **isInterface** set to *true*.
DTM Nodes	All network elements that are DTM network elements, i.e. managed objects with the property **classname** set to *DtmNode*. These are also displayed in the DTM Network map. See DTM Node Properties for a description of the properties.
DTM Interfaces	All DTM interfaces, i.e. managed objects with the property **classname** set to *DtmInterface*. See DTM Interface Properties for a description of the properties.
DTM Links	All DTM by-pass link connections, i.e. manged objects with **classname** set to *DtmLink*. These are also displayed in the **DTM Network** map. See DTM Link Properties for a description of the properties.

If you open the **Managed Object Properties** dialog from the Network Database for the type of object you will include in the list, the Nimbra Vision client will learn what properties that exists for the type of managed object, and will display these in the dialogs for creating Custom Views.

Custom Views (list view)

In this exercise, you will create a new Custom View in the Network Database.

5. Open a list in the Network Database. The custom view will be created as a child to the currently selected custom view in the Tree.

6. Create a new Custom View with **Custom Views | Add Custom View**.

7. Give the custom view a name, and set criteria for what objects to present in the Custom View. In this exercise, set the **Filter View Name** to *zero*, name to *node0**, and type to **DtmNode**. This will include all the DTM nodes with a name starting with *node0*. See the *Web NMS User's Guide*, *Appendix F: Custom View Properties*, *Tips and Tricks* for details on how to write rules.

8. Select what columns to show in the Custom View.

9. If you want to save the filter for the next session, it must be saved at the server. To save the filter on the server, select **Custom Views | Save Custom View**.

Custom View (map view)

A map may contain rules for selecting which managed objects to include (custom map), or can created without a rule, which means that you have to add all the symbols yourself (you could e.g. cut-and-paste from other maps).

10. Create a new DTM map. This map can include only a sub-set of all the available network elements. Select a map and create the new map with **Custom View | Add New Map (DTM Map)…**.

11. Enter the map name and display name, and set the selection criteria. In this exercise, the map shall be named *zero*, and the criteria for the node names shall be **node0**. Click OK. The map will contain all the DTM nodes with a name starting with *node0*. Note: to be able to see the links in the map, the criterion must match the link names as well, hence the wildcard asterisk in the beginning of the string. See the *Web NMS User's Guide*, *Appendix F: Custom View Properties*, *Tips and Tricks* for details on how to write rules.

12. The new map is added amongst the other maps in the tree.

Lab. 20 Service provisioning

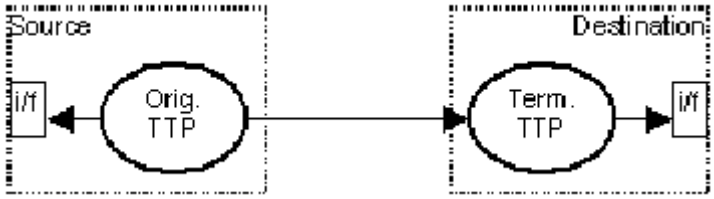
Goal

In this exercise you will learn how to provisioning services.

Service Provisioning is the means of setting up or configuring services in the Nimbra network. Nimbra Vision automatically discovers services when a node is being discovered. All services are added to the database as managed objects with classname DtmService. When a service is updated in the node, Nimbra Vision will automatically update the corresponding managed object in the database.
This means that you can use Nimbra Vision together with the Element Manger or CLI. Actually, when you modify a service from Nimbra Vision, the manage object is updated when Nimbra Vision detects that the service is updated in the nodes.

Note! It is essential that the nodes send config events to Nimbra Vision.

In the nodes, a service consists of a TTP (Trail Termination Point) in the originating node (source node), and a TTP in each terminating node (destination). Access interfaces are associated with the TTP's, either directly in the TTP (for ITS), or associated via VLANs (for ETS). The originating TTP in the node also holds necessary data on capacity, destinations etc. Nimbra Vision represents the service based on data in the originating TTP. This means that Nimbra Vision must know the originating TTP to be able to create a managed object for the specific Service.



Adding a Service

If you select multiple nodes, then the remaining nodes are considered to be destinations, i.e. where the service terminates. The wizard asks for the following information:

- **Source node** is the node where the service originates.
- **Service type** is one of ITS unicast, ITS multicast, ETS unicast or ETS multicast.
- **Source interface** is the ingress interface. This is only specified on ITS services. If an input interface is in use by another service (i.e. if its operational state is up), then this is indicated with [busy] after the interface name.

1. Select a node/some nodes in a map or in the network database.

2. Navigate to **Service | Add Service**….

3. Select source node and click ***Next***. (…. Means that you can fetch a node in the list of nodes.)

4. Select type of service: ITS/ETS unicast or multicast and click ***Next***.

5. Select outgoing interface and click on *Create Service*.

Adding a Source Route

1. Select a node in a map or in the network database.

2. Navigate to **Network Database | Dtm Nodes** select one of the nodes and right click. Select **Edit Source Routes**….

3. This will open a wizard that helps you edit or create a new source routes.

4. Click on *Add* and enter:
   Source Route Name:
   Outgoing interface: Select the correct one in the drop down list
   Select if it is a **loose** or a **strict** route:
   Click on **Add**: enter Node name and interface. Add on nodes until the route is complete.

5. Verify the Source route by clicking on *Verify*. Click *OK*.

List channels in one node

1. Select a node (node1) in a map or in the network database. Right click and select, *List channels…*

2. Select in the node the Interface that you are interested in.
   In: dtm3:2
   Out:dtm2:1

Trace channels in one node

1. Select a node (node1) in a map or in the network database. Right click and select, *List channels…*

2. Select one of the channels and click on Trace Channel. You can also use the channel id, directly in order to trace the channel. (for ex. Channel id 65811).

   (Trace channel from map or Database. In map, select node, right click and select Trace channel. Enter the channel id; 65811)

3. Click on Highlight.

4. Go to the map, to clear high ligt. **Edit Clear Highlight**.

Lab. 21 Policies

Goal

In this exercise you will learn how to work with policies.

You will create and explore a number of polices. To create a policy, select **Policy | Add Policy**.

1. Create and explore the policy: **Save DTM Node Registry.** Notice the similarity with the function **Save Local Configuration on Multiple Nodes**, but using this policy, you can copy a backup of the configuration to Nimbra Vision server. Also, notice how you can filter what nodes to save. This is a scheduled policy, so explore the scheduler as well. You can verify its operation in the tree panel **Configuration | Audit**.

2. Create and explore the policy: **Generate Reports**. Notice how you can create different type of reports. It is possible to generate daily, weekly and monthly reports based on the collected DTM interface statistics. Create and execute the policy, and view the result:

    a. Open the **Configured Collections** node in the **Performance** node (for any node).

    b. Open the reports top page with **View | Reporter Reports**. The page will be shown in the web browser.

3. Create and explore **Host List Push**.

    a. Updates list of DTM host names to DTM addresses.

4. Create and explore the policy: **Statistics Table Cleanup**.

5. Create and explore the policy: **Alert Cleanup**.

6. Create and explore the policy: **Events to Log**.

7. Create and explore the policy: **NMS Backup** (you will try to run this policy in exercise Lab. 25 Backup, Reinitialize and Restore the Database).

8. Create and explore the policy: **Alert Escalation**. You can use the command windows command **msg *user message*** as an action (see Lab. 15 Alarm Actions).

Lab. 22 Pre-emption

General Pre-emption

In network failure situations it is important that sufficient link bandwidth is available for high-priority services to be rerouted. Using the pre-emption function, Nimbra Vision will allow high-priority services to be rerouted by preempting low-priority services, thereby making the necessary bandwidth available.

The user defines the links and low-priority services subject to pre-emption in Nimbra Vision. Upon failure of any of these links, Nimbra Vision will pre-empt all low-priority services. Pre-emption may either be defined as disabling of the service completely or as reduction of service bandwidth (for ASI and Ethernet services). In the latter case bandwidths are pre-configured for Full Operation and Reduced Operation states.

Goal

In this exercise you will learn how to use pre-emption.

1. To configure and edit pre-emption, select the node **Configure | Preemption** This opens a panel with a table containing all configured preemption objects. The panel also has some buttons to add, edit and delete preemption configurations.

2. Click button *Add…* to add a new pre-emption object, or select a row in the table and click button Edit… or Copy… to edit (and copy) an existing pre-emption object. A pre-emption object represents a part of the network, with supervised links, and a set of services that may be pre-empted.

3. Click button *Enable* or *Disable* to enable or disable a selected pre-emption object.

- **Preemption name**: a name of the pre-emption object. This name will appear in the **Configure | Preemption**. You can use any name.

- **Enabled**. If this checkbox I checked, then this pre-emption object will be active.

- **Status**. The status is either *Full Operation* or *Reduced Operation*.

- **Monitored DTM Interfaces**. This is a list of DTM interfaces that shall be monitored.

- **Reduced services**. This is a list of services and their capacity setting when the pre-emption object is in *Full Operation* or *Reduced Operation*. The capacity shall be set in Mbps (or MHz if applicable, e.g. for AES/EBU). If the capacity is set to 0, then instead of changing the capacity, the Administrative state is set to *up* (*Full Operation*) or *down* (*Reduced Operation*).

Lab. 23 Headend Protection

Goal

In this exercise you will learn how to use headend protection

When using a redundant headend, two connections must be configured in the Nimbra nodes: a primary and a secondary connection. The primary connection shall be enabled (operational status up), and the fail-over shall be disabled (operational status down). If the primary connection somehow fails, the function enables the secondary connection and disables the primary connection.
The function monitors the primary access interface and connection status of the headend node. This allows for redundancy on the input data stream, the ingress port and the ingress board. The function also monitors the trunk interfaces on all neighbouring nodes that terminate trunks from the primary node. This allows for node redundancy.
If a fault is detected on the monitored access interface or on the connection, the function will disable the primary connection. This will free network resources and allow the secondary connection to connect. After disabling the primary connection, it will enable the secondary connection, and the service is thus switched over.
If a fault is detected on all supervised trunk interfaces, the function will assume that the node with the primary service is down, and will enable the secondary connection. A periodic status poll would also detect if a node is unreachable, but this is faster. Because the node is most likely down, the function will at this stage not try to disable the primary connection. Instead, the primary connection is disabled as soon as one trunk is detected to be up again, i.e. when the node is likely to be reachable again.
The function makes its decision based on alarms that Nimbra Vision receives from the nodes. It is therefore important that the trap notification receiver is correctly configured on the nodes. Note that the Loss of Signal alarms must not be suppressed on the supervised trunk interfaces.

1. Click on **Add**

The protected service is the service that is monitored:
Source node. The name of the node where the protected service originates.
Service. The name of the protected service.
For an ITS service (e.g. SI, SDI, SDH etc.) the name is on the format itso-n, where n is a unique number for the service.
For an ETS service (Ethernet), the name is on the format etsn, where n is a unique number for the service.
The switch-over service is enabled in case of failure on the protected service:
Source node. The name of the node where the secondary service originates.
Service. The name of the secondary service.

If the checkbox Admin status on destinations follow source at fail-over is checked, then all Ethernet interfaces will be disabled and enabled according to the status of the protected and secondary service. This is only applicable for ETS. See Redundant Headends for details.

Lab. 24 Security Management

Goal

In this exercise you will learn how to use some of the security management functions, like adding users and modifying permissions.

1. Select menu **Tools | Security Administration**. This will open a new window for managing the security settings.

2. Explore the different functions.

Add Users

Add a new user. The procedure to add a new user group is somewhat similar.

1. From the **Security Administration**, select **File | New | AddUser** (or use the toolbar button).

2. Enter:
   the User name,
   Password,
   Confirm the Password and
   Click **Next**.

3. Specify password and account expiration time,
   Click **Next**.

4. Select group membership and/or directly assigned permissions.
   Click on **Finish**.

5. Verify that the user appears in the user tree.

Change of allowed operations

Change the allowed operations for the group *Admin*. The user *root* is a member of this, and will be affected.

1. Select the *Admin* group in the tree under the node *Groups*.

2. Select the **Permitted Operations for Froups** tab.

3. Click on **Set Permissions**.

4. Examine the permission tree.

5. Disable the **Modify System Information** (found as *Operation Tree Root | DTM Network Devices | Modify System Information* closer to the end of the tree). This will disable the ability to set sysName, sysContact and sysLocation using the **Basic System Information** dialog.

6. Click **Done**. Open the **Basic System Information** (select a node and open menu **Nimbra Node | System Information…**). Verify that function: you should now not be able to change any of the settings.

Change of accessible nodes (Custom View Scope)

In this exercise you will limit the all users in the group *Admin* to only see some nodes in the maps. It is possible to perform similar operations for events, alarms, network database etc.

1. Select the *Admin* group in the tree under the node *Groups*.

2. Select the **Custom View Scope for Group** tab.

3. Select the Custom View Scope Name to **Maps**. The Custom View Scope that will be created will in this exercise apply to all the maps.

4. Click the **Add AuthorizedScope** button. This will open a dialog where you enter the Custom View Scope settings.

5. Name the Custom View Scope *zero*, and set the criteria so that **name** must match **node0**. See the *Web NMS User's Guide*, *Appendix F: Custom View Properties*, *Tips and Tricks* for details on how to write rules.

6. Click **Ok**, within seconds the map will only show the matching network elements.

Lab. 25 Backup, Reinitialize and Restore the Database

Goal

In this exercise you will learn how to backup, reinitialize and restore the database.

When you do a backup of Nimbra Vision database, all the data in the database is saved in a file. You can use this file to restore the whole or only a part of the database at a later time.

Backup when the Server is not running

When Nimbra Vision server is **not** running, backup can be taken using the **`BackupDB.bat`** file available under the folder ***`<NMS Home>`*`/bin/backup`**. See the documentation for details.

Note! *Do not use the backup command when the server is running. When the server is running, it is constantly updating tables. Using the script would result in inconsistency in the backed up data.*

Backup when the Server is running

When Nimbra Vision server is running, backup can be done using a policy. The policy **NMS Backup** policy takes a backup of the database. You can set up a scheduler for when to take the backups. The backed up contents are stored under *<NMS Home>*`/backup` folder. The backup filename will bear the date and time of backup. For example, a typical backup filename would look something as follows: `BackUp_JAN1_2003_2_00.data`.

1. Create a **NMS Backup** policy. You do not have to configure the scheduler.

2. Execute the **NMS Backup** policy. Wait a couple of minutes. You shall now have a backup file. Verify this using the Windows Explorer.

Reinitialize the Database

It is sometimes desirable to start Nimbra Vision server with a fresh database. Occasions when you would like to reinitialize the database are when you have installed a Nimbra Vision server on a host where you have used a previous, incompatible installation. Or you for some other reason would like to have a fresh database.

Reinitializing the database will not reset Nimbra Vision server to how it was configured at installation time. Configuration files will not be affected when the database is reinitialized.

1. Log out from the client and shut down the Nimbra Vision server, menu **Start | Programs | Net Insight NimbraVision | Nimbra Vision Server | Stop Server**. Make sure the host name is for you server.

2. Run the command file ***<NMS Home>*\bin\reinitialize_nms.bat**. This will drop entire NMS database.

3. Start the server and log in again. Notice that all the previous data has been deleted and that all the nodes are discovered once again.

Note! *SNMPv3 configuration data configured using the Discovery Configurator was saved in the database. All the SNMPv3 are therefore lost when reinitializing the database.*

Restore the database

1. Log out from the client and shut down the Nimbra Vision server.

2. Use the script **Restore.bat** available under the folder ***<NMS Home>*/bin/backup**. As parameter, give the file name of the backup data file.

For example, if the backup file name is `BackUp_JAN1_2003_2_00.data`, then you restore the contents as (on windows): `RestoreDB BackUp_JAN1_2003_2_00.data`. If the backed up data file is located in some other folder than the default folder, you must supply the full path name for the file, and the path must be entered with forward-slashes, even on windows systems.

Note! *Make sure that you type the file name in correct case. The file name is case sensitive.*

3. Start the server and log in again. Notice that all the previous data has been restored.

Lab. 26 User Clients

Goal

In this exercise you will try some of the other Nimbra Vision clients.

To run the exercise, you must have a Java 1.4.2 installed.

Starting the Applet client

1. Open the web browser to the server, port 9090: `http://server:9090`
2. Select the **Applet client**, provide the user name and password and click **Login** The client is downloaded to the web browser as a Java applet, and will be started.
3. Notice that the client is the same as the installed client.
4. Exit the client.

Starting the Java WebStart client

5. Open the web browser to the server, port 9090: `http://server:9090`
6. Click the button **Web Start** Client. The client is downloaded (unless it already had been before) and started. Once the client has been downloaded, it will be cached on your client PC.
7. Login. Notice that the client is the same as the installed client.
8. Exit the client.
9. Try starting the client form Java Web Start instead. Use the Windows menu **Start | All Programs | Java Web Start | Java Web Start**, and select the Nimbra Vision client.
10. Login and exit when done.

Starting the Web (HTML) client

11. Open the web browser to the server, port 9090: `http://server:9090`
12. Select the **Web client**, provide the user name and password and click **Login**. You become logged into the web client.
13. Explore the Web client. The web client provides some, but not all, of the functionality presented in the other clients.
14. Exit the client.

Lab. 27 License Key

Goal

In this exercise you will practice how to install or upgrade the license key.

A license key is a file with information that grants you to run Nimbra Vision. The license key may contain a time limit on the license (typically for an evaluation license), and a limitation of the number of managed nodes.

To be able to run Nimbra Vision server application, a license key is required. If a license key has not been installed when Nimbra Vision starts, it will ask for you to enter the license key file after accepting the license agreement.

It can sometimes be necessary to install a license key on command. Some cases would be if:

a. Upgrading from evaluation license to full license

b. Upgrading the license to a new number of managed nodes

c. Start Nimbra Vision as an NT service

1. To install a license key on command, navigate to **`<NMS_Home>\bin\admintools`** and run **`license.bat`**.

It is possible to install a new license key while Nimbra Vision server is running. Nimbra Vision server checks every two minutes to see if a new license key has been installed.