Network Manager IP Edition
4.2

User Guide

2021-4213-01

Note

Before using this information and the product it supports, read the information in "Notices" on page 427.

This edition applies to version 4.2 of IBM Tivoli Network Manager IP Edition (product number 5724-S45) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

The *IBM Tivoli Network Manager User Guide* gives an overview of Network Manager and describes how to use the product to troubleshoot network problems. This publication is for network operators and administrators who need to configure their environment.

Publications

This section lists publications in the Network Manager library and related documents. The section also describes how to access IBM publications online and how to order publications.

Your Network Manager library

The following documents are available in the Network Manager library:

- The *IBM Tivoli Network Manager IP Edition Release Notes* give important and late-breaking information about Network Manager. This publication is for deployers and administrators, and should be read first.
- The *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*describes how to install Network Manager. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up Network Manager.
- The *IBM Tivoli Network Manager IP Edition Administration Guide* describes administration tasks such as how to start and stop the product, discover the network, poll the network, manage events, administer processes, and query databases. This publication is for administrators who are responsible for the maintenance and availability of Network Manager.
- The *IBM Tivoli Network Manager Reference* contains reference information including the system languages, databases, and Perl API used by Network Manager. This publication is for advanced users who need to customize the operation of Network Manager.

Prerequisite publications

To use the information in this publication effectively, you must have some prerequisite knowledge, which you can obtain from the following publications:

- *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*

  Includes installation and upgrade procedures and describes how to configure security and component communications. The publication also includes examples of Tivoli Netcool/OMNIbus architectures and describes how to implement them.
- *IBM Tivoli Netcool/OMNIbus User's Guide*

  Provides an overview of the desktop tools and describes the operator tasks related to event management using these tools.
- *IBM Tivoli Netcool/OMNIbus Administration Guide*

  Describes how to perform administrative tasks using the Tivoli Netcool/OMNIbus Administrator GUI, command-line tools, and process control. The publication also contains descriptions and examples of ObjectServer SQL syntax and automations.
- *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*

  Contains introductory and reference information about probes and gateways, including probe rules file syntax and gateway commands.
- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*

  Describes how to perform administrative and event visualization tasks using the Tivoli Netcool/OMNIbus Web GUI.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

IBM posts publications for this and all other products, as they become available and whenever they are updated, to the IBM Knowledge Center Web site at:

http://www.ibm.com/support/knowledgecenter/

Network Manager documentation is located under the **Cloud & Smarter Infrastructure** node on that Web site.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File** > **Print** window that allows your PDF reading application to print letter-sized pages on your local paper.

Ordering publications

You can order many IBM publications online at the following Web site:

http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order IBM publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:

   http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss
2. Select your country from the list and click **Go**. The **Welcome to the IBM Publications Center** page is displayed for your country.
3. On the left side of the page, click **About this site** to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully.

Accessibility features

Network Manager includes the following major accessibility features:

- Operations that use a screen reader.

Network Manager uses IBM Installation Manager to install the product. You can read about the accessibility features for IBM Installation Manager at https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Network Manager uses the latest W3C Standard, http://www.w3.org/TR/wai-aria/, to ensure compliance to http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards), and http://www.w3.org/TR/WCAG20/. To take advantage of accessibility features, use the latest release of your screen reader in combination with the latest web browser that is supported by this product.

The Network Manager online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at https://www.ibm.com/support/knowledgecenter/v1/content/about/releasenotes.html#accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

Network Manager provides the following features suitable for low vision users:

- All non-text content used in the GUI has associated alternative text.
- Low-vision users can adjust the system display settings, including high contrast mode, and can control the font sizes using the browser settings.
- Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

Network Manager provides the following features suitable for photosensitive epileptic users:

- The Network Manager user interfaces do not have content that flashes more than two times in any one second period.

The Network Manager web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Extra steps to configure Internet Explorer for accessibility

If you are using Internet Explorer as your web browser, you might need to perform extra configuration steps to enable accessibility features.

To enable high contrast mode, complete the following steps:

1. Click **Tools** > **Internet Options** > **Accessibility**.
2. Select all the check boxes in the Formatting section.

If clicking **View** > **Text Size** > **Largest** does not increase the font size, click **Ctrl +** and **Ctrl -**.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see https://www.ibm.com/able.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

https://www.ibm.com/training/search?query=tivoli

Support and community information

Use IBM Support, Service Management Connect, and Tivoli user groups to connect with IBM and get the help and information you need.

IBM Support

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Go to the IBM Software Support site at https://www.ibm.com/support/home/ and follow the instructions.

IBM Support Assistant
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to https://www.ibm.com/support/knowledgecenter/SSLLVC/welcome/isa_welcome.html

Part 1. Product overview

Read about the key concepts of IBM Tivoli Network Manager IP Edition.

Chapter 1. About Network Manager

IBM Tivoli Network Manager IP Edition provides detailed network discovery, device monitoring, topology visualization, and root cause analysis (RCA) capabilities. Network Manager can be extensively customized and configured to manage different networks. Network Manager is tightly integrated with IBM Tivoli Netcool/OMNIbus. When installed together with the IBM Netcool Operations Insight infrastructure and operations management solution, then Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis. Network Manager also provides extensive reporting features, and integration with other IBM products, such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Business Service Manager and IBM Tivoli Monitoring.

Network Manager is not suitable for monitoring the performance of networks. To monitor the performance of networks, use the Tivoli Netcool Performance Manager and Network Performance Insight products. For more information, see the Tivoli® Netcool® Performance Management information center at http://www.ibm.com/support/knowledgecenter/SSBNJ7/welcome.

Network Manager features include the following:

Manage modern complex networks
Network Manager discovers, polls, and visualizes complex networks, containing a wide range of network-type devices, such as routers and switches, and using network protocols such as MPLS, BGP, and OSPF, and technologies, such as RAN, LTE, and wifi access points.

View the network in multiple ways
Different ways to visualize the network include network views, which show standard and customized device groupings such as subnets, VLANs, and VPNs, and the **Network Hop View**, which shows a selected device and all devices connected to it up to a configurable number of connections. You can also navigate the interfaces and other components of a device using the Structure Browser. Multi-widget views enable you to put these views together; for example, you can select a device in the **Network Hop View** and instantly see the interfaces and other components of the device in an adjacent Structure Browser widget. You can also use multiwidget views to show simultaneous topology maps and event lists.

Apply ready-to-use device and interface polling capabilities
Network Manager provides a set of ready-to-use device and interface polls, including ICMP polls and MIB variable threshold polls. The MIB variable threshold polls generate network events if thresholds are violated on specified MIB variables. You can customize network polling so that events are received when thresholds are violated on any MIB variable on your network devices.

Leverage built-in root cause analysis capabilities
Network Manager sorts through multiple network events and uses knowledge of network topology to determine a single root cause event. Network Manager highlights root cause events in event lists and in topology maps so that your operators can instantly determine where to begin troubleshooting the network.

Troubleshoot network problems using right-click tools and topology search
Network Manager provides a set of ready-to-use right-click tools to enable operators to troubleshoot network devices shown in network topology maps and event lists. For example, you can perform diagnostic actions such as ping and traceroutes and you can retrieve device information such as DNS lookups or retrieve more complex protocol information such as BGP and OSPF information. You can add custom right-click tools to perform any desired action on a device.

You can also perform a search to retrieve events between selected devices. If you have integrated with Netcool Configuration Manager, then you can retrieve configuration history and other relevant configuration information for devices in your maps by right-clicking directory into Netcool Configuration Manager reports. Using the map search you can quickly identify an entity within a map using a partial identifier, such as part of an IP address or hostname.

Generate richer network visualization and event data

You can enrich the network topology by customizing the discovery to retrieve and store data about the discovered devices from third-party data sources. For example, you could retrieve customer information related to devices from a third-party inventory database, thereby enabling network operators to see the customer associated with a given device or network event.

You can also enrich network events with any topology data retrieved by the discovery process. For example, standard network events on device interfaces that originate from traps show the interface index only. You can enrich these events with interface name and description data. Operators viewing network events on device interfaces can then easily identify the interface.

Discover increasingly bigger networks

Network Manager can discover and manage increasingly bigger networks.

Run reports to retrieve essential network data

You can run reports to retrieve a wide range of network data, including data on network availability, network assets, and network technology.

Build custom multi-widget pages

You can build pages that contain any combination of data. For example, you can combine topology maps with device structure views and event lists. You can also combine discovery status information with event lists that show custom discovery events.

Integrate with a wide range of Tivoli products

Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis. Network Manager also provides extensive reporting features, and integration with other IBM products, such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Business Service Manager and IBM Tivoli Monitoring.

What's new in this release

Network Manager V4.2 provides new features and enhancements that include the following areas: enhanced upgrade and migration process, enhanced GUI framework that makes uses of Dashboard Application Services Hub features, enhanced search and zoom network visualization features, enhanced GUI responsiveness due to the removal of applet technology, and the ability to aggregate and store significantly more amounts of historical poll data and display this data directly from the network GUIs. Users of IBM Netcool Operations Insight are also able to access the **Network Health Dashboard**, which provides new capabilities for monitoring and troubleshooting the network. Fix Pack 1 In addition Netcool Operations Insight users can use the **Device Dashboard** to troubleshoot network issues by navigating the network topology and see performance metric values, anomalies and trends on any device, link, or interface.

Summary of new features

IBM Tivoli Network Manager IP Edition 4.2 offers the following new features and functions. For links to related topics for each new feature and function, see the equivalent section online at http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/relnotes/reference/rn.html?lang=en-us#relnotes__new-prod-feats-funks.

This description of the new features and enhancements is also available in the *.IBM Tivoli Network Manager IP Edition Release Notes*.

New product features and functions in Fix Pack 13

Fix Pack 13

The following features and functions are introduced in Fix Pack 13.

New product features and functions in Fix Pack 12

Fix Pack 12

The following features and functions are introduced in Fix Pack 12.

Tabular network views to display severity icons

You can now select the option to display the status as text or icon for `severity` and `managedStatus` columns.

For more information, see *Configuring column display in the tabular view* in the *IBM Tivoli Network Manager User Guide*.

Support for storing the Poll Data for Float Value

IBM Tivoli Network Manager now allows you to store float, 64-bit integer, and 32-bit integer values in DB table for Db2 and Oracle.

For more information, see *Storing Poll Data for DB2 and Oracle* section in the *IBM Tivoli Network Manager User Guide*.

Connectivity between MME and HSS IMS

ALU SAM Collector is now extended to support the Mobility Management Entity (MME) to Home Subscriber Server (HSS) over S6a interface.

Nokia 5529 IDM collector extended for additional parameters

The Nokia 5529 IDM collector is now extended for additional parameters. The collector allows you to add any additional attributes mapping to the properties file for all the managed objects coming in the EMS export file. All those additional attribute will be populated as name or value pairs in `workingEntities.finalEntity`.

Warning if domain name is not all uppercase

If the name of the new domain contains any lowercase letters, the script prompts to ask if you want to create a domain with that name. The script also now has a `-force` command-line option, which suppresses this question and creates the new domain unconditionally. If you have any custom scripts that call `domain_create.pl`, you may need to add the `-force` option to them to preserve existing behavior.

Support for 5G gNodeB

IBM Tivoli Network Manager now supports 5G NR GNodeB devices.

Support for Apache Storm

Apache Storm has been upgraded from version 2.1.0 to 2.2.0.

New product features and functions in Fix Pack 11

Fix Pack 11

The following features and functions are introduced in Fix Pack 11.

Tivoli Common Reporting is not supported

Tivoli Common Reporting is no longer supported. You must use Cognos Analytics on all platforms.

All references to Tivoli Common Reporting have been updated to Cognos Analytics in the Fix Pack 11 documentation.

Link Status Option

Your administrator can now configure links to display link status information from poll policies. Links can be displayed as colored, or colored with an associated severity icon.

For more information, see *Monitoring links* in the *IBM Tivoli Network Manager User Guide*.

Warning if a user is about to create an excess number of views

If the system contains a large number of views, this can adversely affect performance. The administrator can restrict the number of child views that a dynamic view is allowed to contain when a

user creates or edits a dynamic view. If the number of child views that a dynamic view would contain is greater than the `topoviz.tree.size.warning` property in `topoviz.properties`, the GUI displays a warning,

For more information, see *Creating dynamic network views* in the *IBM Tivoli Network Manager User Guide*.

New usageStringsRef string

This is a new array reference that contains an element for each of the non-standard command line argument scenarios. If the application takes only standard arguments, this constructor argument should be set to `undef`.

For more information, see *RIV::Param Constructor* in the *IBM Tivoli Network Manager Reference*.

`ncp_gis` able to display custom icons based on the device class

You can now customize the node icon for a device class in a geographical view.

To customize the node icon, see *Configuring the appearance of geographical views* in the *IBM Tivoli Network Manager User Guide*.

New product features and functions in Fix Pack 10

Fix Pack 10

The following features and functions are introduced in Fix Pack 10.

Hop view can now search across domains

You can now search for network entities across all domains at once.

For more information, see *Using the basic search* in the *IBM Tivoli Network Manager User Guide*.

New product features and functions in Fix Pack 9

Fix Pack 9

The following features and functions are introduced in Fix Pack 9.

New Telnet agent

The HuaweiLLDPTelnet agent discovers the Layer 2 physical switch-to-switch links between Huawei switches. For more information, see *Discovery agents that discover connectivity among Ethernet switches* in the *IBM Tivoli Network Manager Reference*.

Change encryption strength

You can change the strength of the encryption used by the Network Manager core components and GUI components. You can also change the type of encryption. For more information, see *Configuring encrpytion length and type* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Configure the display of interface information in the Structure Browser

The **Structure Browser** displays the interface name in the Device Structure Tree by default. You can append the interface alias to the interface name by configuring a properties file.

For more information, see *Customizing Structure Browser preferences* in the *IBM Tivoli Network Manager User Guide*.

Configure the display of the Bookmarks and Libraries tabs

The **Network Views** display the Bookmarks tab by default. You can show the Libraries tab by default instead, and hide one of the tabs, by configuring a properties file. You can also open the **Network Views** by using a URL parameter that defines which tab is opened by default.

For more information, see *Configuring the tabs displayed in the Network Views* and *Network Views URL parameters* in the *IBM Tivoli Network Manager User Guide*.

All entity attributes can be retrieved from a network view query

You can use the `allAttributes=true` parameter to retrieve all entity attributes from a network view Topology API query, instead of only the entity IDs.

For more information, see *Extracting topology data for all chassis devices within a specified network view*.

New product features and functions in Fix Pack 8

Fix Pack 8

The following features and functions are introduced in Fix Pack 8.

All view maintenance settings can be enabled at once

You can enable or disable all automatic view maintenance properties at once by setting a single property, `topoviz.engine.views.enabled`.

For more information, see *Setting up automatic view maintenance* in the *IBM Tivoli Network Manager User Guide*.

Structure Browser table columns widths can be adjusted

You can control the width of columns in the Structure Browser Devices table in the same way as for the Structure Browser Interfaces table. For more information, see *Customizing Structure Browser Preferences* in the *IBM Tivoli Network Manager User Guide*.

Related to this feature, the `entityId` and `entityType` columns can now be in any order in the table definition for the Structure Browser and the Network Views table mode. The default layout for the Network Views table mode and the Interfaces view in the Structure Browser is coded differently in the `ncimMetaData.xml` file. You must observe the new conventions if you change the column display for these views. For more information, see *Configuring column display in the tabular view* and *Configuring column display in the Structure Browser* in the *IBM Tivoli Network Manager User Guide*.

Topology API can filter by sub-chassis

An optional Boolean parameter, includeSubChassis, has been added to `nm_rest/topology/devices/all` and `nm_rest/topology/devices/classes`. Using this property, you can include or exclude results from sub-chassis.

For more information, see *Extracting topology data for all chassis devices* and *Extracting topology data for all chassis devices that belong to a set of classes* in the *IBM Tivoli Network Manager Reference*.

Note:

As part of this feature, the definition of the `ncim.mainNodeDetails` database view has been changed. The `domainMgr` table has been replaced with the `domainMgrExcludeManual` view, to filter out duplicated rows for manual devices. If you have changed the definition of the `ncim.mainNodeDetails` database view, incorporate your changes into the new view definition.

For an upgrade, the script that changes the `mainNodeDetails` database view is in `$ITNMHOME/scripts/sql/updates/$server/4.2-fp8.sql`, where `$server` is db2 or `oracle`.

For a new installation, the script that defines the `mainNodeDetails` database view is in `$ITNMHOME/scripts/sql/$server/createPrecisionIPDb.sql`, where `$server` is db2 or `oracle`.

New product features and functions in Fix Pack 7

Fix Pack 7

The following features and functions are introduced in Fix Pack 7.

Changing GUI properties does not require a restart of the Dashboard Application Services Hub
If you edit a `.properties` file in the `$NMGUI_HOME/profile/etc/tnm` directory, which contains properties used by the Network Manager GUI, you no longer have to restart the Dashboard Application Services Hub in order for the changes to take effect.

Backing up ncp_store cache files

You can back up and restore the `ncp_store` cache, so that you have a copy of the topology.

For more information, see *Configuring backups of the ncp_store cache* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Topology API can filter by class

The Topology API can now include or exclude devices that belong to a specified class or set of classes.

For more information, see *Extracting topology data for all chassis devices that belong to a set of classes* and *Extracting topology data for all chassis devices within specified domains* in the *IBM Tivoli Network Manager Reference*.

Support for Google Chrome Browser

Google Chrome is now a supported browser for using the Network Manager GUI.

For more information on supported browsers, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Hiding the option to enable caching of discovery tables

Caching discovery tables can significantly affect discovery performance. An administrator can now remove the option to enable this feature from the GUI. Caching can still be enabled on the command line.

For more information, see *Advanced discovery parameters* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Configuring displayed columns in the Structure Browser

You can choose which columns are displayed in the **Structure Browser** tabular view.

For more information, see *Configuring column display in the Structure Browser* in the *IBM Tivoli Network Manager User Guide*.

Customize horizontal alignment of text in the Structure Browser and tabular views

You can change the horizontal alignment of text to be left, right or center-aligned.

For more information on this feature in the **Structure Browser**, see *Configuring column display in the Structure Browser* in the *IBM Tivoli Network Manager User Guide*.

For more information on this feature in the tabular views, see *Configuring column display in the tabular view* in the *IBM Tivoli Network Manager User Guide*.

New product features and functions in Fix Pack 6

Fix Pack 6

The following features and functions are introduced in Fix Pack 6.

Support for cloud-based MMEs and Nokia SAE Gateways
The Alcatel5620Sam Java Collector has been extended to support cloud-based, or virtual, MMEs (Multimedia Extensions), and to support Nokia SAE Gateway devices, which have both LTE PDNGateway and ServingGateway functionality. If the data has been discovered, you can select LTE S1-U, LTE S5-U, and LTE S8 connectivity from the topology views. For more information, see *Predefined Collectors* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Support for IBM Db2 version 11.1 Advance Enterprise Server Edition

IBM Db2 version 11.1 Advance Enterprise Server Edition is supported for use a topology database. For more information, see *Supported topology databases* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Customize the Structure Browser view for a single device

You can specify the view in which the Structure Browser portlet opens when a single device is displayed.

For more information, see *Customizing Structure Browser preferences* in the *IBM Tivoli Network Manager User Guide*.

Third-party library upgrade

Tom Sawyer libraries have been upgraded to version 7.6. This is intended to improve performance in the GUI.

Support for TLS protocol versions in Cisco APIC collector

You can specify the version of TLS protocol that you want the collector to use.

For more information, see *Configuring the Cisco APIC REST collector* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Support for discovering Cisco CRS LAG information

Fix Pack 6 The IEEE8023LAG agent discovers the LAG (Link Aggregation Group) Link entities and physical ports associated with the LAG between two network devices. The agent discovers information from Cisco Carrier Routing System (CRS) LAG networks.

For more information, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Support for discovering Nokia OMS 1350 EMS

The NokiaOMS1350 Java collector retrieves data from the Nokia OMS 1350 EMS.

For more information, see *Configuring the NokiaOMS1350 Java collector* in the *IBM Tivoli Network Manager IP Edition Administration Guide*

New product features and functions in Fix Pack 5

Fix Pack 5

The following features and functions are introduced in Fix Pack 5.

New IP SLA agents

Discovery support is introduced for Huawei NQA and Juniper RPM devices by using two new agents:

HuaweiNQA

The Huawei Network Quality Analyser (NQA) agent discovers IP SLA-related data from Huawei NQA devices that support the NQA-MIB MIB. The agent retrieves data such as information on the configured probes.

JuniperRPM

The Juniper Realtime Performance Monitoring (RPM) agent discovers IP SLA-related data from Juniper RPM devices that support the DISMAN-PING-MIB and JUNIPER-PING-MIB MIBs. The agent retrieves data such as information on the configured probes.

View device information in the Device View

The **Device View** is a composite GUI that displays information about a device. Select a device in the **Network Hop View** widget to display the following information in the other portlets within the **Device View**:

- The **Top Performers** widget shows poll data for the device.
- The **Event Viewer** widget shows events for the device.

- The **Structure Browser** widget shows the containment of the device.

For more information, see *Using the Device View* in the *IBM Tivoli Network Manager User Guide*.

Export a network view

You can export the contents of a network view to a comma-separated values (CSV) file.

For more information, see *Visualizing devices in tabular layout* in the *IBM Tivoli Network Manager User Guide*.

Add columns to the tabular view

You can add and remove columns when the network topology is displayed in tabular layout.

For more information, see *Configuring columns displayed in the tabular view* in the *IBM Tivoli Network Manager User Guide*.

Geographical maps updates

You can choose from available base mapping layers and custom mapping layers in the geographical views. For more information, see *Viewing devices in geographical context* in the *IBM Tivoli Network Manager User Guide*.

Important: The syntax of the `config.json` configuration file is different in Fix Pack 5. Before installing Fix Pack 5, back up your existing `config.json` configuration file. Migrate any configuration changes that you made, referring to the new syntax as described in *Adding custom map layers* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

You can change the default connectivity in the Network Hop View

When the **Network Hop View** is opened from the Dashboard Application Services Hub menu, **Structure Browser**, or **Event Viewer**, it displays layer 2 connectivity by default. You can change this default setting.

For more information, see *Changing the default topology layer for the **Network Hop View*** in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

PDF guides reorganized

The PDF documentation deliverables have been consolidated into the following items:

- The *IBM Tivoli Network Manager IP Edition Release Notes* give important and late-breaking information about Network Manager. This publication is for deployers and administrators, and should be read first.
- The *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*describes how to install Network Manager. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up Network Manager.
- The *IBM Tivoli Network Manager IP Edition Administration Guide* describes administration tasks such as how to start and stop the product, discover the network, poll the network, manage events, administer processes, and query databases. This publication is for administrators who are responsible for the maintenance and availability of Network Manager.
- The *IBM Tivoli Network Manager Reference* contains reference information including the system languages, databases, and Perl API used by Network Manager. This publication is for advanced users who need to customize the operation of Network Manager.

Show or hide layout buttons in the Path Views GUI

You can use the new property `topoviz.pathview.layout.enabled` in the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file to show or hide the layout buttons for the **Path Views GUI**.

The default value for this property is `false`, which hides the layout buttons.

New product features and functions in Fix Pack 4

Fix Pack 4

The following features and functions are introduced in Fix Pack 4.

Monitoring IP Service Level Agreement (IP SLA) configurations

You can configure discovery to discover and visualize probes that are configured to monitor IP SLA response times. Collections of probes are displayed in the network views. You can also view the status of events on the probes and the links between them.

Important: You must install version 4.8.7 of the Netcool/OMNIbus Knowledge Library and configure it for use with the IBM Tivoli Netcool/OMNIbus SNMP Probe. For information on how to install and configure the Netcool/OMNIbus Knowledge Library, see http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/nckl/wip/concept/nckl_intro.html.

For more information about monitoring IP SLA, see the *IBM Tivoli Network Manager User Guide*.

Firefox 52 support

The Network Manager web applications now run on Firefox 52.

For more information about supported browsers, see *Supported browsers for Web applications* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Updates to Telnet Helper encryption algorithms

The Telnet Helper now supports the AES-128-CTR , AES-192-CTR and AES-256-CTR encryption algorithms.

For more information, see *Helpers* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

New product features and functions in Fix Pack 3

Fix Pack 3

The following features and functions are introduced in Fix Pack 3.

Support for SLES 12.0

SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) is a supported operating system in Fix Pack 3.

Support for Db2 version 11.1

IBM Db2 version 11.1 Enterprise Server Edition is supported for use as the topology database in Fix Pack 3.

Support for Linux on IBM z Systems

Network Manager is now supported on Linux on IBM z Systems. The following versions are supported:

- SuSE Linux® Enterprise Server (SLES) 12.0 SP2 and SP3 on IBM z Systems (s390x, 64 bit)

If you use Network Manager on Linux on IBM z Systems, Tivoli Common Reporting is not supported. Use Cognos Analytics for reporting. For more information about Cognos Analytics, search for *Cognos Analytics* in the IBM Order Management Software Knowledge Center at https://www.ibm.com/support/knowledgecenter/en/SS6PEW.

Offline geographical maps

You can use an appropriate mapping provider to enable access to geographical maps without an internet connection. For more information, see *Integrating an online or offline Web Map Service* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Custom geographical map layers

You can add custom layers to geographical maps. For example, you can add geographical information that is made available by a public server. for more information, see *Adding custom map layers* in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Regional aggregation for geographical maps

You can group locations into cities, group cities into states, and group states into countries. This grouping is called regional aggregation. For more information, see ***Enabling regional aggregation for geographical views*** in the *IBM Tivoli Network Manager User Guide*.

New product features and functions in Fix Pack 2

Fix Pack 2

The following features and functions are introduced in Fix Pack 2.

Geographical views

You can configure geographical discovery to enrich devices with location information. These devices can be displayed in the new **GIS Device Health View** and **GIS Device Map**. Devices can be grouped into locations. Status is shown on devices, locations, and links.

Note:

If you installed a beta version of this feature, you must uninstall the geographical views feature before updating to Fix Pack 2 or later. Run the following command from the top level directory where you unpacked the beta `.zip` file:

```
sh bin/install.sh -u
```

The application WAR files are removed and the WebSphere Application Server is restarted.

To download the beta files again, contact IBM Support.

For more information about this feature, see the *IBM Tivoli Network Manager User Guide*.

Network Views GUI: background images can be set for Network Views

When you create views, you have the option to provide background images for **Network Views**.

New product features and functions in Fix Pack 1

Fix Pack 1

The following features and functions are introduced in Fix Pack 1.

Applying NCIM topology database schema updates for one or more fixpacks or interim fixes

It is now possible to run a script to apply all necessary NCIM topology database schema updates for one or more fixpacks or interim fixes.

For more information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Device Dashboard to enable operators to troubleshoot network issues on any device, link, or interface

Netcool Operations Insight users can use the **Device Dashboard** to troubleshoot network issues by navigating the network topology and see performance metric values, anomalies and trends on any device, link, or interface.

Netcool Operations Insight users can also launch to the new **Device Dashboard** directly from the **Network Health Dashboard**.

To support presentation of performance data in the **Device Dashboard**, Network Manager now integrates with Network Performance Insight to enable sharing of poll data. This integration is facilitated using an Apache Kafka bus mechanism.

For more information, see the Netcool Operations Insight Knowledge Center, at http://www.ibm.com/support/knowledgecenter/SSTPTP/welcome.

New product features and functions in Interim Fix 2

The following additional support is provided in Interim Fix 2.

Support for Oracle Database version 11g
Network Manager V4.2 Interim Fix 2 supports Oracle Database version 11g, Enterprise Edition with Partitioning option (Support added in Network Manager 4.2 Interim Fix 2).

Support for Tivoli Netcool/OMNIbus on Windows
Network Manager V4.2 Interim Fix 2 provides the ability to configure an existing Windows ObjectServer for use with Network Manager. This configuration is done by a new script called `config_object_server_for_itnm.sh`, which supports an ObjectServer running on Windows as well as UNIX. If you want to use this ObjectServer as the user repository, then you must also run scripts to configure the users and assign roles to these users.

For more information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

New product features and functions in V4.2

The following new features are provided in V4.2.

Ability to seed discoveries based on third-party database content
Network Manager V4.2 provides a new discovery finder process. Discovery finder processes are responsible for determining device existence. Network Manager V4.2 introduces a new Database finder, ncp_df_dbentry. The Database finder reads a database to retrieve a list of devices to find on the network.

For more information, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

AIX® support

Network Manager V4.2 introduces support for AIX platforms.

AIX On IBM® PowerPC®-based systems, the following versions are supported:

- AIX 6.1 iSeries and pSeries
- AIX 7.1 iSeries and pSeries
- AIX 7.2 iSeries and pSeries

For more information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Default optimization of network polling
Two instances of the network polling process, **`ncp_poller`**, are configured on installation. The `ncp_poller_admin` poller performs administrative tasks such as monitoring the size and age of the poll data database tables, updating caches, dropping partitions, and MIB Grapher support. The `ncp_poller_default` poller is used for SNMP and Ping polling. This distribution of functions can help to improve performance. In previous versions of Network Manager, the administrator had to configure an administrative poller. In Network Manager 4.2, this configuration is done automatically.

For more information, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Enhanced network map features, including enhanced search and zoom features
The network map function is extended and now includes enhanced search and zoom functions.

Enhanced upgrade and migration process
The upgrade and migration process was redesigned with ease of use in mind. The number of files that typically need to be manually migrated is now reduced.

If you need to upgrade to Network Manager V4.2, be sure to read the updated instructions in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide* carefully.

GUI responsiveness
The Network Manager GUI no longer uses Java™ applets. This redesign aims to help the GUI responsiveness for users.

Installation process now uses IBM Installation Manager

Network Manager V4.2 uses IBM Installation Manager for installation. IBM Installation Manager is used by most other IBM products, and is designed for speed and ease of use.

For more information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Network Health Dashboard to enable operators to monitor and troubleshoot network health

Netcool Operations Insight users can use the **Network Health Dashboard** to monitor and troubleshoot network health. The **Network Health Dashboard** monitors a selected network view, and displays device and interface availability within that network view. It also reports on performance by presenting graphs, tables, and traces of KPI data for monitored devices and interfaces. A dashboard timeline reports on device configuration changes and event counts, enabling you to correlate events with configuration changes. The dashboard includes the **Event Viewer**, for more detailed event information.

For more information, see the Netcool Operations Insight Knowledge Center, at http://www.ibm.com/support/knowledgecenter/SSTPTP/welcome.

New mechanism for aggregating raw poll data into historical polling data

Network Manager now uses the Apache Storm real-time computation system to aggregate raw poll data into historical poll data, and stores raw and historical poll data in the NCPOLLDATA database. You can access this data on a per device or link basis from the topology map within the Network Hop View GUI, Network Views GUI, and **Path Views GUI**. Raw and historical poll data is also presented in graphs and tables in performance reports, and for Netcool Operations Insight users in the **Network Health Dashboard**.

Right-click option to display historical poll data for all metrics on a device or interface

Within a topology view, users can right-click on a device, multiple devices, a subview, or a subnet to display the historical poll data. To do display historical poll data, first right-click a device, and then select **Polling** > **MIB Info** > **Show Performance**.

Note: This new feature replaces the **SNMP MIB Grapher** historical data function.

For more information, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Support for Mozilla Firefox ESR 38

Network Manager V4.2 introduces support for Mozilla Firefox Extended Service Release (ESR) 38.

Using the new Dashboard Application Services Hub features

Network Manager now uses functions of the Dashboard Application Services Hub within Jazz® for Service Management to administer pages, folders, views, widgets, and console preference profiles.

The integration between Network Manager V4.2 and Tivoli Netcool/OMNIbus Web GUI V8.1 is simpler, because both products are now hosted by Dashboard Application Services Hub. The Network Management Integration for Tivoli Netcool/OMNIbus V8.1 is no longer required.

For more information, see the *IBM Tivoli Network Manager User Guide*.

Network Manager architecture

The Network Manager architecture can be divided into three layers: network layer, data layer, and visualization layer.

Network

The network layer interacts directly with the network. This layer contains network discovery and polling functionality. Network discovery retrieves topology data and network polling retrieves event data.

Data

The data layer stores the topology data retrieved by network discovery and the event data retrieved by network polling. Network polling also includes storage of polled SNMP and ICMP data for reporting and analysis. This layer also provides root cause analysis functionality that correlates topology and

events to determine the source of network faults, and event enrichment functionality that adds topology data to events.

Visualization
The visualization layer provides the tools operators and administrators need to view topology, view events, and run network troubleshooting tools.

The following figure shows a conceptual overview of the Network Manager functional layers. Please note the following points when consulting the figure:

- It is possible to configure the Network Manager to include failover. This is not shown in the figure.
- Network Manager is designed to be installed with Tivoli Netcool/OMNIbus to enhance fault management, including root cause analysis, and correlation of alerts with the network topology.

  This figure depicts a standard Network Manager installation, and shows Tivoli Netcool/OMNIbus handling the storage and management of network events and the Tivoli Netcool/OMNIbus Web GUI handling visualization of network events.

  Note: Tivoli Netcool/OMNIbus is a separate product. If you do not already have OMNIbus then you must get a copy and install it. For more information, see the Network Manager installation documentation. Note also that Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis.
- The Dashboard Application Services Hub GUI framework is an application that runs GUIs from different Tivoli products, including Network Manager. The GUIs represented in the following figure, including the topology visualization GUIs and the event visualization GUIs all run within the Dashboard Application Services Hub GUI framework.
  - The topology visualization GUIs include single-widget views, such as the Hop View, Network Views, and Structure Browser. Default topology views also include multi-widget views, such as the Fault-Finding View and the Network Health View.
  - The Tivoli Netcool/OMNIbus Web GUI event visualization GUIs include the **Event Viewer**.
  - Network administrators can also build their own multi-widget views, which customize combinations of the single widget views.

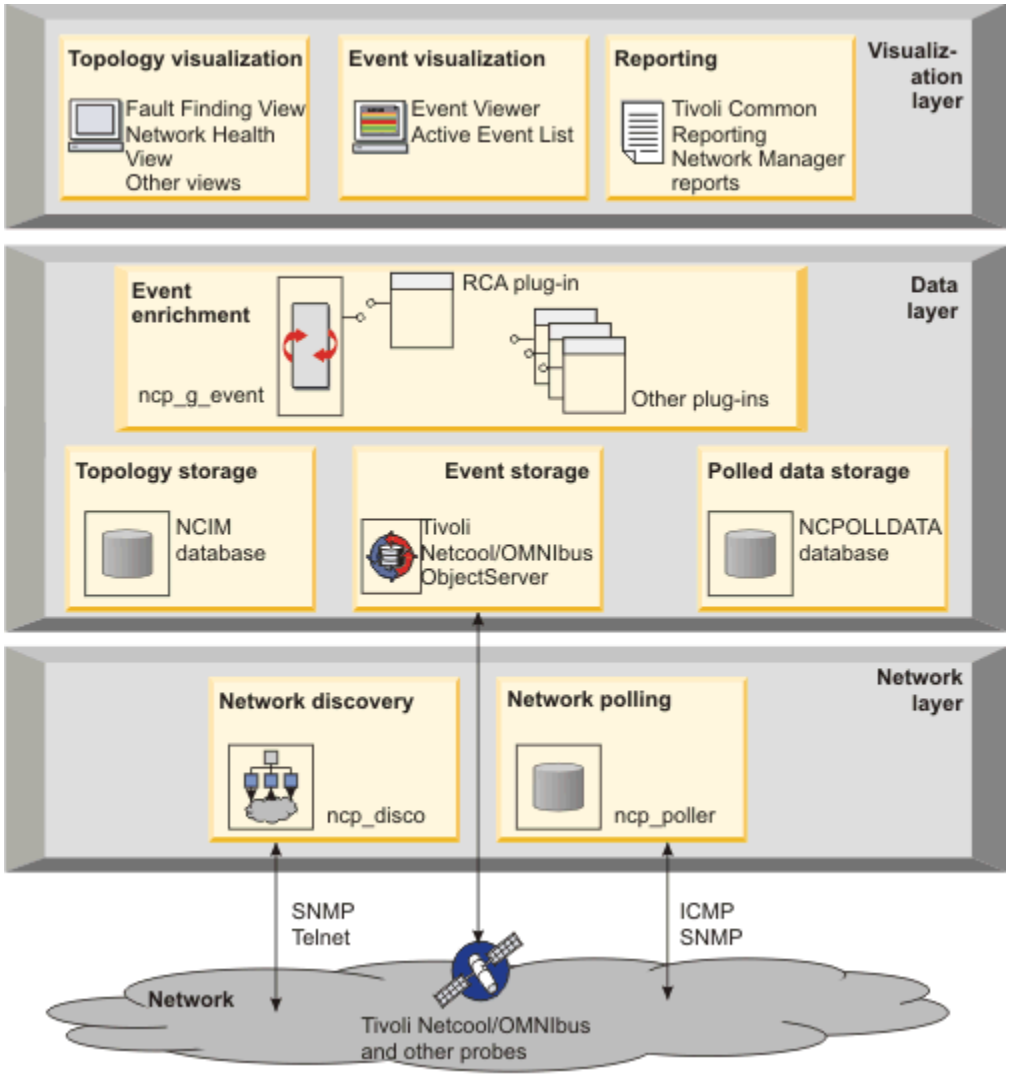

Figure 1. Network Manager functional layers

Network discovery

Network discovery involves discovering your network devices, determining how they are connected (network connectivity), and determining which components each device contains (containment). The complete set of discovered devices, connectivity, and containment is known as a network topology. You build your network topology by performing a discovery and then ensuring that you always have an up-to-date network topology by means of regular rediscoveries.

Network polling

Network polling determines whether a network device is up or down, whether it has exceeded key performance parameters, or whether links between devices are faulty. If a poll fails, Network Manager generates a device alert, which operators can view in the **Event Viewer**.

Topology storage

Network topology data is stored in the Network Connectivity and Inventory Model (NCIM) database. The NCIM database is a relational database that consolidates topology data discovered by Network Manager.

Event enrichment

Event enrichment is the process by which Network Manager adds topology data to events, thereby enriching the event and making it easier for the network operator to analyze. Examples of topology data that can be used to enrich events include system location and contact information.

Root-cause analysis

Root cause analysis is the process of determining the root cause of one or more device alerts. Network Manager performs root cause analysis by correlating event information with topology information. The process determines cause and symptom events based on the discovered network device and topology data.

Event storage

Event data is generated by Network Manager polls and also by Tivoli Netcool/OMNIbus probes installed on network devices. A probe is a protocol or vendor specific piece of software that resides on a device, detects and acquires event data from that device, and forwards the data to the ObjectServer as alerts. Event data can also be received from other event sources.

Event data from all of these event sources is stored in the Tivoli Netcool/OMNIbus ObjectServer.

Note: Tivoli Netcool/OMNIbus is a separate product. If you do not already have OMNIbus then you must get a copy and install it. For more information, see the Network Manager installation documentation.

Polled data storage

At any time a network administrator can set up polling of specific SNMP and ICMP data on one or more network devices. This data is stored in the NCPOLLDATA historical polled data database. Operators can then use the Cognos Analytics viewer to run performance reports to interpret the data.

Topology visualization

Network operators can use several topology visualization GUIs to view the network and to examine network devices. Using these GUIs operators can switch between topology views to explore connectivity or associations, and to see alert details in context. Operators also have access to diagnostic tools such as SNMP MIB Browser, which obtains MIB data for devices.

Event visualization

Operators can view event lists and use alert severity ratings to quickly identify high-priority device alerts. Operators can switch from event lists to topology views to see which devices are affected by specific alerts. They can also identify root cause alerts and list the symptom alerts that contribute to the root cause.

Reporting

Network Manager provides a wide range of reports, including performance reports, troubleshooting reports, asset reports, and device monitoring reports. Right click tools provide immediate access to reports from topology maps.

Related concepts

Network layer
The network layer consists of network discovery and polling tools.

Data layer
The data layer consists of topology storage, event storage, performance reporting data storage, and root cause analysis tools.

Visualization layer

This layer consists of topology visualization and event visualization tools.

Network Manager data flow

Use this information to understand how the components of Network Manager fit together

The following figure shows the main areas of functionality within Network Manager and depicts how data flows between them.

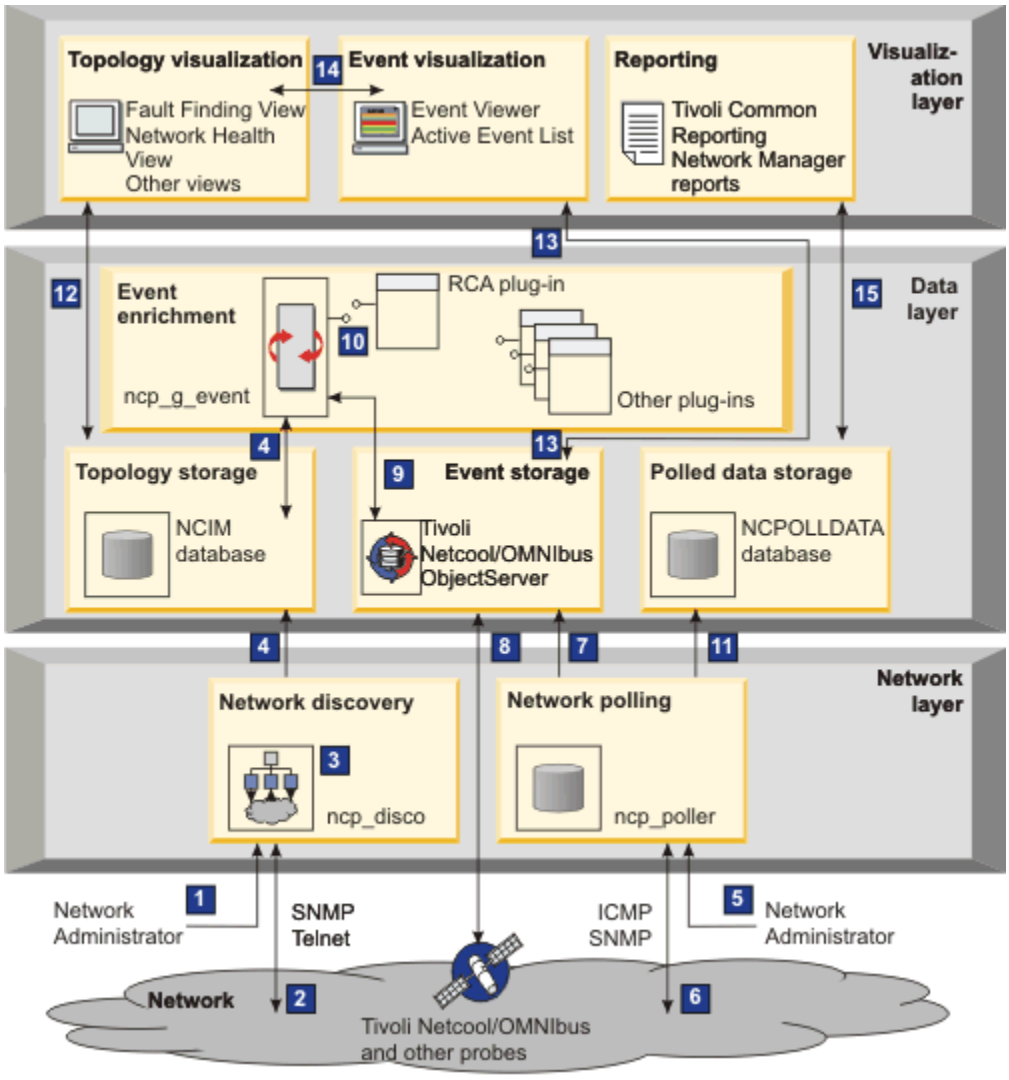

Figure 2. Network Manager data flow

1 Network administrators configure and run a discovery
Batch-mode discoveries can be run on demand or can be scheduled. In batch mode, the whole network can be discovered (this is known as full discovery), or just a single subnet or device (partial discovery). Essential discovery configuration information consists of device seeds, network scope, and device access details such as SNMP community strings.

2 Data is gathered from the network
Devices are found on the network by the Ping finder, File finder, Database finder, or collector framework when interrogating Element Management Systems (EMS) such as the Alcatel 5620 SAM. Discovery agents are invoked when devices of specific types are found on the network by the Ping or File finder. The agents request connectivity information from devices that the finders have discovered. Discovery agents interrogate network devices for information using methods such as ICMP, SNMP, SSH, and TELNET

3 Network topology is created
Data gathered from devices is processed and a network topology is created and stored in a discovery database.

4 Network devices are classified by type and the network topology is stored
Following discovery, topology data is classified according to device type, and the topology data is stored in the NCIM topology database. Topology data is also made available to the Event Gateway, ncp_g_event, which uses this data to enrich events and to the Root-cause analysis plug-in to the Event Gateway, which uses this data to identify root cause events.

5 Network administrators configure device polling
Network Manager has a default set of polling policies. These polling policies include simple device or interface pings and more complex threshold polls against specific MIB variables. Network administrators can configure polling policies to poll a more restricted set of devices, to change polling frequency, to change the data collected, and to make other custom changes.

6 Network Manager polls the network
Network Manager polls the network based on default and configured polls.

7 Network Manager converts relevant poll results into Tivoli Netcool/OMNIbus events and sends them to Tivoli Netcool/OMNIbus
Network Manager converts the results of relevant polls into Tivoli Netcool/OMNIbus events, and sends these events to the Tivoli Netcool/OMNIbus ObjectServer, which stores the events. Poll results that are converted into Tivoli Netcool/OMNIbus events include those polls where the response indicates a device or other network failure of some sort, such as a threshold violation or an ICMP ping fail.

8 Tivoli Netcool/OMNIbus and other event sources populate the ObjectServer
Tivoli Netcool/OMNIbus probes, and potentially other network event sources, populate the ObjectServer with network events.

9 Events are enriched with topology data
Events are passed to the Event Gateway, ncp_g_event, where they are enriched with topology data. Some events are passed directly back to the ObjectServer. Event Gateway plug-ins subscribe to certain types of events. Based on these subscriptions, events are passed to the Event Gateway plug-ins.

10 Event Gateway plug-ins perform root cause analysis and other actions based on events
Event Gateway plug-ins perform various actions based on events received from the Event Gateway. For example, the RCA plug-in performs further event enrichment. The SAE plug-in generates synthetic service-affected (SAE) events based on events received. Other plug-ins take other actions based on the occurrence of certain events; for example, the Failover plug-in initiates failover based on the occurrence of Network Manager health check events. Plug-ins pass enriched events back to the ObjectServer.

11 Network Manager gathers device performance data on demand
At any time a network administrator can set up polling of specific SNMP and ICMP data on one or more network devices. Network Manager gathers this data and stores it in the NCPOLLDATA historical polled data database.

12 Topology visualization software accesses the NCIM database
The topology visualization web application, running within the Dashboard Application Services Hub application, accesses the topology within the NCIM database. Network operators can now log into the Dashboard Application Services Hub and view their network devices and components using the Network Manager topology visualization GUIs, including multi-widget views, such as the Fault-Finding View and the Network Health View, and single-widget views, such as the Network Hop View, Network Views, and Path View.

13 Event visualization software accesses the ObjectServer
The Tivoli Netcool/OMNIbus Web GUI requests the latest set of events from the ObjectServer. Any changes network operators make to these events using the Web GUI are sent back to the ObjectServer. Network operators can now log into the Dashboard Application Services Hub and view events using the **Event Viewer**.

14 Event information is requested
The Topology Visualization Web application requests event information from the Tivoli Netcool/OMNIbus Web GUI application.

15 Report data for performance reports is retrieved from the NCPOLLDATA historical polled data database
Network operators log into the Dashboard Application Services Hub, access Tivoli Common Reporting, and run performance data and other reports. The report data for performance reports is retrieved from the NCPOLLDATA historical polled data database.

Related concepts

Network layer
The network layer consists of network discovery and polling tools.

Data layer
The data layer consists of topology storage, event storage, performance reporting data storage, and root cause analysis tools.

Visualization layer
This layer consists of topology visualization and event visualization tools.

Integration with other products

Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis. Network Manager also provides extensive reporting features, and integration with other IBM products, such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Business Service Manager and IBM Tivoli Monitoring.

Standard Network Manager installation

Network Manager is designed to be installed with Tivoli Netcool/OMNIbus to enhance fault management, including root cause analysis, and correlation of alerts with the network topology. This standard installation provides the following capabilities:

- Network discovery
- Storage of network topology information using the NCIM database
- Visualization of network topology using the Network Views, Hop View, and Structure Browser GUIs
- Various network diagnosis facilities using tools including the SNMP MIB Browser, SNMP MIB Grapher, and other dedicated diagnostic tools
- Active monitoring of network availability. Alerts generated based on availability issues are forwarded to Tivoli Netcool/OMNIbus
- Monitoring of SNMP MIB values and generation of alerts when predefined thresholds are crossed
- Correlation of events with network topology information to provide event enrichment and root cause analysis features
- Visualization of events in the network visualization tools, including the Network Views, Hop View, and Structure Browser GUIs
- Ability to generate service-affected event (SAEs). An SAE is an alert that warns operators that a critical customer service has been affected by one or more events.
- Ready-to-use reports, combining event information with network topology information

Integration with other IBM products

Network Manager can be integrated with the following IBM products:

IBM Netcool Operations Insight
Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis.

IBM Netcool Configuration Manager

Netcool Configuration Manager provides extensive configuration management capabilities for network devices, as well as network policy thresholding capabilities.

If it is integrated with Network Manager, then you can use the**Configuration and Event Timeline** in the **Network Health Dashboard** to correlate configuration data with alert data.

Netcool Configuration Manager can also be integrated with Network Manager and Tivoli Netcool/OMNIbus to provide more powerful diagnostic functionality to network operators.

IBM Cognos Analytics

The integration with Cognos Analytics provides ready-to-use reports, including reports on network configuration information.

IBM Tivoli Application Dependency Discovery Manager

IBM Tivoli Application Dependency Discovery Manager provides the following functionality:

- Imports network topology information discovered by Network Manager into IBM Tivoli Application Dependency Discovery Manager to complete the view of application-to-network dependencies.
- The Network Manager inventory report is available in IBM Tivoli Application Dependency Discovery Manager.
- Allows users to launch in context into Network Views to investigate which problems in the infrastructure might be affecting application performance.
- Network Manager can also launch in context into IBM Tivoli Application Dependency Discovery Manager to display the Change History view and the Details view associated with the devices.

IBM Tivoli Monitoring

IBM Tivoli Monitoring provides the following functionality:

- Monitors the health of the Network Manager application and displays key metrics and situations that help administrators monitor the health and status of Network Manager.
- Can be used to monitor resources within the Network Manager network.
- It is possible to launch from IBM Tivoli Monitoring directly into Network Manager, although this is not an in-context launch.

IBM Tivoli Business Service Manager

IBM Tivoli Business Service Manager provides the following functionality:

- Populates the business service model using network information discovered by several applications, including Network Manager.
- Maps events from multiple sources to the resources in IBM Tivoli Business Service Manager, including those resources discovered in Network Manager. In this case resources refers to devices, interfaces, and so on.
- Troubleshoots faults in the infrastructure by launching in context from the IBM Tivoli Business Service Manager service views to one of several Network Manager topology views.

Network layer

The network layer consists of network discovery and polling tools.

About discovery

As a network administrator, you configure and run full and partial discoveries to generate a network topology.

You can keep the discovered topology up to date by scheduling regular discoveries, configuring automatic rediscovery, and manually rediscovering devices.

If new subnets or new devices are added to your network, you can use partial discovery to discover just those subnets and devices.

If you have a very large network, then you can break the discovery of your network into different network domains. Partitioning your network into domains allows you to discover your network in sections. Reasons for partitioning your network include the following:

- Scalability: Your network might be too big to be discovered in one piece.
- Geography: You might want to break the network into geographical regions, and make each region correspond to a domain.
- Logical network boundaries: You might want to discover and manage the network based on particular network boundaries.

You can also discover links between devices in different domains, and create an aggregated domain, by configuring and running *cross-domain* discoveries.

Network Manager can also collect network topology data from Element Management Systems (EMSs). Once data is collected from EMSs, it is integrated with other data collected during the discovery.

For more information on network discovery, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related concepts

About EMS-based discovery

Network Manager can be configured to collect topology data from Element Management Systems (EMSs) and integrate this data into the discovered topology.

Discovery architecture

Use this information to understand how the components of the discovery process work together to perform a full discovery of the network.

During a full discovery, the Discovery Engine, ncp_disco, detects the existence of devices on the network and queries the devices for inventory and connectivity information. This information is subsequently processed or 'stitched' together to generate a connectivity or topology model.

After a full discovery, the system classifies devices based on a predefined Active Object Class (AOC)[1] hierarchy. The network topology is stored in the topology database and can be visualized by network operators as topology maps, customized to show specific devices or specific device groupings such as subnets and VLANs.

The following figure shows how the components of the discovery process work together to perform a full discovery of the network.

[1] An AOC classifies devices based on vendor, type, and model family.

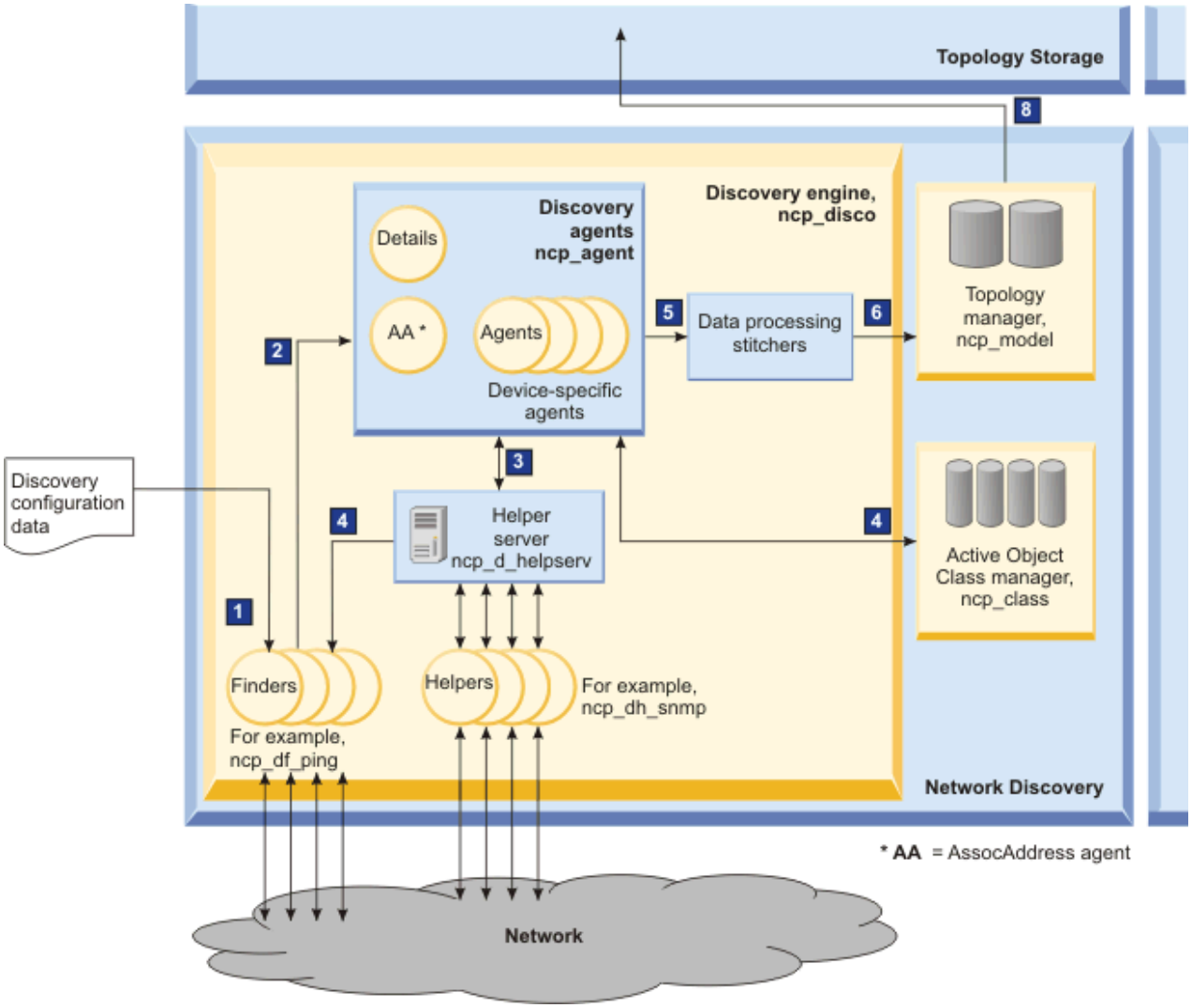

Figure 3. Full discovery data flow

1 Seed devices are discovered
Based on discovery configuration seed settings, the Discovery engine, ncp_disco, sends finders onto the network to find seed devices. The finders discover the existence of devices but do not retrieve connectivity information.

2 Agents are invoked to identify devices details, connected devices, and device type information
As devices are found, discovery agents are invoked to retrieve details of discovered devices, device connectivity information, and information specific to device types. There are multiple discovery agents to support the wide variety of network devices. Discovery agents interrogate network devices for information using methods such as ICMP, SNMP, SSH, and TELNET.

3 Connected devices are identified and device details and device type information are retrieved
Discovery agents do not have direct interaction with the network, but instead retrieve information from network devices using the Helper Server. The Helper Server manages the helpers and stores the information that is retrieved from the network. The helpers retrieve information from the network on behalf of the discovery agents. Helpers also translate agent queries into the appropriate network protocol and make requests to the devices.

4 Connected devices are discovered
Connected IP addresses identified by the discovery agents are fed back into the finders, which discover the existence of these connected devices. Discovery agents are then invoked for these connected devices (step 2) and the feedback process repeats itself until the discovery encounters the boundary delineated by the discovery scope settings.

Note: The Discovery communicates with the Active Object Class (AOC) manager, ncp_class, to classify all the devices in the topology based on vendor, type, and model family. It uses the sysObjectId value held in the device MIB and assigns the device a particular classification based on logic held within active object class files.

5 Network topology is 'stitched' together
Once all devices and device connectivity has been discovered, discovery processing stitchers are invoked. These stitchers 'stitch' together the data gathered by the agents to generate a connectivity or topology model.

6 Discovered topology is processed by Topology manager, ncp_model
The discovery sends the topology model to Topology manager, ncp_model. The Topology manager processes the discovered topology. For example, it processes linger time for devices and makes appropriate modifications. The topology is also stored in ncp_model.

7 Network topology is stored
The Topology manager, ncp_model, sends the topology to the Topology database, NCIM. The topology data in NCIM can be queried using SQL.

About cross-domain discovery

Cross-domain discovery can be configured to join two or more discovered domains together.

For performance or operational reasons, networks are often discovered in sections, known as *discovery domains*. For example, if your network is so large that discovering it in one discovery takes too long, you might choose to split network discovery into different domains.

Discovering the network in domains can be more convenient and faster. You can also choose to have different configuration options for different domains. For example, each domain has its own poll policies. However, there are disadvantages to discovering the network in pieces. If a device in domain A is connected to a device in domain B, this connection is not represented in the topology database or in the GUI. Domains must be viewed separately.

If you want to visualize multiple domains linked together in one network view, you must enable, configure, and run cross-domain discoveries. Connections between devices in different domains are found and added to the topology.

When all discovered domains have been aggregated, **Network Views** can be composed of devices from all domains. In the **Network Hop View**, searches for devices can span domains.

Note: Cross-domain network views can not be polled; only network views from individual domains can be polled.

Considerations for splitting the network into domains

Links between devices in different domains are not as easy to discover as links between devices within one domain.

It is important to scope your discovery domains to ensure the minimum of links between domains. For example, you would not normally split the network such that highly connected switches were in different domains. Natural splits for domains are often along geographical lines.

Restriction:

However you split your network, you must ensure that any given device appears in only one domain. That is, the discovery domains must not overlap if you want to join them together using cross-domain discovery.

Discovery tasks

Network administrators configure and run discoveries in order to generate a network topology. Network operators can rediscover specific devices and thereby refresh device data by simply right-clicking a device in a topology map.

Discovery user tasks fall into the following two categories:

- Configuring discoveries
- Running discoveries

Configuring full and partial discoveries

Network administrators configure network discoveries by specifying a wide range of discovery parameters. These parameters include the following:

- Discovery scope: the subnet ranges to include in or exclude from a discovery
- Discovery seeds: devices or subnets to discover first. You can seed a limited set of devices and subnets and use the discovery feedback mechanism to discover all devices connected to your seeds. You can also specify discovery seeds using other mechanisms such as a seed file
- Device access: SNMP community strings, and Telnet or SSH access parameters to enable Network Manager to access your network devices

Administrators can specify discovery parameters using the Discovery Configuration GUI or directly from the command line.

Running full and partial discoveries

Network administrators run discoveries to discover the entire network and have the ability to schedule regular full discoveries to keep the network topology up to date.

Administrators can also run partial discoveries to add new subnets or new devices to the topology. Administrators can run full and partial discoveries using the Discovery Status GUI or directly from the command line. Network Manager also provides tools to schedule regular discoveries.

About EMS-based discovery

Network Manager can be configured to collect topology data from Element Management Systems (EMSs) and integrate this data into the discovered topology.

For more information about how to configure an EMS discovery and for detailed process information about EMS discovery, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related concepts

About discovery
As a network administrator, you configure and run full and partial discoveries to generate a network topology.

Overview of EMS-based discovery architecture

Use this information to understand how Network Manager collects topology data from Element Management Systems (EMSs).

The following figure shows how Network Manager EMS-based discovery process retrieves topology data from EMSs.

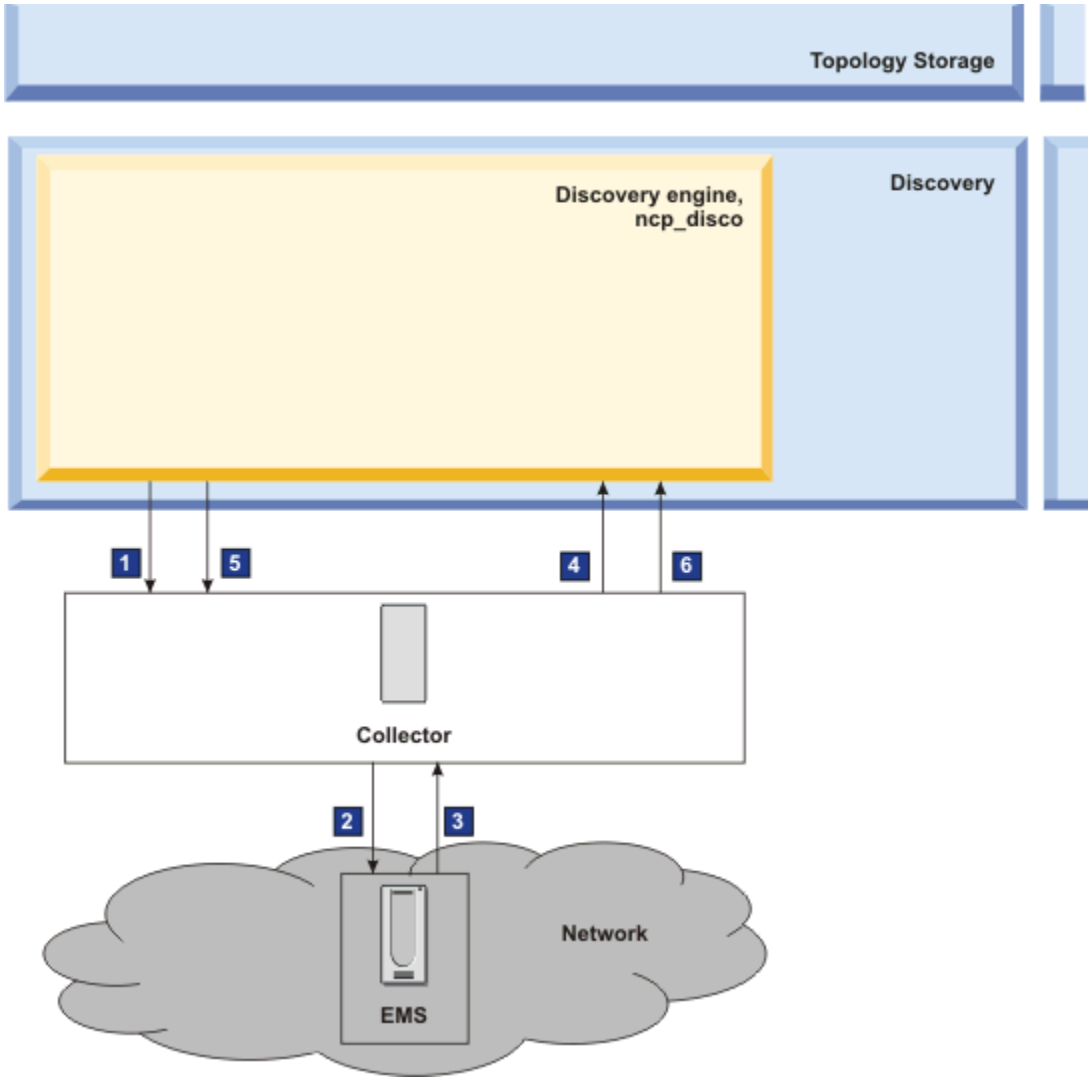

Figure 4. EMS-based high-level architecture

1 Collector finder queries EMS collector for device list
Using the Collector finder, the Discovery subsystem queries the collector to obtain a list of devices managed by the EMS. In the case of a partial rediscovery, the discovery may query for a single device or subnet only.

2 EMS is queried
The collector queries the EMS for the list of devices.

3 EMS responds
EMS responds with list of managed devices.

4 Collector provides list of devices to the discovery process
Collector responds by providing the list of devices.

5 Agents request detailed information from the EMS collector
Using a number of specialized collector discovery agents at different times during the discovery, the Discovery subsytem queries the collector for basic and detailed information about each of the devices in the list. Detailed information requested includes inventory information, layer 1, layer 2, and layer 3 connection details, and VPN information.

6 Collector provides detailed device information
Collector responds by providing basic and detailed information as this is requested.

Details of EMS-based discovery architecture

Use this information to understand how the components of EMS-based discovery work together.

The following figure shows how the components of the Network Manager EMS-based discovery process work together to retrieve topology data from EMSs.

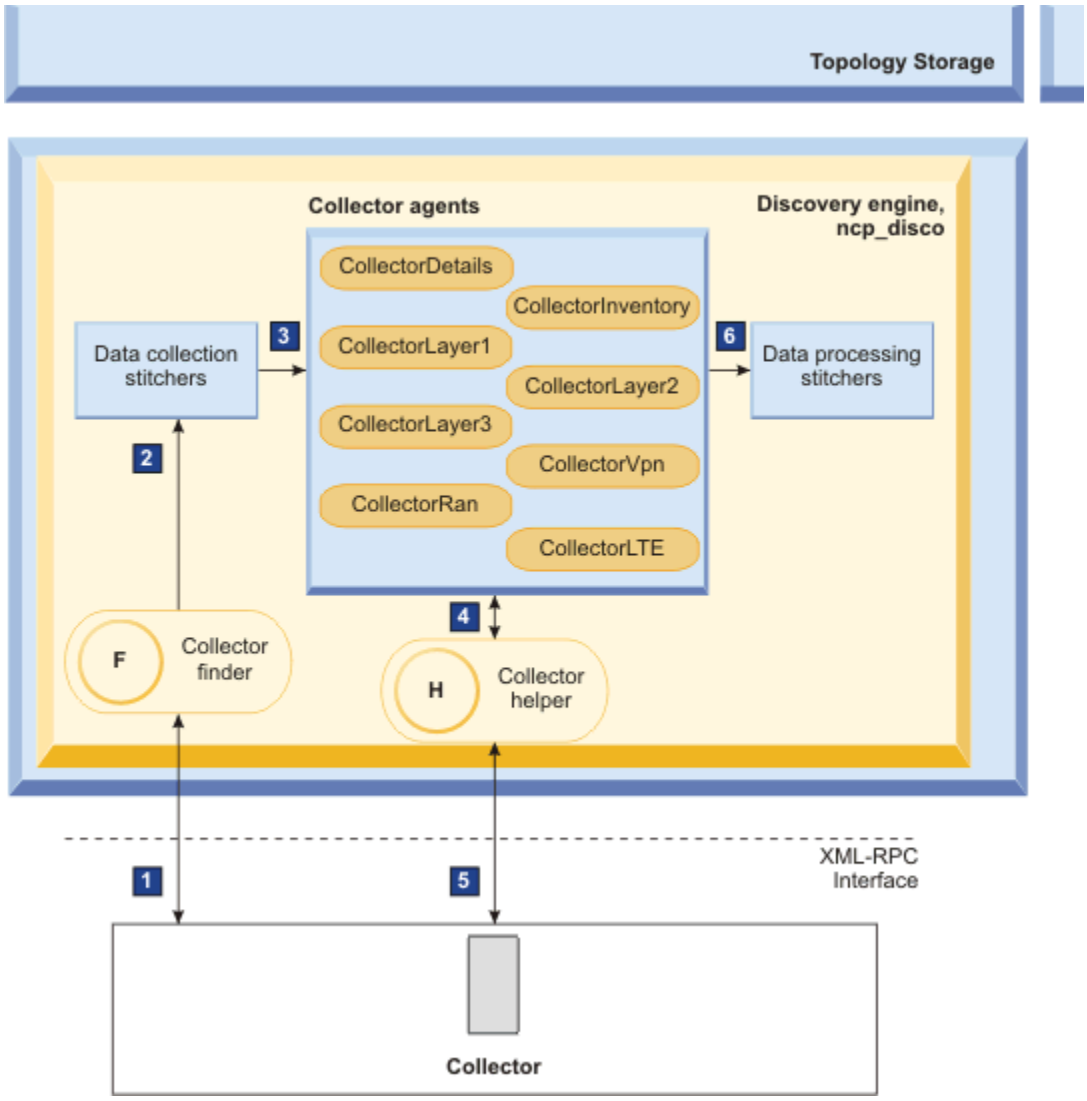

Figure 5. EMS-based discovery detailed data flow

1 Collector finder queries EMS collector for device list
The Collector finder reads the collector host seeds from a seed table in the collectorFinder database. It then queries the collectors specified in this table to get a list of devices managed by the EMSs associated with each collector.

2 Collector finder sends data to stitchers
The Collector finder sends the list of devices managed by the EMSs to the data collector collection stitchers.

3 Collector agents are invoked
The data collection stitchers invoke the Collector agents.

4 and 5 Collector agents retrieve information about the devices from the collectors
The Collector agents retrieve basic and detailed information about the devices on the collector. Each agent makes use of the Collector helper to retrieve this information. The Collector helper, ncp_dh_xmlrpc, enables Network Manager to communicate with the collectors using the XML-RPC interface. The Collector agents retrieve the following information:

CollectorDetails agent

Retrieves basic information about the devices on the collector, including sysObjectId, sysDescr, and naming data.

CollectorInventory agent

Retrieves local neighbor, entity and associated address data for each of the devices on the collector.

CollectorLayer1 agent

Retrieves layer 1 and microwave connectivity information for the devices on the collector.

CollectorLayer2 agent

Retrieves layer 2 connectivity information for the devices on the collector.

CollectorLayer3 agent

Retrieves layer 3 connectivity information for the devices on the collector.

CollectorLTE agent

Retrieves LTE-specific entity information for the devices on the collector.

CollectorRan agent

Retrieves radio access network (RAN) information for the devices on the collector.

CollectorVpn agent

Retrieves layer 2 and layer 3 VPN data for the devices on the collector.

6 Stitchers are invoked
Collector agent data is passed to the data processing stitchers.

EMS-based discovery tasks

Network administrators configure an EMS-based discovery by configuring and starting the different elements of the EMS-based discovery process. Network Manager ships with a number of ready-to-use collectors, each of which processes data from a different EMS, and with Java and Perl modules to support the development of custom collectors. Network Manager also provides CSV collectors, which process input data from CSV files.

These are the EMS-based discovery tasks:

- Creating custom collectors
- Configuring collectors
- Starting collectors
- Seeding the Collector finder
- Enabling collector agents

Creating custom collectors

Network Manager ships with ready-to-use collectors, each of which processes data from a different EMS, and with Java and Perl modules to support the development of custom collectors. Network administrators can develop custom collectors to process data from other EMSs using the Java or Perl modules provided, or using other languages, as documented in the *Tivoli Field Guide: EMS Collector Developer Guide*.

Configuring collectors

You must configure each collector so that it is able to pass data requests between Network Manager and the associated data source (for example, EMS or CSV file). Configuring the collector depends on the type of data source:

- *EMS*: specify the hostname, port, username and password of the EMS.
- *CSV file*: specify details of the CSV files and how to parse them.

You must also instruct the collector which port to listen on for XML-RPC requests from Network Manager. This is typically a one-time setup task required when a new collector is added to your Network Manager installation.

Starting collectors

Before discovery starts, all the collectors must be running.

Seeding the Collector finder

In order to enable Network Manager to find the collectors, you must seed the Collector finder. This task involves specifying for each collector, the hostname of the device on which the collector is running and the port on that device on which the collector is listening. If a collector is running on the same host as Network Manager, then you need only specify the port. This is typically a one-time setup task required when a new collector is added to your Network Manager installation.

Enabling collector agents

By default, the Collector agents are not enabled. You must enable these agents if you are running a discovery that includes collector-based discovery.

About polling

Network polling determines whether a network device is up or down, whether it has exceeded key performance parameters, and identifies inter-device link faults. If a poll fails, Network Manager generates a device alert, which operators can view in the **Event Viewer**.

Network Manager polling policies poll network devices at regular intervals, and if something does not match the polling criteria, an event is generated. For example, a polling policy might retrieve the CPU utilization of a device at a periodic interval. If the CPU utilization exceeds a predefined threshold, then an event is generated.

A set of polling policies are enabled by default. A policy specifies:

- A set of devices to poll
- Poll definitions, including threshold triggers
- Frequency of the polling
- Whether to store the data for historical reporting

Polling architecture

Use this information to understand how the components of the Network Manager polling process work together to poll network devices.

The Polling engine, ncp_poller, is the component that controls network polling. The Polling engine uses active polling operations to gather data. This data is used to trigger alerts if appropriate, and can optionally be stored in the NCPOLLDATA database for later analysis in the performance reports.

Note: By default, there is are two instances of ncp_poller running on the Network Manager server:

- `ncp_poller_default`
- `ncp_poller_admin`

Therefore by default there are two instances of ncp_poller running on the Network Manager server, each with a different service name, as specified above.

After you create polls and poll definitions, they are saved to the NCMONITOR schema within the NCIM database. The ncp_poller process reads the poll definitions from the NCMONITOR schema. The following

figure shows how ncp_poller interacts with other Network Manager components and the ObjectServer. Note that the figure does not include the historical data storage feature.

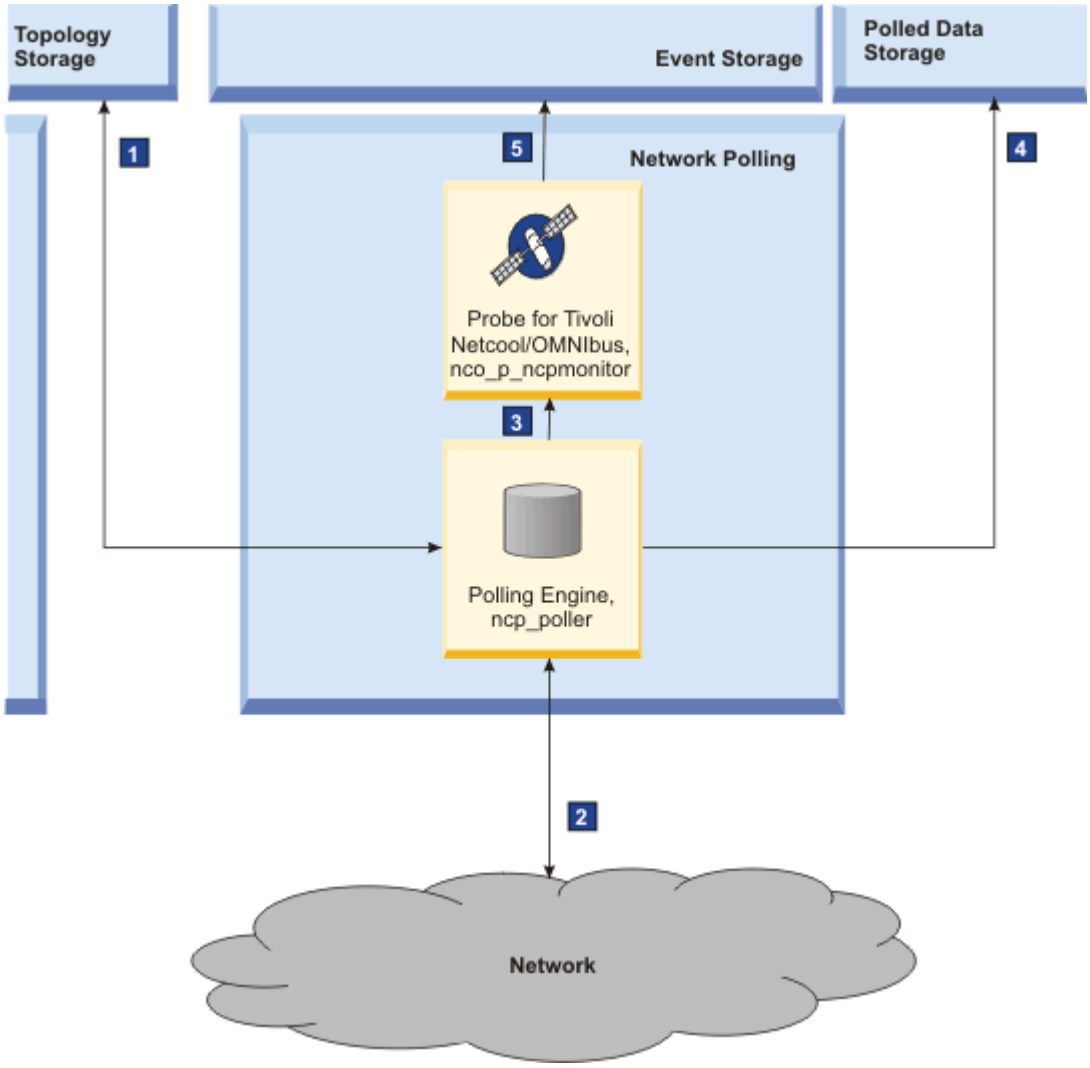

Figure 6. Polling data flow

1 Polling targets are retrieved
Network Manager has a default set of polling policies. These polling policies include simple device or interface pings and more complex threshold polls against specific MIB variables and are stored in the NCIM database. The Polling engine, ncp_poller, retrieves polling policies from the NCIM database and determines the target devices to poll, and how to poll them. Network administrators can log into the Polling GUI to configure these polling policies. For example, they can configure the system to poll a more restricted set of devices, to change polling frequency, to change the data collected.

2 Network devices are polled
The Polling engine, ncp_poller, polls network devices based on the polling policies defined in Network Manager. Devices are polled based on polling frequency and based on the set of devices specified in the polling policy.

3 Relevant poll results are converted to Tivoli Netcool/OMNIbus events
Poll results that are converted into Tivoli Netcool/OMNIbus events include only those polls where the response indicates a device or other network failure of some sort, such as a threshold violation or an ICMP ping fail. The Polling engine, ncp_poller, sends these poll results to the Probe for Tivoli Netcool/OMNIbus. This probe maps the poll results into Tivoli Netcool/OMNIbus event format.

4 Optionally polled data is stored in the NCPOLLDATA database
Depending on poll policy configuration settings, ncp_poller sends collected data to the NCPOLLDATA database, where it is stored and can be retrieved using reports. The NCPOLLDATA database should reside on the same server as the NCIM database for optimal performance.

5 Events sent to ObjectServer
Probe for Tivoli Netcool/OMNIbus sends the converted event data to the Tivoli Netcool/OMNIbus ObjectServer. Tivoli Netcool/OMNIbus and other probes also sent events to the ObjectServer.

Polling tasks

Network Manager has a default set of polling policies. These polling policies include simple device or interface pings and more complex threshold polls against specific MIB variables. Network administrators can configure polling policies to poll a more restricted set of devices, to change polling frequency, to change the data collected, and to make other custom changes. Administrators can also enable and disable polling policies. They can also set a device or component to an unmanaged state to suspend it from Network Manager network polling

Polling tasks fall into the following categories:

- Configuring polling policies
- Configuring the multiple poller feature
- Suspending polling of specified devices

Configuring polling policies

Network administrators can customize how Network Manager polls discovered devices by modifying polling policy parameters. These parameters include the following:

- Polling frequency
- Whether to store historical data for the poll to be used in performance reporting
- The set of devices or interfaces to poll. Devices can be selected based on device class. In addition, the network administrator can create an SQL filter to poll a more restricted set of devices or interfaces.
- Which data to collect from the polled devices. The data to poll for is defined using poll definitions.

Network administrators configure ping, link-state, and threshold polls using poll definitions. The poll definition specifies whether the polling policy should simply ping a device or interface, or should apply a threshold value to a MIB variable within the device MIB. A threshold violation causes Network Manager to generate a network event, which network operators can view in the **Event Viewer**.

Configuring multiple polling engines

Network Manager provides a mechanism to help distribute the load due to polling, by configuring multiple polling engines . If the default Polling engine cannot handle the polling demands for your network, then the network administrator can configure multiple polling engines on the Network Manager server. Administration tasks here include the following:

- Deploying additional pollers on the Network Manager server
- Removing pollers if these are no longer being used to poll the network

Suspending polling of specified devices

Network administrators can suspend polling of devices and specific interface types. Administrators can specify files containing lists of devices for which polling is to be suspended. Network operators can suspend polling of individual devices.

Data layer

The data layer consists of topology storage, event storage, performance reporting data storage, and root cause analysis tools.

About topology storage

Topology data is stored in the Network Connectivity and Inventory Model (NCIM) database. Network Manager reports also use the NCIM database.

The NCIM database is a relational database that consolidates topology data from Network Manager (OSI layers 1, 2 and 3).

Topology storage architecture

Use this information to understand how the NCIM database interacts with other components of Network Manager.

The following figure shows how data flows through the NCIM database.

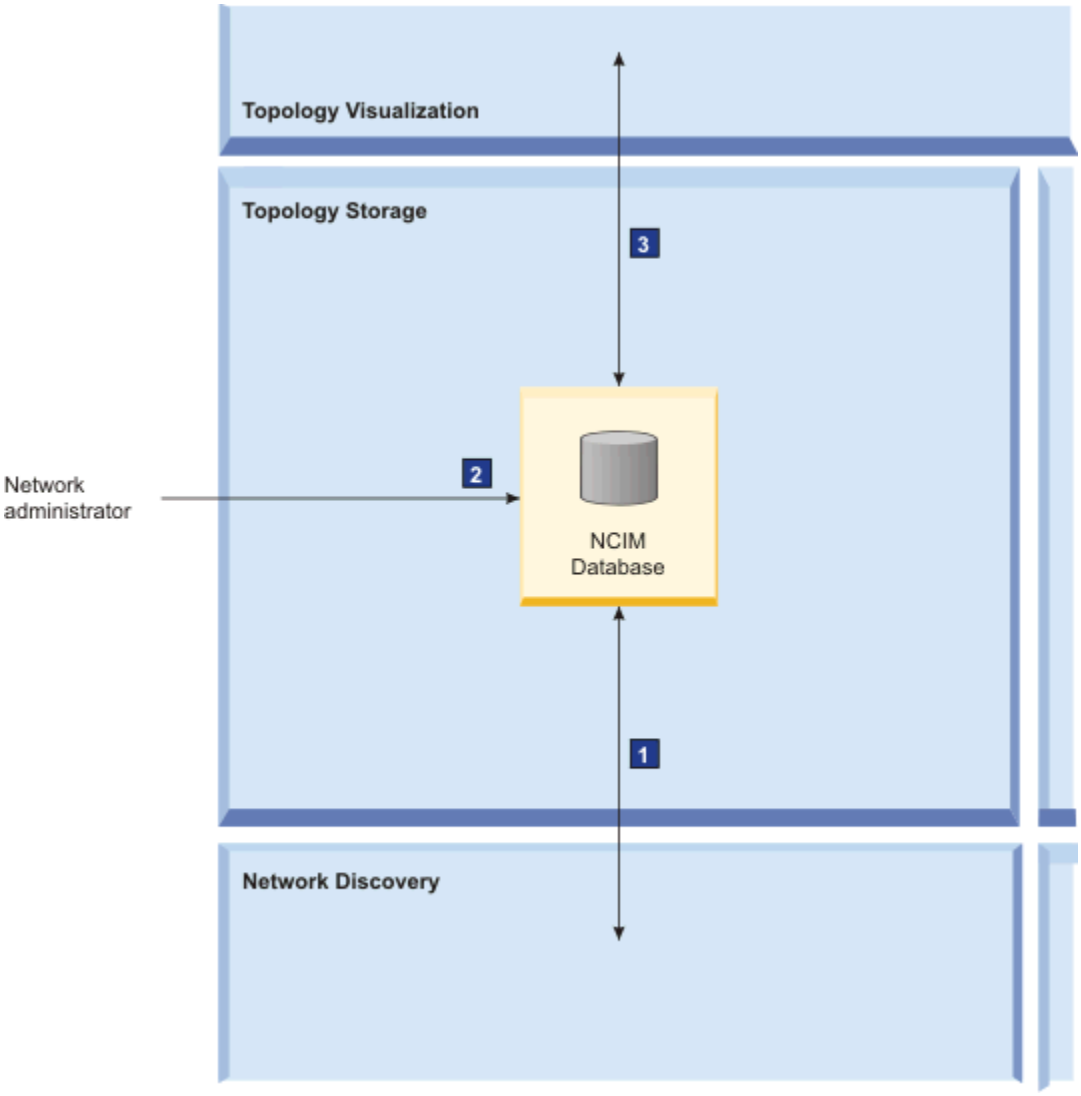

Figure 7. Topology storage data flow

1 Topology is transferred from the Topology manager, ncp_model
Following a discovery, the Topology manager, ncp_model, sends the topology to the Network Connectivity and Inventory (NCIM) database.

2 Network administrators query the NCIM database
Network administrators query the NCIM database using SQL queries to retrieve detailed topology data.

3 Topology visualization web applications access the topology
The topology visualization web applications, running within Dashboard Application Services Hub, access the topology. This enables the topology visualization GUIs, Hop View, Network Views, and Structure Browser, to display network topology and device structure.

Topology storage tasks

Network administrators query the NCIM database to programmatically retrieve topology information. Administrators can support topology enrichment from third-party data sources by adding tables and fields to the topology database.

Network administrators can also access visual representations of the network topology by viewing topology maps in the Hop View and Network Views, and by using the Structure Browser to explore details about a device.

Querying the database

Network administrators can write SQL queries to retrieve topology information from the NCIM database. The administrator can retrieve any topology information, including the following:

- Network domain information; for example, list all devices in a domain
- Device information; for example, list all devices with corresponding class name
- Containment information; for example, list all components in a device
- Port and interface information; for example, list all interfaces that have specific attributes
- Connectivity information; for example, identify all connections between routers
- Hosted services; for example, list all chassis devices hosting OSPF services
- Collection information; for example, list all devices in a specified VPN
- Enumeration information; for example, identify all hardware manufacturers listed in the database

For more information on SQL queries to retrieve topology information from the NCIM database., see the *IBM Tivoli Network Manager Reference*.

Modifying the database to support topology enrichment

It is possible to customize discovery to retrieve and store data about the discovered devices from third-party data sources. This is known as topology enrichment. For example, a discovery stitcher could be created to retrieve customer information related to devices from a third-party inventory database. This would enable network operators to see the customer associated with a given device or network event. Network administrators can support topology enrichment from third-party data sources by adding tables and fields to the topology database.

For more information on event enrichment, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

About root cause analysis and event enrichment

Root cause analysis (RCA) and event enrichment are conceptually distinct topics; however, within the Network Manager architecture, RCA is a plug-in to the Event Gateway, the process that manages event enrichment.

About event enrichment

The more information that is contained within a network event, the easier it is to determine what caused the event and who it is impacting. Event enrichment is the process of adding topology information to the event.

Network Manager gathers a lot of information about devices and topology in the network. You can use this information to enrich events with data, such as the system location, contact information, and product serial number.

The event enrichment process is known as the Event Gateway, ncp_g_event. The Event Gateway has a set of associated plug-ins, which are modular processes that receive enriched events from the Event Gateway and perform further event enrichment or take other action on these events. One of the Event Gateway plug-ins is the RCA plug-in.

Event enrichment tasks

Network Manager adds a default set of topology information to events. Network administrators can configure event enrichment to enrich events with extra topology data.

Event Gateway configuration

Examples of event enrichment include the following

- Enriching an event with main node location: administrators can configure event enrichment so that the location of the main node associated with an event is added to a field in the event.
- Enriching an event with interface name: administrators can configure event enrichment so that for all interface events, the name of the interface on which the event occurred is added to a field in the event.

Other examples of useful information that can be used to enrich events include the following:

- System contact
- Interface description
- Interface alias

To configure event enrichment, network administrators must first create new fields to hold the extra topology data in the Tivoli Netcool/OMNIbus ObjectServer. The next step is to configure the Event Gateway config database to pass the relevant topology data to the ObjectServer.

For information on how to add new columns to the Tivoli Netcool/OMNIbus ObjectServer alerts.status column, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Event Gateway plug-in configuration

Event Gateway plug-ins are modular processes that receive enriched events from the Event Gateway and perform further event enrichment or take other action on these events. One of the Event Gateway plug-ins is the RCA plug-in. Event Gateway plug-in configuration tasks include the following:

- Enabling and disabling plugins
- Modifying event map subscriptions This changes the type of events that each plug-in acts on.
- Setting plug-in configuration parameters You can set optional configuration parameters for the Event Gateway plug-ins.

For more information on Event Gateway and Event Gateway plug-in configuration, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Default event enrichment

The default set of topology information added to events includes information about whether this is a root cause event and the managed status of the entity on which the event occurred.

By default, events are enriched with the following topology information.

Table 1. Default set of topology information added to events

Field in ObjectServer alerts.status table	Description
NmosSerial	The serial number of a suppressing event. **Note:** The suppressing event is not necessarily a root cause event. There could be a chain of suppressing events from the perspective of the suppressed event.
NmosObjInst	An ID representing the device to which the event corresponds.
NmosCauseType	Indicates whether this is a root cause or symptom alert.
NmosDomainName	The name of the Network Manager domain that is managing the event. The Event Gateway sets this field value based on a topology lookup.
NmosEntityId	A unique numerical ID that identifies the Network Manager topology entity with which the event is associated. This column is similar to the NmosObjInst column, but is more granular. For example, the NmosEntityId value can represent the ID of an interface within a device.
NmosEventMap	Specifies the event map that is used to process the event. The event map defines how the RCA plugin processes the event. For example, you can configure which Event Gateway stitcher is called for which event map.
NmosManagedStatus	The managed status of the network entity for which the event was raised. Can apply to events from Network Manager and from any probe. You can use this column to filter out events from devices, interfaces, and other entities that are not considered relevant.

About root cause analysis

Within Network Manager, the term root cause analysis is used to refer to topological root cause analysis. Topological root cause analysis means that, in a situation where there are multiple events, Network Manager uses knowledge of the network topology to establish a point of failure and to identify those events that are symptomatic.

A failure on the network usually generates multiple alerts. This is because a failure condition on one device may render other devices inaccessible. Alerts are generated indicating that all of these devices are inaccessible.

Network Manager performs root cause analysis by correlating event information with topology information, and thereby determining which devices are temporarily inaccessible due to other network failures.

Alerts on devices which are temporarily inaccessible are suppressed, that is, shown as symptoms of the original, root cause alert. Root-cause alerts are shown in alert lists and topology maps with the highest severity so that operators can easily identify them.

Root cause is implemented using a series of root cause analysis rules. These rules are enabled by default. No manual configuration is required.

Root-cause analysis tasks

Network administrators can perform administrative tasks, such as enabling and disabling RCA, and changing the event maps handled by RCA in order to modify which types of events are handled by RCA. Network operators use RCA to investigate the root cause of events.

Administering RCA

Network administrators can perform various administrative tasks, including the following:

- Enabling and disabling RCA.
- Modifying which types of events are handled by RCA by changing the event maps handled by RCA.
- Changing the relative importance of different event types. When there are multiple events on the same entity, the event with the highest precedence value on the entity is used to suppress other events.
- Configuring features of RCA behavior, such as the maximum age difference between events that pass through the RCA plug-in. Events that have a difference in age greater than this specified value cannot suppress each other. The default value is 5 minutes.

For more information on RCA administrative tasks, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Investigating root cause

Network operators use RCA to investigate the root cause of events. They can determine which events are root cause and which events are results of that root cause (symptom events) and this enables them to to quickly focus on the events that are causing network problems.

For more information on investigating the root cause of network events, see the *IBM Tivoli Network Manager User Guide*.

Event Gateway and Event Gateway plug-in architecture

Use this information to understand how the Event Gateway, ncp_g_event and Event Gateway plug-ins interact with other components of Network Manager.

The following figure shows how data flows through ncp_g_event and the Event Gateway plug-ins.

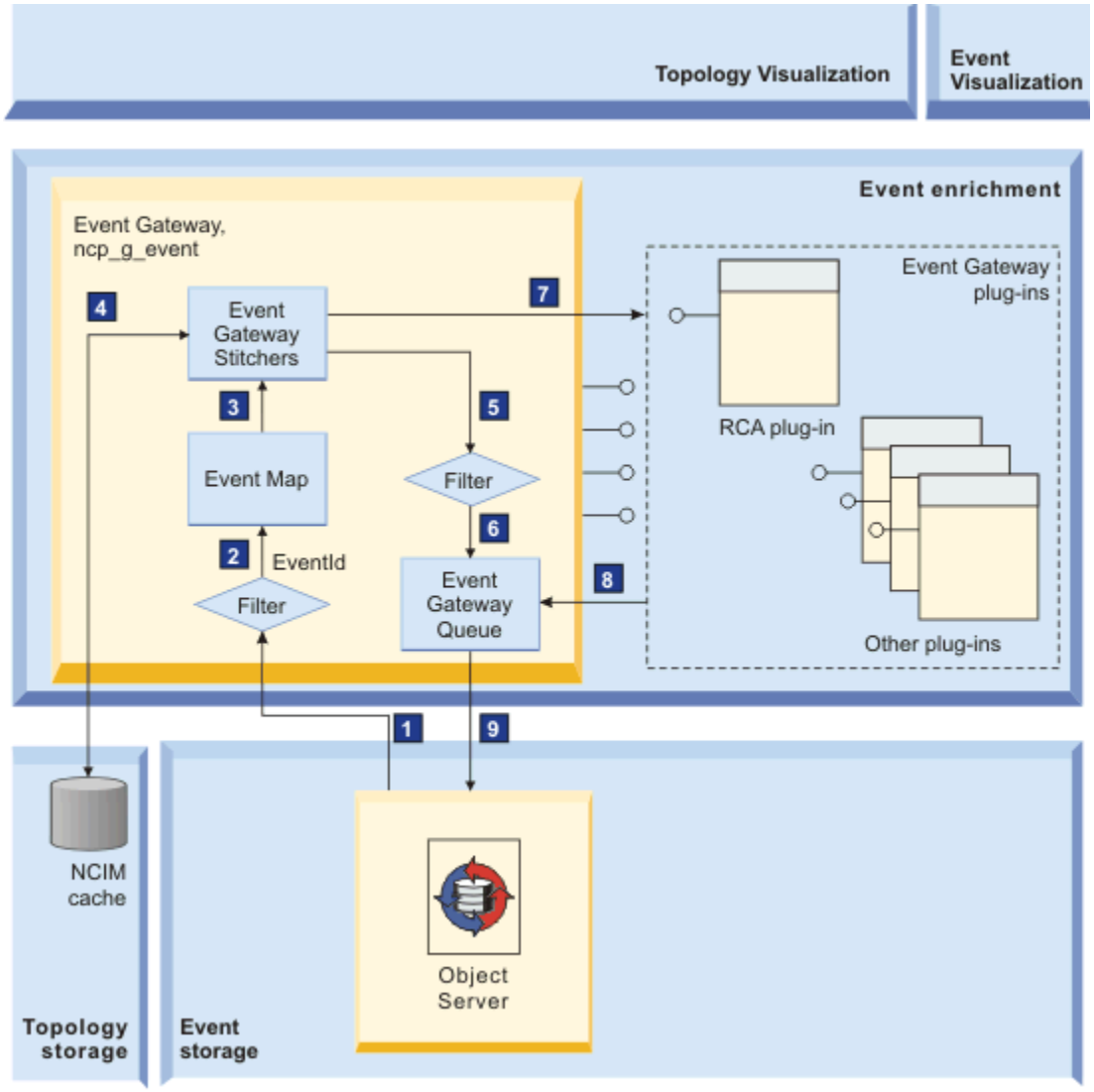

Figure 8. Event enrichment data flow

1 Event received from ObjectServer

Events are received from the Object Server at startup, upon receiving a SIGHUP command to the Event Gateway to change the configuration of the Event Gateway, and subsequently over the IDUC channel at a configurable 5 second interval. An incoming event filter rejects any events that do not have an associated LocalNodeAlias field (this field usually contains data that points to the main node device). An incoming field filter filters out alerts.status fields that do not participate in the Event Gateway processing.

2 Event map is selected

Based on the value of the event ID field in the event, the Event Gateway determines an event map to use to handle the event.

Note: The event map can also be set directly within the event by configuring the associated probe rules file or the Netcool/OMNIbus Knowledge Library to populate the NmosEventMap alerts.status field directly with an event map value. In this case the event arrives with one of its fields containing a preset event map value. However, any event map settings configured in the Event Gateway override the event map settings configured in either the probe rules files or in the Netcool/OMNIbus Knowledge Library. This enables you to locally override any event map settings configured in the network.

3 Event map points to a topology lookup stitcher
Optionally, the selected event map contains a pointer to a topology lookup stitcher. This step and the next step are optional. Some events do not call a topology lookup stitcher. For example, a Network Manager health check event passes through the Event Gateway purely in order to trigger the Failover Event Gateway plugin, and does not perform a topology lookup.

4 Topology lookup performed
The topology lookup stitcher performs a topology lookup to retrieve topology data associated with this event. Topology data is retrieved from NCIM cache.

For more information on these topics, see the following documentation:

- For information on Event Gateway stitchers, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
- For information on stitcher rules used in the Event Gateway stitchers, see the *IBM Tivoli Network Manager Reference*.
- For information on NCIM cache, see the *IBM Tivoli Network Manager User Guide*.

5 Outgoing filter applied to event
The outgoing filter only passes the fields enriched by the Event Gateway.

6 Enriched fields are placed on the Event Gateway queue
The outgoing Event Gateway queue receives enriched events from the Event Gateway stitchers (main event enrichment) and from the plug-ins.

7 Based on a return value in the stitcher, the Event Gateway determines whether to send the enriched event to the plug-ins
The Event Gateway determines whether a plug-in is interested in the event based on the state and event maps subscribed to by the plug-ins, and forward the event to the relevant plug-ins.

For information on plug-in subscriptions, and how to modify them, and on the gwPluginEventMaps and gwPluginEventStates tables that hold information on plug-in subscriptions, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

8 Plug-ins perform further event enrichment or take other action
Plug-ins process the events to which they subscribe, and either perform further event enrichment, such as the RCA plug-in, which sets a field in the event to indicate whether this is a root cause or symptom event, or take further action, such as the Disco plugin, which can initiate partial rediscovery based on an event.

9 Event data sent back to ObjectServer
Event data is sent back to the ObjectServer at a configurable interval of 5 seconds.

For more information on the outgoing Event Gateway queue and how to configure it, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

For more information on the event enrichment dataflow, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

About event storage

Event and alert data is stored in the Tivoli Netcool/OMNIbus ObjectServer. The ObjectServer is a high-speed, in-memory event database at the center of Tivoli Netcool/OMNIbus.

Network Manager is one among many possible applications that feed events to the Tivoli Netcool/OMNIbus ObjectServer. Each of these applications is called an *event source* Other event sources can include Tivoli Netcool/OMNIbus probes and monitors, Tivoli Business Service Manager, and other event management systems.

The ObjectServer receives and stores events from event sources. It eliminates duplicate events. The ObjectServer also correlates events by removing, for example, matching pairs of problem and resolution events.

For more information on Tivoli Netcool/OMNIbus, refer to the publications described in "Publications" on page ix.

Event storage architecture

Use this information to understand how the ObjectServer interacts with components of Network Manager.

The following figure shows how data flows through the ObjectServer.

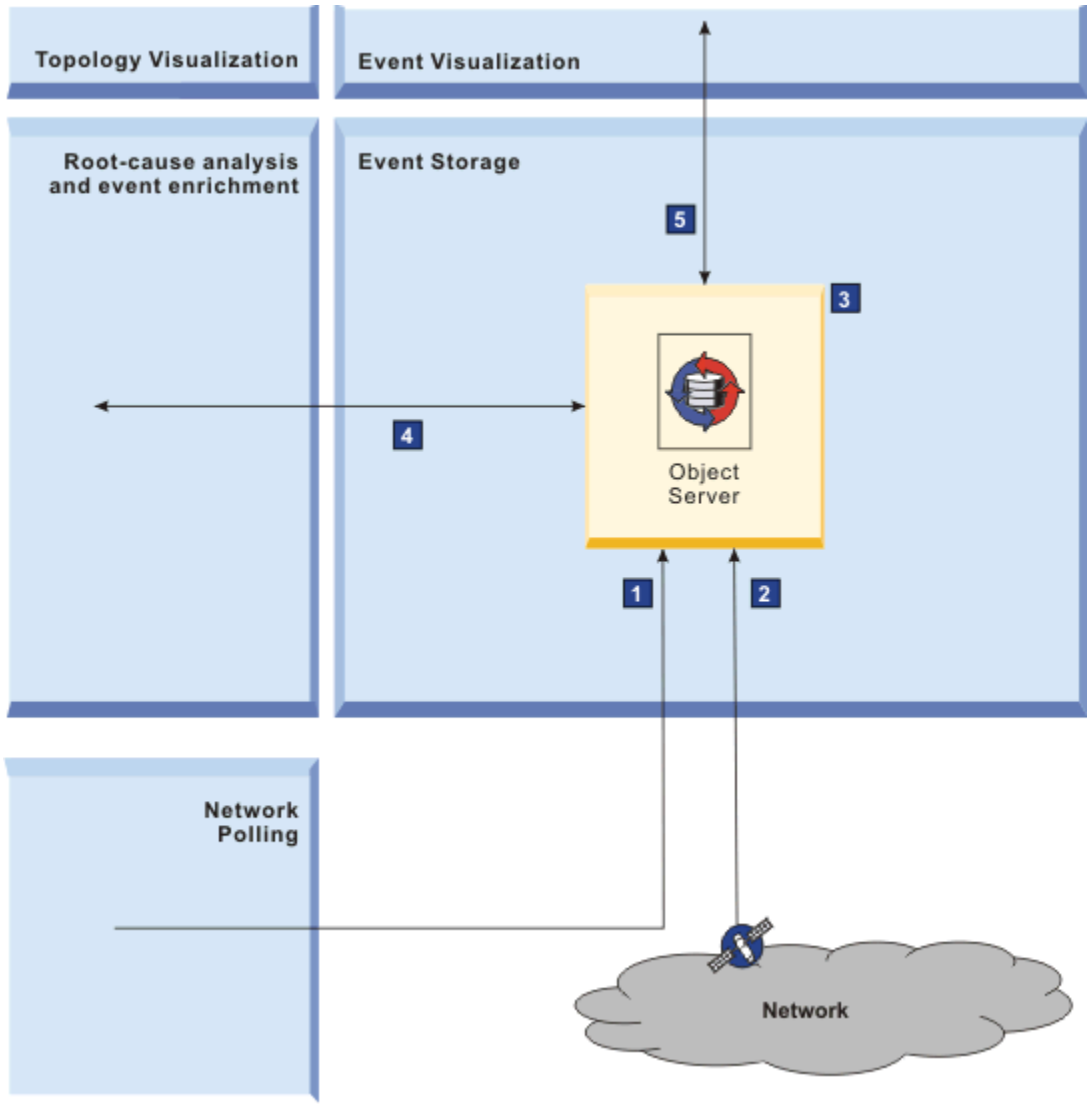

Figure 9. Event storage data flow

1 Events generated by Network Manager polls are sent to the ObjectServer
Probe for Tivoli Netcool/OMNIbus sends the converted event data to the Tivoli Netcool/OMNIbus ObjectServer.

2 Tivoli Netcool/OMNIbus probes and other event sources populate the ObjectServer
Tivoli Netcool/OMNIbus probes and potentially other network event sources, populate the ObjectServer with network events.

3 Event correlation and deduplication
The ObjectServer performs event correlation and deduplication on all the events that it stores.

4 Event enrichment and root cause analysis
The Event Gateway requests a filtered subset of events from the ObjectServer. Enriched events are returned to the ObjectServer. These events are enriched with a default set of topology information. The returned events are also modified with root cause analysis and symptom information.

5 The Tivoli Netcool/OMNIbus Web GUI accesses the event data
Web GUI requests the latest set of events from the ObjectServer. Any changes that the user makes to events using the Web GUI are sent back to the ObjectServer.

Event storage tasks

Network administrators can add fields to the ObjectServer to support event enrichment and topology enrichment activities. In addition, network administrators can perform the full range of Tivoli Netcool/OMNIbus tasks.

As part of event enrichment activity, network administrators might need to extend the ObjectServer to hold extra topology information added by the Event Gateway, ncp_g_event. For example, network administrators might add fields to the ObjectServer alerts.status table to store the following information:

- System location
- System contact

Network operators displaying information for an event in an event list would then see the standard event information, together with location information, such as the city or building in which the affected device is located, and the name of the administrator responsible for that device.

For more information on Tivoli Netcool/OMNIbus, refer to the publications described in "Publications" on page ix.

About historical polled data collection and storage

At any time a network administrator can set up polling of specific SNMP and ICMP data on one or more network devices. This data is stored in the NCPOLLDATA historical polled data database. Operators can then use the Cognos Analytics viewer to run performance reports to interpret the data. Users of Netcool Operations Insight can also visualize historical polled data in the **Network Health Dashboard**. Use this information to learn about historical polled data collection and storage architecture and some of the tasks that network administrators and network operators perform that relate to historical polled data.

Historical polled data collection and storage architecture

Historical poll data is collected and stored by the Apache Storm realtime computation system, running within Network Manager. This process prepares daily, weekly, and monthly, and annual sets of historical polling data and stores the data in the NCPOLLDATA database, thereby making this data available to reports and dashboards.

Network Manager implements the NCPOLLDATA historical polled data database (hereinafter referred to as the NCPOLLDATA database) using a database schema within the NCIM topology database. You can not separate the NCPOLLDATA database and the NCIM database.

The Apache Storm process provides a data summarization capability. This enables data to be presented, in summary form, as follows:

- Last Day (24 hours)
- Last Week (7 days)
- Last Month (30 days)
- Last Year (365 days)

Summarized data is calculated by applying an exponential weighted moving average (EWMA) to the raw polling data at regular intervals and storing the averages.

The Apache Storm process also supports advanced data pruning, archiving, and management functionality.

The following figure shows how historical polled data flows through the NCPOLLDATA database.

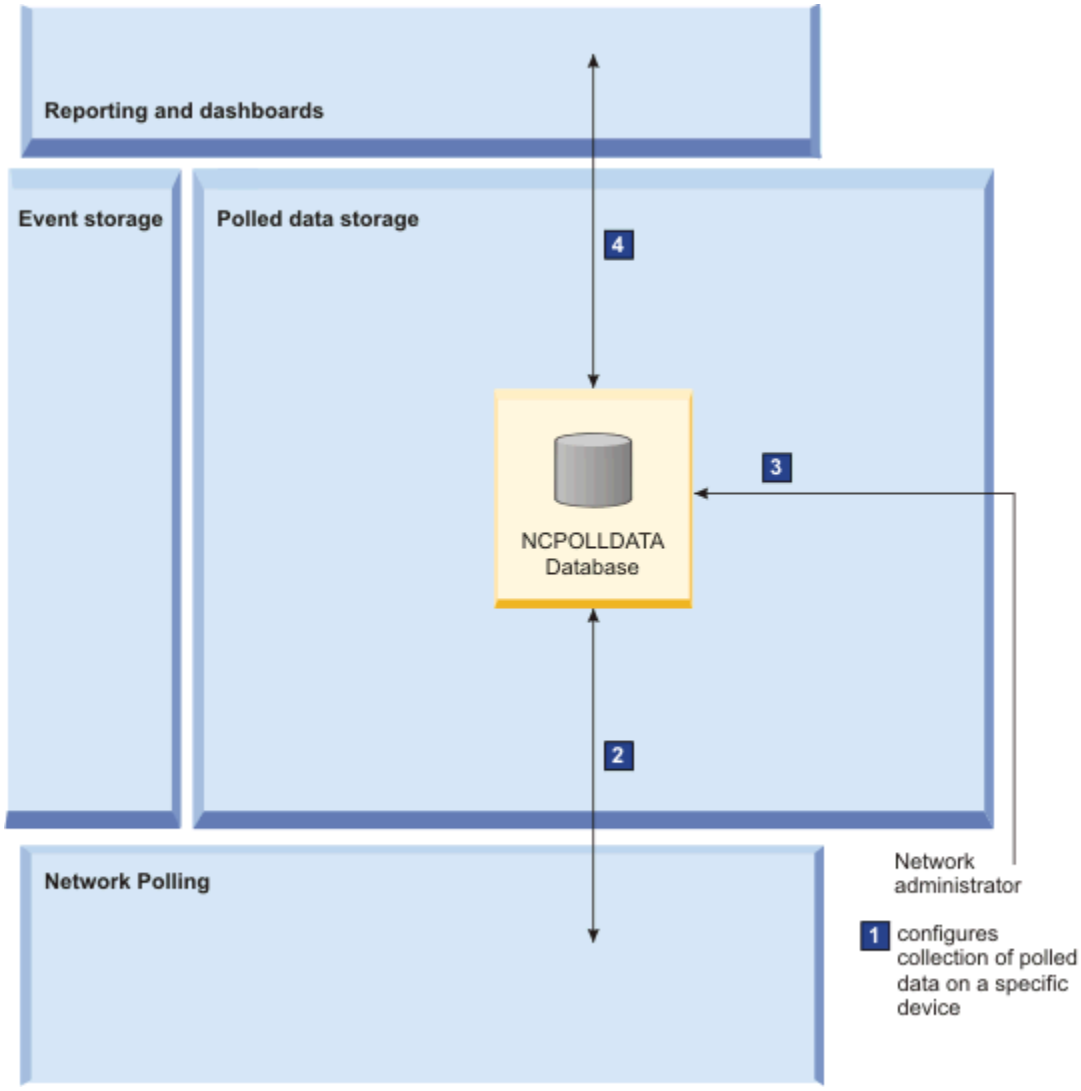

Figure 10. Historical polled data storage data flow

1 Historical polled data option is configured
A network administrator or operator configures collection of historical polled data by changing configuration settings within the polling system. Collection of historical data is selected for specific poll data metrics.

2 Network devices are polled for SNMP and ICMP data
Based on the configuration settings, the Polling engine, ncp_poller, polls the network and stores raw data in the NCPOLLDATA database. For those poll data metrics selected for historical poll data collection and processing, averages are calculated at regular intervals and are stored in dedicated tables in the NCPOLLDATA database.

3 Network administrators tune the NCPOLLDATA database
Within the Apache Storm process, Network administrators manage the storage rates for historical polled data to ensure optimum report response times.

4 Historical polled data is retrieved from the NCPOLLDATA database
Network operators access the **Network Health Dashboard** network health dashboards and run performance data reports. The historical polled data for these dashboard and reports is retrieved from the NCPOLLDATA database.

Note: The **Network Health Dashboard** is only available if you have Network Manager as part of Netcool Operations Insight.

Historical polled data collection and storage tasks

Use this information to learn about some of the tasks that network administrators and network operators perform that relate to historical polled data collection and storage.

Configuring a collection of historical polled data

Network administrators who engage in a carefully thought out historical polling data collection and storage strategy can provide a better understanding of behavior trends associated with throughput rates, device CPU and memory resources, interface usage, errors, discards, and so on. For example, such a strategy could allow network administrators to closely monitor:

- Problematic or key network devices after a maintenance period
- An area of the network where there are suspected problems

Network administrators use the **Network Polling GUI** to configure a collection of historical polled data, which typically consists of the following tasks:

- Defining the specific SNMP and ICMP data to collect, including threshold triggers for alerts
- Defining the scope and time interval for polling
- Determining what SNMP and ICMP data to store
- Starting the data collection

For more information about tasks associated with polling the network and administering historical polled data, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Running performance reports using historical polled data

Network administrators and operators can access historical polled data reports by accessing the Cognos Analytics section of Network Manager and running performance reports, or by issuing a right-click command on a selected device in a topology map.

Specifically, network administrators and operators can use the Cognos Analytics to:

- View sets of defined reports detailing trends and analysis based on SNMP and ICMP short term historical data collections for a subset of the collected data
- View generic Trend and TopN graphs of ad hoc collections of stored data

The TopN reports can help compare and focus on the right network devices and drill down to see patterns over time. Summarization reports can help extend the time period for which to compare performance results. The reports offered out of the box can be used as examples to create custom reports to meet specific needs.

For information on the tasks associated with reports, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Managing storage limits for historical polled data

Network administrators manage the storage rates for historical polled data to ensure optimum report response times and to allow the performance data reports to display a greater amount of historical data.

For more information on storage rate limits for historical polled data, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Storing Poll Data for DB2 and Oracle

You can enable the poller to store the floating point, 64-bit integer, and 32-bit integer values of the polled data.

In the following table, modify the value column type to DECFLOAT for Db2:

```
    * ncpolldata.polldata
    * ncpolldata.pdEWMAForDay
    * ncpolldata.pdEWMAForWeek
    * ncpolldata.pdEWMAForMonth
    * ncpolldata.pdEWMAForYear
```

In the following table, modify the value column type to BINARY_DOUBLE for Oracle:

```
    * ncpolldata.polldata
    * ncpolldata.pdEWMAForDay
    * ncpolldata.pdEWMAForWeek
    * ncpolldata.pdEWMAForMonth
    * ncpolldata.pdEWMAForYear
```

Visualization layer

This layer consists of topology visualization and event visualization tools.

About topology visualization

Network Manager provides two types of topology views for network visualization. It is also possible to explore the structure of network devices using the Structure Browser.

The topology visualization GUIs include single-widget views, such as the **Network Hop View**, Network Views, and Structure Browser. Default topology views also include multi-widget views, such as the Fault-Finding View and the Network Health View.

Network Hop View

The **Network Hop View** shows a selected device and all devices connected to it up to a configurable number of hops, or connections. You can use the **Network Hop View** to search the network for a specific device and display the network around that device. This view is useful for viewing the impacted area of an outage.

The **Network Hop View** provides Layer 1, Layer 2, and Layer 3 views, and converged topology views based on available layer 1 to layer 3 topology information. This GUI also presents a variety of other view types, including groupings such as IP subnets, protocols, such as OSPF, BGP, PIM adjacency information, and technologies such as RAN, LTE, and microwave technologies.

Network Views

Topology maps can be customized to show specific devices or to show specific device groupings such as subnets and VLANs.

Network administrators and operators can monitor distinct sections of the network by creating and visualizing partitioned network views using filters on any device or component attribute. For example, you can display network views based on location, technology, more complex filtered combinations of attributes.

Path Views

Path Views can display system paths such as MPLS TE paths and Virtual Circuits, as well as user-defined paths. You can trace IP paths on an ad hoc basis to view a snapshot of a network path at a specific moment. Once saved, you can monitor these paths regularly.

MIB Grapher

Graphing a MIB variable is useful for fault analysis and resolution of network problems. By graphing a MIB, operators and administrators can see a real-time graph of specific MIB variables for a network device. The MIB variable is polled at a user-defined interval and displayed in a graph over time. Optionally, you can display historical data for the MIB variable.

Multiwidget views

Multiwidget views enable you to put single-widget views, such as the **Network Hop View** and the Structure Browser together; for example, you can select a device in the **Network Hop View** and instantly see the interfaces and other components of the device in an adjacent Structure Browser widget. You can also use multiwidget views to show simultaneous topology maps and event lists.

Topology visualization architecture

Use this information to understand how the topology visualization web applications interact with other components of Network Manager.

The following figure shows how data flows through the topology visualization web applications.

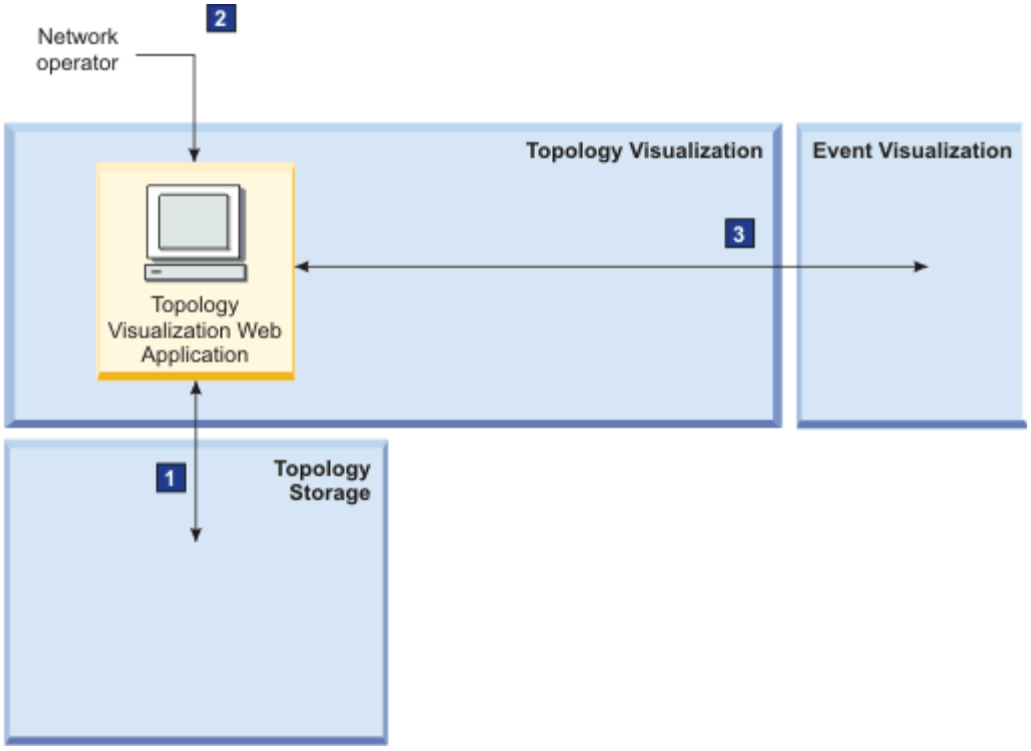

Figure 11. Topology visualization data flow

1 Topology visualization web application accesses the topology
The topology visualization web application accesses data in the NCIM database.

2 Event information requested
The topology visualization web application requests event information from the Tivoli Netcool/OMNIbus Web GUI.

3 Network operators visualize network topology
A network operator uses a web client to connect to the topology visualization web application and display **Network Hop View**, network views, and structure browser views. Multiple users can connect to the topology visualization web application.

Topology visualization tasks

Network administrators and operators can use topology visualization tools, such as the **Network Hop View**, Network Views, and the Structure Browser, to view the topology following a discovery. They can also perform diagnostic tasks on the network devices and components by launching in-context tools from topology maps.

Network administrators and operators can use topology visualization tools to perform a wide range of diagnostic and information retrieval tasks, including the following:

- Identifying network problems
- Troubleshooting network problems by running troubleshooting tools within the **Network Hop View** and network views, as listed below
- Drilling into network devices to see faulty components
- Performing SNMP MIB queries on devices for diagnosis purposes
- Investigating network routes by issuing ping and traceroute commands
- Retrieving device information, such as domain registration information, DNS lookups, and retrieving specialized protocol information from Cisco and Juniper devices

Operators can also switch between topology views to explore connectivity or associations, and to see alert details in context. Operators also have access to diagnostic tools such as SNMP MIB Browser, which obtains MIB data for devices.

About event visualization

In Network Manager events are viewed using the Tivoli Netcool/OMNIbus Web GUI event lists. Event lists can be filtered to monitor the health of specific areas of the network. Event severity is displayed to facilitate rapid identification of the more serious events. Right click tools provide immediate access to related topology views, stored information about affected devices, and real-time SNMP tools for problem diagnosis.

The Tivoli Netcool/OMNIbus Web GUI event lists provide a number of event display and event handling features, including the following:

- Event filtering: filters can be created to monitor different sections of the network. Multiple filters can be created and can be assigned to different operators based on operator responsibilities.
- Event severity: events are highlighted in the event list by severity. Events can be sorted and filtered by severity to enable rapid identification of more severe alerts.
- Right-click tools: a right-click takes the operator to any topology view in context, which displays the relationship of the affected device within the network. From the topology views, user can access a wide range of stored information about the affected device and run diagnostic tools in real time. Users can also use right click tools to acknowledge events and perform other event management tasks.

Event visualization architecture

Use this information to understand how the Tivoli Netcool/OMNIbus Web GUI interacts with components of Network Manager.

The following figure shows how data flows through the Web GUI.

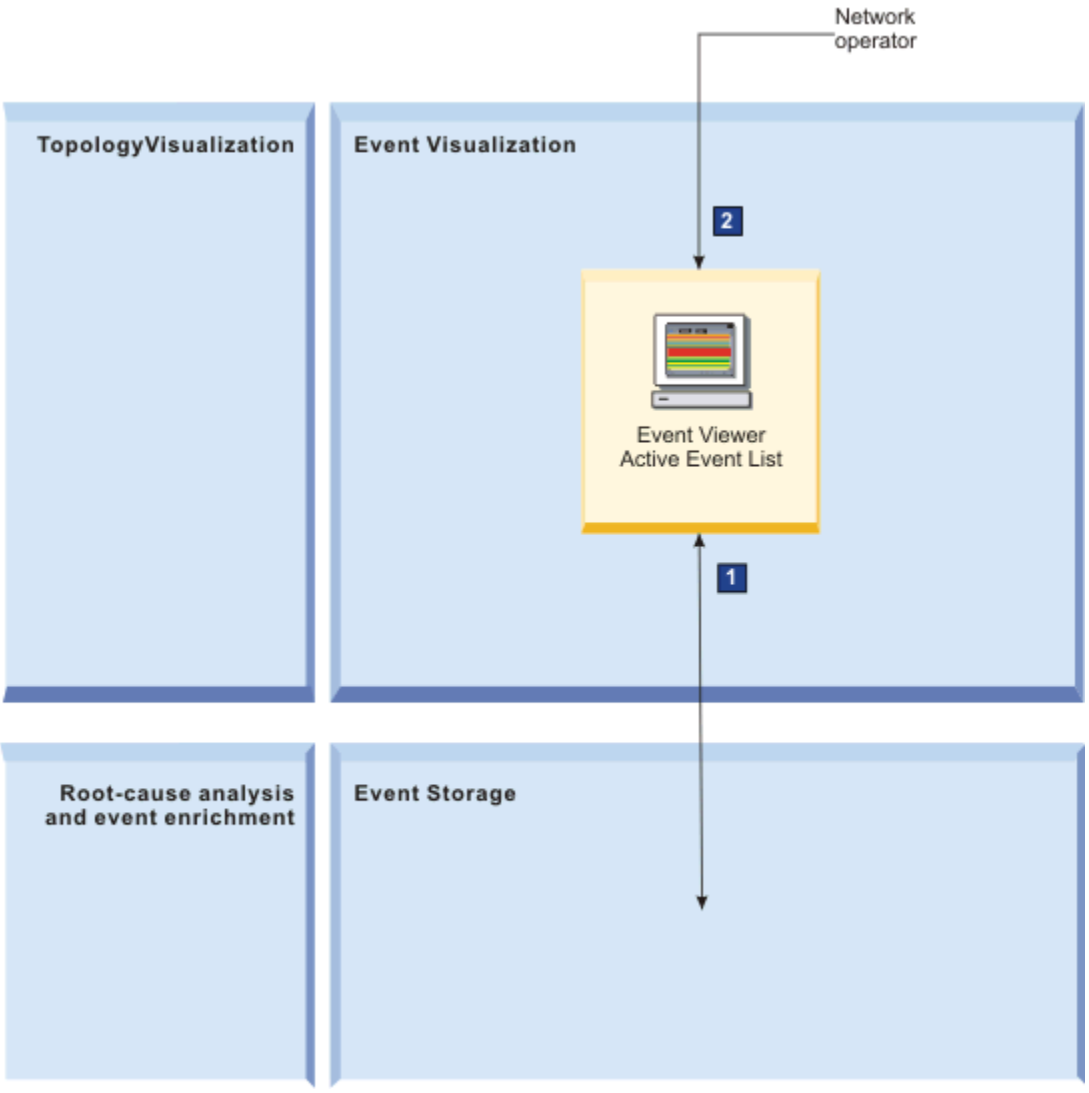

Figure 12. Event visualization data flow

1 Events are requested from the ObjectServer
The Web GUI requests the latest set of events from the ObjectServer. Any changes that the user makes to events using the Web GUI are sent back to the ObjectServer.

2 Network operators monitor events in event lists
A network operator uses a Web browser to connect to the Web GUI and display event lists. Multiple clients can connect to the Web GUI. Network operators take action on the events.

Event visualization tasks

Operators can view events lists and use event severity ratings to quickly identify high-priority device events.

Operators can switch from alert views to topology views to see which devices are affected by specific alerts. They can also identify root cause alerts and list the symptom alerts that contribute to the root cause. Alerts may be generated by the Network Manager polling mechanism, or may be received from other network management systems.

Network operators use event visualization tools to perform the following tasks:

- Viewing event lists and using event severity ratings to quickly identify high priority device alerts.
- Switching from event lists to topology views (Network Hop Views and network views) to see which devices are affected by specific events, and to explore the network in context for related issues

- Identifying root cause events and listing symptom alerts that contribute to the root cause.
- Identifying service-affected events, which are indicators that a critical customer service, such as a VPN, has a fault, and listing device events that contributed to a service-affected event

About reporting

Network Manager provides a wide range of reports, including performance reports, troubleshooting reports, asset reports, and device monitoring reports. Right click tools provide immediate access to reports from topology maps.

Reporting architecture

Restriction: Cognos Analytics and the Network Manager reports must be installed in order to be able to use the Reports feature.

The following figure shows how data flows through Network Manager reporting.

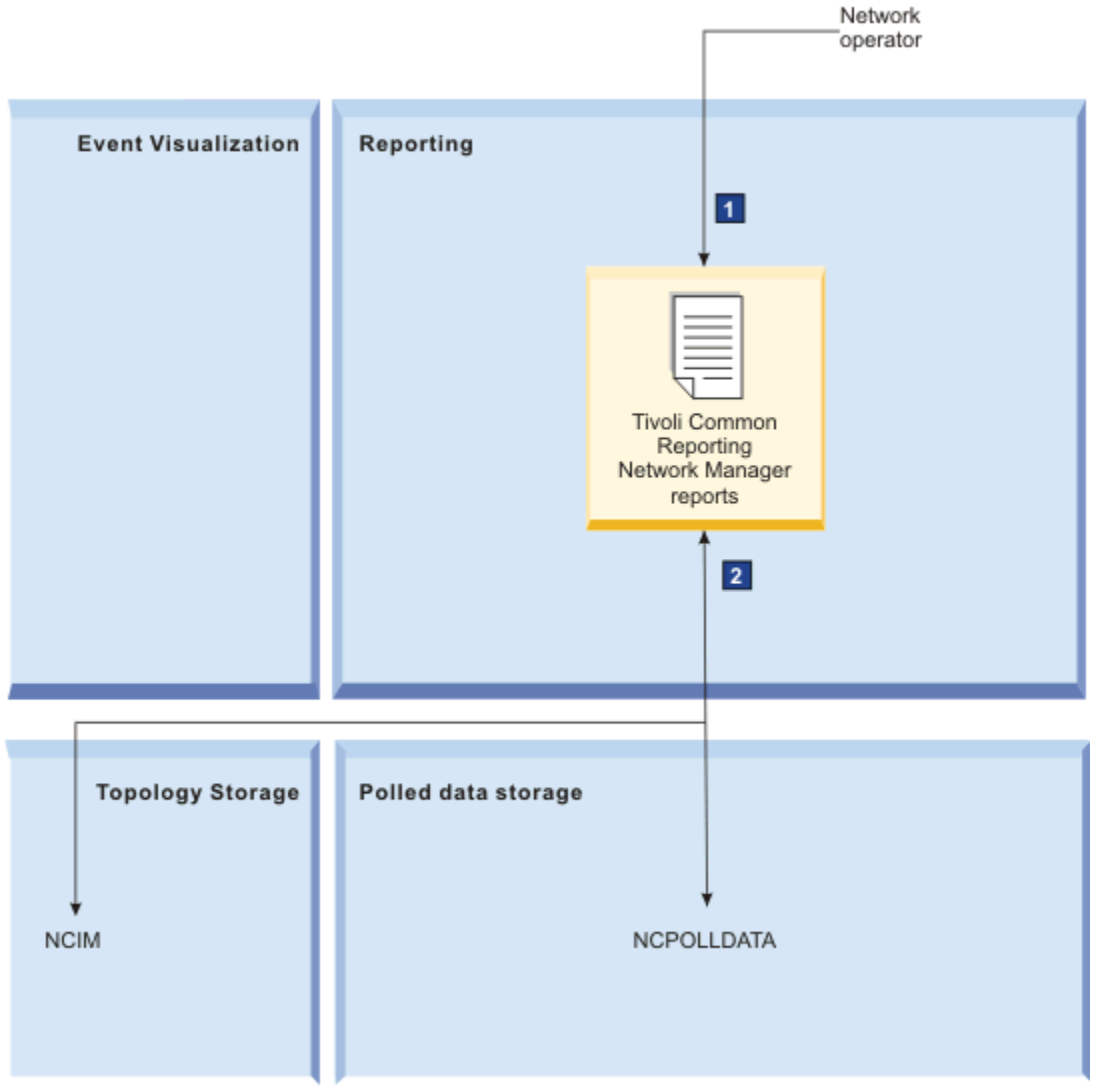

Figure 13. Reporting data flow

1 Network operator runs a report
A network operator runs a report.

2 Data is requested from the relevant database
Data is requested from the NCIM and the NCPOLLDATA databases. If the operator ran a performance report, then the latest set of historical polled data is requested from the NCPOLLDATA database.

Reporting tasks

Network Manager has a default set of reports under the following categories:

- Asset reports
- Current Status reports
- Monitoring reports
- Network technology reports
- Network View Reports
- Path View Reports
- Performance reports
- Summary reports
- Troubleshooting reports
- Utility reports

Network administrators create new reports and run existing reports. Network operators run reports.

Dashboard Application Services Hub

Dashboard Application Services Hub is the application that runs GUIs from different Tivoli products.

Dashboard Application Services Hub provides a single point for authentication and authorization of multiple web applications within that Dashboard Application Services Hub environment. Dashboard Application Services Hub also provides consolidated user management, and a single point of access for different applications. Dashboard Application Services Hub also provides the ability to create customized pages and administer access to content by user, role, or group.

For more information about single sign-on, see *Configuring Jazz for Service Management for SSO* on the Jazz for Service Management Knowledge Center at https://www.ibm.com/support/knowledgecenter/SSEKCU.

Dashboard Application Services Hub is installed automatically with the first Dashboard Application Services Hub-enabled product. Support for additional Dashboard Application Services Hub-enabled products can be added if installed in the same Dashboard Application Services Hub environment.

Network Manager web applications

Network Manager runs a number of web applications within Dashboard Application Services Hub.

Multiple web clients
Multiple web clients interact with the network topology, and distribute topology maps on demand. The topology maps include device status information, that is, the severity of the highest alert that affects a device, which is calculated from ObjectServer events. You can also use the Structure Browser to view device structure information.

The following web-client views are provided :

- Hop View
- Network Views

SNMP MIB browser
The MIB browser enables on-demand SNMP queries to network device MIBs.

MIB graphing
The MIB graphing function provides a real-time graph of specific MIB variables and MIB expressions on a network device. This graph is useful for fault analysis and resolution of network problems.

Path Views
Path Views display discovered system paths and paths through the network that are specified by the user.

Reporting
The Reporting section provides a set of default Tivoli Common Reporting reports, including performance reports. Reports are formatted for `.html`, `.pdf`, and `.csv` output, and can be formatted to PostScript. Ensure that at a minimum a reader is installed on your computer for the file format to which you output reports. For example, to output reports in `.pdf` format, install a PDF reader.

Network Discovery GUI
The Network Discovery GUI enables web-based configuration of network discovery.

Management Database Access page
The **Management Database Access** page enables web-based querying of Network Manager databases.

Network Polling GUI
Provides the front end for managing the Network Manager poll policies and definitions.

Web application architecture

To visualize the network, multiple Web clients (both **Network Hop View** and **Network Views** GUIs) connect to a single Dashboard Application Services Hub (DASH) server. The Tivoli Netcool/OMNIbus Web GUI also connects to the DASH server to enable Web-based viewing and interacting with alerts held in the ObjectServer.

The following figure shows how topology and event information is displayed in Network Manager.

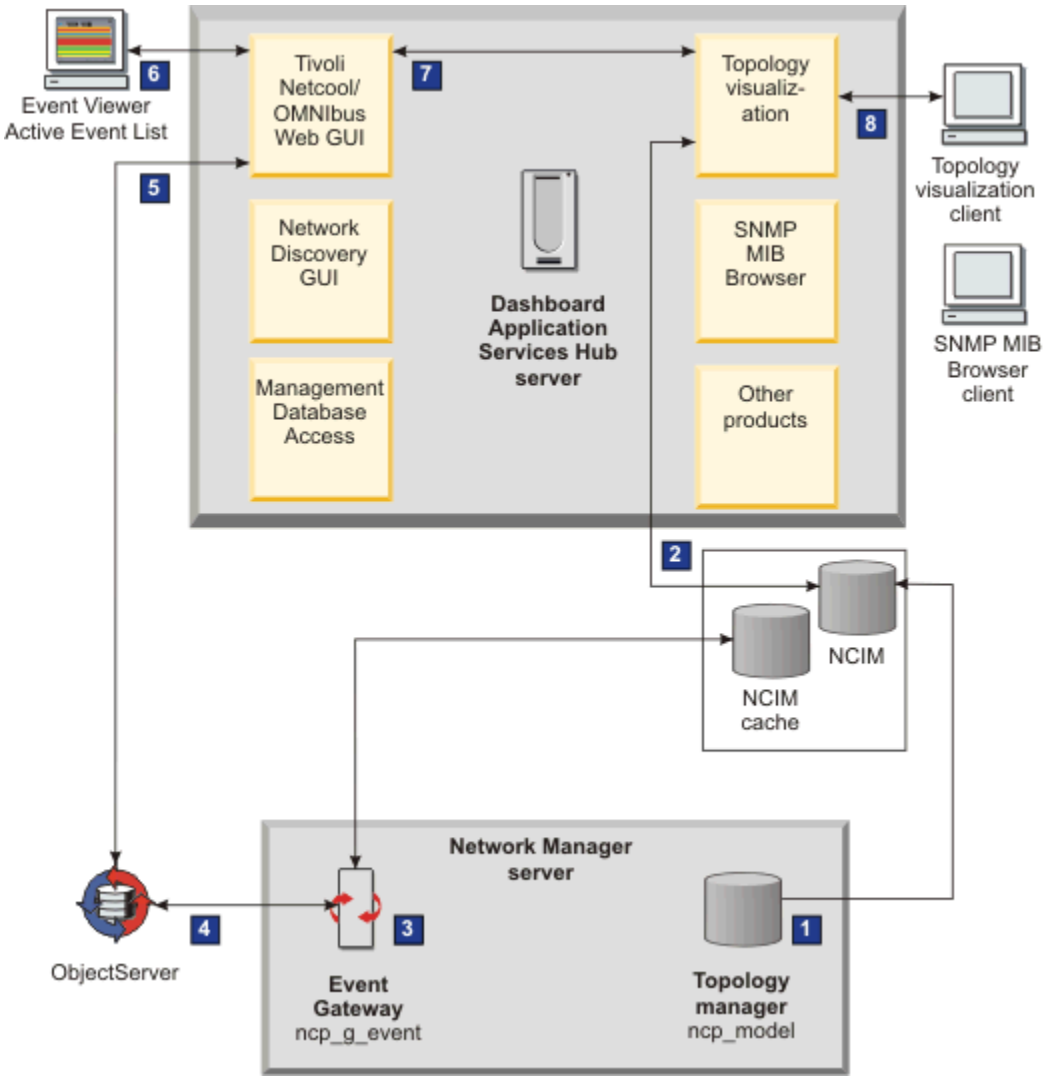

Figure 14. Visualization architecture

1 Topology transferred to NCIM
The Topology manager, ncp_model sends the topology to NCIM.

2 The Topology Visualization Web application accesses the topology
The topology is accessed by the Topology Visualization Web application running within Dashboard Application Services Hub.

3 Topology lookup performed by the Event Gateway
Topology data from NCIM cache is made available to the Event gateway, ncp_g_event.

4 Event enrichment and root cause analysis
Using topology data from NCIM cache, the Event Gateway performs relevant topology lookup operations to enrich events from the ObjectServer. The Event Gateway then sends relevant event to the RCA plug-in to perform root cause analysis on events, as configured.

5 Events requested from the ObjectServer
The Web GUI requests the latest set of events from the ObjectServer. Any changes that the user makes to events using the Web GUI are sent back to the ObjectServer.

6 Multiple client/server connections
Each Web GUI server can have multiple Web GUI clients connected to it.

7 Event information requested
The Topology Visualization Web application requests event information from the Web GUI application.

8 Events sent to topology visualization Web clients
The Dashboard Application Services Hub server sends topology maps to **Network Hop View** and **Network Views** clients on demand. The topology maps include device status information, that is, the severity of the highest alert affecting a given device, calculated from ObjectServer events.

Chapter 2. Benefits of Network Manager

Network Manager is a highly flexible system. Discovery, polling, and other parts of Network Manager can be extensively customized. Network Manager is also scalable; this means that it can discover increasingly bigger networks

Comprehensive network management

Network Manager discovers, polls, and visualizes complex networks, containing a wide range of network-type devices, such as routers and switches, and using network protocols such as MPLS, BGP, and OSPF, and technologies, such as RAN, LTE, and wifi access points.

Network Manager provides SNMP v1, v2, and v3 capabilities, and uses these capabilities to interrogate and poll network devices. Network Manager also provides the capability to discover and poll IPv6 devices.

Flexible network visualization

Network Manager provides different ways to visualize the network include network views, which show standard and customized device groupings such as subnets, VLANs, and VPNs, and the **Network Hop View**, which show a selected device and all devices connected to it up to a configurable number of connections.

Users can also navigate the interfaces and other components of a device using the Structure Browser. Multiwidget views enable you to put these views together; for example, you can select a device in a **Network Hop View** and instantly see the interfaces and other components of the device in an adjacent Structure Browser widget. You can also use multiwidget views to show simultaneous topology maps and event lists.

Built-in device and interface polling capabilities

Network Manager provides a set of ready-to-use device and interface polls, including ping polls and MIB variable threshold polls. The MIB variable threshold polls generate network events if thresholds are violated on specified MIB variables. You can customize network polling to so that events are received when thresholds are violated on any MIB variable on your network devices.

Built-in root cause analysis capabilities

Network Manager sorts through multiple network events and uses knowledge of network topology to determine a single root cause event. Network Manager highlights root cause events in event lists and in topology maps so that your operators can instantly determine where to begin troubleshooting the network.

Single-click network troubleshooting

Network Manager provides a set of ready-to-use right-click tools to perform diagnostic and information retrieval actions on network devices shown in network topology maps. For example, you can perform diagnostic actions such as ping and traceroutes and you can retrieve device information such as DNS lookups or retrieve more complex protocol information such as BGP and OSPF information. You can add right-click tools to perform any desired action on a device.

Rich network topology and event data

You can enrich network topology using data from third-party sources, and you can enrich event data with topology data.

Topology enrichment

You can customize discovery to retrieve and store data about the discovered devices from third-party data sources. For example, you could retrieve customer information related to devices from a third-party inventory database. This would enable network operators to see the customer associated with a given device or network event.

Event enrichment

You can enrich network events with any topology data retrieved by the discovery process. Standard network events on device interfaces that originate from traps show the interface index only. You can enrich these events with interface name and description data. Operators viewing network events on device interfaces can then easily identify the interface. Another example of event enrichment is where you enrich events with topology information specifying the location of the network entity affected and a contact name for that network entity. Network operators can then use this information to support problem resolution, either by directly contacting the device administrator, or by including the contact information in a trouble ticket.

Increasingly bigger network discovery

Network Manager can discover and manage increasingly bigger networks.

Related concepts

Network and deployment comparisons

Use this information to compare the example customer networks and to compare the Network Manager deployments for each of the example customer networks.

Extensive reporting capabilities

Run reports to retrieve a wide range of network data, including network performance, network assets, and network technology.

Restriction: Cognos Analytics and the Network Manager reports must be installed in order to be able to use the Reports feature.

Fully customizable content

You can build pages that contain any combination of data. For example, you can combine topology maps with device structure views and event lists. You can also combine discovery status information with event lists that show custom discovery events.

Multiple integration options

Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis. Network Manager also provides extensive reporting features, and integration with other IBM products, such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Business Service Manager and IBM Tivoli Monitoring.

Chapter 3. Deployment of Network Manager

Use this information for guidance on how to configure the physical deployment of your Network Manager installation.

Deployment scenarios

How you deploy Network Manager depends on your environment, including factors such as the size and complexity of your network and the number of operations staff who require system access.

The following are typical Network Manager deployment scenarios:

- Small demonstration or educational system deployment
- Small customer network
- Medium customer network
- Large customer network
- Very large customer network

A further deployment scenario is the following: Telecommunications company or service provider network.

Note: Failover can be applied to each of these Network Manager deployments.

This section provides general guidance to assist you in deciding how to deploy Network Manager. For more detailed information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide* and the *IBM Tivoli Network Manager IP Edition Release Notes*.

Network and deployment comparisons

Use this information to compare the example customer networks and to compare the Network Manager deployments for each of the example customer networks.

Customer networks compared

Use this information to compare the example customer networks and to identify which example most closely matches your network.

The following table lists typical features for each of the example customer networks. These values are example values only. Your specific network values might vary. In particular, you should note the following:

- With regard to the values for *Average number of interfaces per device* specified in this table, the actual interface counts can vary considerably from the average interface count. An example of this is found in MPLS networks, where the number of interfaces per device is very high in the core network, but might be as low as 2 to 3 interfaces per device for the edge devices.
- With regards to the number of devices for a telecommunications company, the value specified (15,000) is an average value. A national telecommunications company will have a far larger number of devices, a small local telecommunications company will have far fewer.

Table 2. Example customer networks compared

Feature	Demo	Enterprise				Telco
		Small	Medium	Large	Very large	
Number of devices	25	150 to 300	250 to 5,000	5,000 to 15,000	15,000 to 30,000	15,000

Table 2. Example customer networks compared (continued)

Feature	Demo	Enterprise				Telco
		Small	Medium	Large	Very large	
Average number of interfaces per device	1-2	3-5	20-30	30 or more	30 or more	1,200
Network locations	Single location	Single location	Distributed	Global network	Global network, distributed management	One or more locations
Network architecture	Flat	Flat	Flat	Complex	Complex	Complex
Number of active GUI clients	1 to 3	3	5 to 20	5 to 20	5 to 20	5 to 20
Chassis ping polling examples	Values set for demonstration purposes	2-minute intervals	2 - 5 minutes	2 - 5 minutes	2 - 5 minutes	2 - 5 minutes
SNMP polling examples	Values set for demonstration purposes	3 to 6 values at 30 minute intervals	5 to 15 minute intervals	10 to 15 minute intervals.	Intervals of 15 minutes or longer	5 values at 5 minute intervals
	SNMP v1, 2c, or 3 polling in any of the environments listed Device and interface polls in any of the environments listed.					
Tivoli product integrations	None	None	None	Netcool Operations Insight TADDM	Netcool Operations Insight TADDM	Netcool Operations Insight TADDM

Network Manager deployments compared

Use this information to compare the Network Manager deployments for each of the example customer networks.

The following table lists the settings required for the Network Manager deployments for each of the example customer networks. These values are example values only. The values that are appropriate for your specific deployment might vary.

Note: With regard to the values for *Deployment* specified in this table, these values do not take failover servers into account.

Table 3. Example Network Manager deployments compared

Settings	Demo	Enterprise				Telco
		Small	Medium	Large	Very large	
Platform	Linux x86	Any supported platform	Any supported platform	Linux	Linux	Any supported platform

Table 3. Example Network Manager deployments compared (continued)						
Settings	**Demo**	**Enterprise**				**Telco**
		Small	**Medium**	**Large**	**Very large**	
Deployment	Single server	Single server	1- 2 servers	3-4 servers	4 or more servers	3 servers
Client system	Single processor 2 GB DRAM minimum, or 4 GB DRAM for large networks Supported JRE and Internet browser					
Topology database	Default database	Default database	Db2® or Oracle RDBMS	Db2 or Oracle RDBMS	Db2 or Oracle RDBMS	Db2 or Oracle RDBMS
Number of network domains	1	1	1 - 2	2 or more	2 or more	1 - 2
Number of polling engines based on network size	1	1	Consider more than one poller	Consider more than one poller	Consider more than one poller	Consider more than one poller

Reasons for multiple domains

There are a number of reasons why you might need to partition your network into multiple domains.

You might need to partition your network into multiple domains for one of the following reasons:

- Your network exceeds a certain size. See the section *Guidelines for number of network domains* to determine whether your network requires multiple domains.
- Discovery takes a very long time. You can shorten your discovery times by partitioning your network into multiple domains.
- Operational boundaries dictate the need for multiple domains. Examples of operational boundaries include geographical boundaries and security boundaries.
- Your network contains overlapping IP addresses.

Tip:

If you are intending to run cross-domain discoveries in order to visualize links between the different domains, you must consider how the boundaries between domains affects cross-domain links. In particular, ensure that you choose domain boundaries with a minimum of cross-domain links.

Related concepts

Guidelines for number of network domains
If your network exceeds a certain size, you might need to break up the network into multiple domains. Use this information to work out the number of network domains needed for your deployment.

Guidelines for number of network domains

If your network exceeds a certain size, you might need to break up the network into multiple domains. Use this information to work out the number of network domains needed for your deployment.

Depending on the operating system, a single Network Manager domain can support approximately 1,000,000 network entities that are created during a discovery operation. Network entities include ports, interfaces (including logical interface elements), cards, slots, and chassis. It is theoretically possible to include more network entities in a single domain, but discovery might take a long time to complete.

On 64-bit Linux, the maximum memory allowed for an individual Network Manager process is not arbitrarily limited but depends on how much memory is installed on the server.

Generally, the discovery process (ncp_disco) and the topology model process (ncp_model) use the most memory.

The number of network entities that a discovery operation creates is dependent on a number of factors that might require you to create and configure extra network domains. These factors include the following:

- Device types — For example, a Cisco NEXUS or Juniper router with virtual router instances can contribute hundreds or thousands of network entities (ports, interfaces, cards, slots, and so on) per chassis.
- Network type — For example, a discovery operation performed on a local area network (LAN) typically contributes more network entities than a comparable size wide area network (WAN).
- Type of discovery agents enabled — For example, the Entity and JuniperBoxAnatomy discovery agents are inventory based discovery agents that typically create extra network entities that other agents do not create.
- Routed or switched network — For example, switched networks tend to generate more network entities than routed networks because they contain VLANs, which contain multiple entities.

The size of a Network Manager domain might be driven by business requirements. For example, a customer might require a network discovery to complete within defined daily maintenance periods. In this scenario, although a single Network Manager domain running on UNIX systems can support approximately 1 million network entities, the length of time to complete a discovery of this size might not fit within the daily maintenance period. Consequently, two scoped domains, each supporting approximately 500,000 network entities, are required to support this business requirement.

Use the following procedure to determine the number of required domains. For information on how to create and configure extra network domains, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Note: The calculations presented here provide approximate figures only. The actual number of domains required varies, depending on various factors, including the factors described previously.

1. Gather the following data:
   - Number of devices in the network
   - Average number of interfaces per device

     Note: The actual interface counts on a given device can vary considerably from the average interface count. An example of this is found in MPLS networks, where the number of interfaces per device is very high in the core network, but might be as low as 2 to 3 interfaces per device for the edge devices.
2. Apply the following equation to determine an approximate number of network entities:

   Number of network entities = Number of devices * Average interface count * *multiplier*

   Where:

   - *multiplier* = 2 for a routed network
   - *multiplier* = 3.5 for a switched network

   Note: Switched networks tend to generate more network entities because they contain VLANs, which contain multiple entities.
3. Apply the following equation to determine the suggested number of network domains:

   Number of domains required = (Number of network entities) / 1000,000

   Note: The suggested maximum number of network entities is only a rough guideline for domain sizing. The actual number of network entities per domain varies depending on various factors, including the factors described previously.

Router-centric customer

The data for this customer is as follows:

- Number of devices in the network: 60,000
- Average number of interfaces per device: 20

This customer network will produce approximately 2,400,000 network entities:

Number of network entities = 60,000 * 20 * 2 = 2,400,000

Based on the following calculation, this network requires *three* network domains:

Number of domains required = 2,400,000 / 1,000,000 > 2

Switch-centric customer

The data for this customer is as follows:

- Number of devices in the network: 1,000
- Average number of interfaces per device: 24

This customer network will produce approximately 84,000 network entities:
Number of network entities = 1,000 * 24 * 3.5 = 84,000

Based on the following calculation, this network requires *one* network domain:
Number of domains required = 84,000 / 1,000,000 < 1

Demonstration or educational system deployment

This is a small installation for use as a demonstration system or for training and educational purposes.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

This environment consists of about 25 network devices and key servers combined. All devices are in one location, on the same network subnet as the devices to be managed. There is one local GUI client session supported by the same machine that hosts the Network Manager product components. There might be one or two GUI client sessions on other machines. The network devices come from multiple vendors. The network architecture is flat. All devices are attached to a LAN and have Fast Ethernet connections. For demonstration purposes only, a number of network devices have SNMPv3, and a number of workstations have IPv6.

Within this environment the following example conditions apply:

- 1 to 3 active GUI clients.
- Chassis ping polling and some SNMP polling activity is required.
- No major Tivoli products are integrated with the system, other than the required Tivoli Netcool/OMNIbus.
- Performance reports are required for short data collection periods (typically 1 to 5 days) to match the length of the training course.

Network Manager deployment

A single-server deployment is sufficient for this type of environment. In addition to the single-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- System is an entry workstation class machine, with 8 GB of memory, dual-core processor preferred, single-core acceptable, reasonable current processor speed, and Fast Ethernet capability.
- Default database used for the NCIM database.

- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Small customer network

This customer is a company with a network consisting of about 150-300 network devices and key servers. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The primary users of the product are the networking operations staff. All devices are in one location and managed by a small operations group of a few people. Network devices come from multiple vendors. A mixture of layer 2 and layer 3 network devices are present. Approximately 20 to 30 VLANs are defined. The network architecture is fairly flat and simple. All devices to be managed are located in the same network as the Network Manager system and have Fast Ethernet connections. Internet connections are passed through a firewall and access to the systems within the protected network is available through a company VPN. The network operations staff have clients attached by means of one of the following: a local LAN, WiFi connections, or by means of a VPN established by a telecommunications service provider. Network changes are made once a month and a new discovery is anticipated at this time.

Within this environment the following example conditions apply:

- 3 active GUI clients.
- Chassis ping polling at two-minute intervals. SNMP polling at 30 minute intervals. Typically three to 6 SNMP MIB values require polling.
- No major Tivoli products are integrated with the system, other than the required Tivoli Netcool/OMNIbus.

Network Manager deployment

A single-server deployment is sufficient for this type of environment. In addition to the single-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- A single network domain is sufficient for this size of network.
- System can be any of the supported platforms. System requires 16 GB of memory, quad-core processor, and multiple physical disks in RAID 5 configuration.
- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- Default database used for the NCIM database.
- A single ncp_poller polling engine is sufficient for this environment.
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Medium customer network

This customer is a company with a central major data center and connections to several remote sites. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

This network has between 250 and 5,000 network devices and key servers of interest. Workstations, while numbering in the thousands, are not managed. Network devices come from multiple vendors. All

devices in the central location have Fast Ethernet or Gigabit Ethernet connections. Remote sites are connected by WAN connections. The devices and servers to be managed are distributed among the central and remote sites.

Within this environment the following example conditions apply:

- There are 5 to 20 active GUI clients.
- Chassis ping polling at two to five-minute intervals. SNMP polling at five to 15-minute intervals.
- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus.

Network Manager deployment

Each customer environment with this kind of network is different. The key to success is adequate memory and a careful understanding of the polling targets, combined polling rates, and the event rates. The following deployment settings are appropriate for this type of environment.

- One or more network domains are required, depending on the size of network.
- Single server deployment (up to 250 network devices and 5 to 10 concurrent users).

  Four processors.
  Up to 32 GB of memory.
  Multiple physical disks in RAID 5 configuration.
- Two-server deployment (up to 5,000 network devices and 10 to 20 concurrent users).

  Four processors for system with Network Manager.
  Four processors for system with Tivoli Netcool/OMNIbus and Dashboard Application Services Hub.
  Up to 32 GB of memory for each server.
  Multiple physical disks in RAID 5 configuration.
- System may be any of the supported platforms.
- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- Db2 or Oracle RDBMS used for the NCIM database on server with 4 processors and 32Gb RAM.
- Number of polling engines:

  Single-server deployment: 1
  Two-server deployment: One poller for chassis pings, one or more pollers for SNMP polls.
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Large customer network

This customer is a large enterprise company with a globally deployed network. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures and to support the latest network devices and network architecture.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The architecture of the network is complex. and contains the most up to date technology. For example, the network contains MPLS core networks. The network device count ranges from 5,000 to 15,000 devices, and the complexity of the network is reflected in the fact that there are 30 or more ports per device on average. Network operations are done from a central location with operations staff constantly monitoring the core network. Network devices come from multiple vendors.

Within this environment the following example conditions apply:

- There are typically 5 to 20 concurrently active GUI clients.
- Polling:

  Chassis ping polling at two to 5 minute intervals.

SNMP polling at 10-15 minutes.
SNMPv3 polling of key network devices
SNMPv1 polling for real time graphing as well as storage for performance reports.

- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus:

  IBM Tivoli Business Service Manager (TBSM)
  IBM Tivoli Application Dependency Discovery Manager (TADDM)

Network Manager deployment

Deployment choices vary depending on the size of the network. For the 5000 device network in this customer range, the choice ranges from a single-server to a two-server deployment. Key factors for success include the network response time for the targets (given that this is a county or global distribution of target devices), memory availability on the supporting servers, the polling selected and the rates of polling.

For the top end of the network (approximately 15,000 devices), a distributed, multiple domain deployment is required. In addition to the multiple-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- Deploy two domains.
- Deployment of a dedicated database server.
- Each of the servers requires the following:

  8 processors.
  Up to 128 GB of memory.
  3 disk, RAID 5 multiple disk array

- For the systems used, deploy as follows:

  Server 1: Network Manager with 36 GB of memory.
  Server 2: Tivoli Netcool/OMNIbus and Dashboard Application Services Hub with up to 12 GB of memory.
  Server 3 a customer-selected RDBMS (Db2 or Oracle) with up to 84 GB of memory.

- Systems to be deployed on Linux or UNIX platform.
- Db2 or Oracle RDBMS used for the NCIM database.
- Two polling engines:

  Use the default ncp_poller process for chassis ping.
  Create a separate ncp_poller for the SNMP polls.

- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Very large customer network

This customer is a very large global enterprise company with a simple network architecture but very large numbers of devices. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures and to support short-term capacity planning.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

Network management is done from a central location and from regional locations. The network is very large and contains over 15,000 network devices and critical servers. Network devices come from multiple vendors. The devices fall into two categories:

- Network device infrastructure with interface counts in the range of 30 or more per device.

- Managed devices with 1-2 interfaces per device.

Most of the devices are in the second category, managed devices. To manage a network of this size, the network is partitioned for management on a geographical basis.

Within this environment, the following example conditions apply:

- There are 5 - 20 active GUI clients.
- Polling:

  Chassis ping polling at two to 5-minute intervals.
  SNMP polling at 15 minutes or longer.
  SNMPv1 data collection
- Other major Tivoli products that are to be integrated with the system, other than the required Tivoli Netcool/OMNIbus:

  IBM Tivoli Business Service Manager
  IBM Tivoli Application Dependency Discovery Manager

Network Manager deployment

Assistance from an experienced IBM services group or qualified IBM Business Partner is highly advisable for a successful deployment. Multiple domains are needed, supported by a collection of individual servers, or running together on a very large system. After you survey the network to be managed, break up the network into sections that can be managed, and then assign each of the sections to a domain. In addition to the multiple-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- Multiple network domains.
- Platform selections: Linux and UNIX.
- Large systems (many processors and very large amounts of memory) can host multiple domains if the memory allocations and processor counts are acceptable.

  Memory: 32-64 GB per domain
  Processors: 4-8 per domain, depending on workloads
- Db2 or Oracle RDBMS used for the NCIM database.
- Two polling engines for each domain:

  Use the default ncp_poller process for chassis ping.
  Create a separate ncp_poller for the SNMP polls.
- Individual process memory limitations are a factor in this environment. If you are using AIX, enable large memory access.
- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Telecommunications company network

This customer is a telecommunications company and internet services provider. The purpose of this installation is to manage this customer network by alerting 24x7 network operations center staff to major failures.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The network to be managed has about 600 network devices; with an average interface count per device of 500. This is an MPLS network, and consequently the network devices are “large” in terms of their interface counts and complexity. Network devices come from multiple vendors. All devices are in one or

more locations and are managed by a small network operations group. All devices to be managed are connected via Fast Ethernet or Gigabit Ethernet.

Within this environment the following example conditions apply:

- Number of simultaneous active clients: 5-20.
- Polling requirements: chassis pings at two to 5-minute intervals; SNMP polling of 5 values at 5 minute intervals.
- Some SNMPv3 polling is in place.
- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus:

  IBM Tivoli Business Service Manager (TBSM)
  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Performance reports done once a day for key devices, used to assemble weekly capacity reports.

Network Manager deployment

A three-server deployment is needed for this type of environment. In addition to the multiple-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- One to two domains.
- A three-server deployment is advised.
- System specifications:

  System 1 (where Network Manager is installed): four processors, 32-64 GB of memory, two or more disks. Note that beyond four processors or processor cores, the core clock speed and on-chip cache can be more important than additional cores. The general rule is as follows: select the fastest 4 cores before additional cores.
  System 2: (where the Dashboard Application Services Hub and Tivoli Netcool/OMNIbus are installed) four processors, 16 GB of memory, two or more disks
  System 3: database server; 4 processors, 16 GB of memory
- Db2 or Oracle RDBMS used for the NCIM database.
- Two polling engines:

  Use the default ncp_poller process for chassis ping.
  Create a separate ncp_poller for the SNMP polls.
- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

LTE 4G wireless telecommunications company network

This customer is a large wireless telecommunications company providing 4G wireless telephony services using their LTE (Long term Evolution) infrastructure. The purpose of this installation is to manage this customer network by alerting 24x7 network operations center staff to major failures.

The following sections provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The network to be managed has about 5000 eNodeBs, together with a further 3000 devices, which are either in the associated Evolved Packet Core (EPC) network or functioning as mobile backhaul router devices. The Network Manager entity count discovered for this network would typically be as follows:

- For the eNodeB devices: on the order of 20 to 25 entities per eNodeB.
- For the EPC network and backhaul equipment devices: on the order of 10 to 15 entities per device.

The LTE eNodeB and associated equipment is provided by multiple vendors which can vary in complexity and scale. These devices are distributed across many locations, as is typical in a 4G mobile network. All devices to be managed are connected using Fast Ethernet or Gigabit Ethernet. The topology and network inventory data discovered by Network Manager is received from vendor-specific EMS systems, and is processed by corresponding vendor-specific Network Manager collectors.

Within this environment the following conditions typically apply:

- Number of simultaneous active GUI clients: 5 to 20.
- Polling requirements: none, since topology data is received from the EMS, hence no polling of devices is assumed.

Network Manager deployment

A three-part deployment is needed for this type of environment.

1. Network Manager core components.
2. Dashboard Application Services Hub and Cognos Analytics.
3. NCIM topology database.

These three parts can be deployed on servers (single or multiple) or on virtual machines (single or multiple). A single domain is sufficient for this type of environment. Furthermore, the following deployment settings are appropriate:

- Network Manager core components
  - 4 to 6 processors.
  - Approximately 20 GB of memory.
  - 50 GB of disk space.
- Dashboard Application Services Hub and Cognos Analytics
  - 4 to 6 processors.
  - 6 to 8 GB of memory.
  - 20 GB of disk space.
- NCIM topology database
  - 4 processors.
  - 10 GB of memory.
  - 50 GB disk space minimum configured in a suitable RAID configuration, to provide required level of fault tolerance, reliability, and performance.
  - Db2, or other supported database platform.

In addition, the following GUI client system is appropriate:

- Single processor.
- 3 GB of memory.
- Supported JRE and Internet browser.

Deployment considerations

You can deploy your entire Network Manager installation on a single server or as a distributed installation.

During a Network Manager installation, you install a number of Network Manager components' including the following:

Network Manager core components
This component consists of the core Network Manager processes: network discovery, polling, root cause analysis and event enrichment.

NCIM database
This database stores topology data.

Tivoli Netcool/OMNIbus
This component consists of the Tivoli Netcool/OMNIbus event management software. Many customers choose to have a trouble-ticketing system integrated with Tivoli Netcool/OMNIbus.

Network Manager GUI components
This component includes the Dashboard Application Services Hub GUI framework, Web GUI components, Jazz for Service Management, and Java.

Other components
Other components include Cognos Analytics and Network Manager reports.

The objective of the installation is to place these components on one or more servers.

Restriction: You must not use different versions of the same products or components together, unless advised otherwise by instructions in the IBM Knowledge Center or by IBM Support. If you need multiple instances of a product or component, you must install or upgrade them to the same version and fix pack. You must also ensure that the same set of test fixes, if any, are installed. For example, if you need multiple instances of the Network Manager GUI Components in one deployment, ensure that they are the same version, fix pack, and test fixes.

The following are typical Network Manager deployment configurations:

- Single-server deployment
- Distributed deployment: two servers or more

The factors that require an increased number of servers in a distributed deployment include the following:

- Active event rates
- Amount and rate of stored polling data
- Device status polling rates and number of polling targets
- Network response times for polled targets
- Discovery frequency and
- Size of the network to be discovered (for each domain, where there are multiple domains)

Note: These deployment configurations do not take into consideration requirements for other product integrations.

In addition, you must consider deployment of appropriate systems to support GUI client sessions.

Also, IPv6 dual stack support is required if workstations or network devices have IPv6.

Single-server deployment

Single-server deployments are appropriate for small demonstration or educational systems, and for systems to support small to medium customer networks.

Restriction: A limitation of a single-server deployment is that Tivoli Netcool/OMNIbus and Network Manager must be upgraded at the same time. All upgrades to major releases must be done at the same time to avoid compatibility issues. A major release is a release that has its own documentation set, for example, Tivoli Netcool/OMNIbus V8.1.0. Fixpacks can be applied at different times.

Distributed deployment: two servers or more

In distributed deployments, Network Manager components are distributed across multiple servers, that is, two servers or more. Here are some guidelines for distributed deployments:

- Two-server deployments are appropriate for the top end of the range of medium customer networks.
- Deployments might require three servers or more in situations where there are multiple network domains.

- Three-server deployments might also be deployed where it is determined that a separate server is required to support a relational database product that provides topology data storage. In addition, a separate database server enables the relational database to support multiple applications, in addition to Network Manager.

Two-server deployment

An example of a two-server deployment consists of the following allocation of host workstations:

- *Server 1*: Network Manager core components, Tivoli Netcool/OMNIbus, and the NCIM database. The core components are the network discovery, polling, root cause analysis and event enrichment components.
- *Server 2*: Dashboard Application Services Hub with associated Network Manager web applications.

Three-server deployment

An example of a three-server deployment consists of the following allocation of host workstations:

- *Server 1*: Network Manager core components.
- *Server 2*: Tivoli Netcool/OMNIbus
- *Server 3*: Dashboard Application Services Hub with associated Network Manager web applications, together with the NCIM database.

Client systems

You must consider deployment of appropriate systems to support GUI client sessions.

The following system specification provides support for a wide range of end-user activities on GUI client sessions:

- Larger display supporting comfortable viewing at higher resolution, such as 1280x1024
- Current speed single or dual core processor
- 3 GB of memory
- Supported JRE and Internet browser
- Fast Ethernet.
- Processor specification:

  For normal topology displays or event displays
  Single processor with the following speeds: 1 GHz or better, as found on many laptops, 2.4 GHz, as found in many workstations

  Enhanced time to display larger or complex topology maps and enhanced display of MIB graphs
  A very current processor (3.0 GHz or better) typically available in the latest workstation class systems.

Deployment examples

Use these examples of Network Manager to help you plan your deployment architecture.

Example simple deployment architecture

Use this example to familiarize yourself with the architecture of a simple Network Manager deployment.

Components

This example simple deployment consists of the following components:

- One ObjectServer virtual pair.
- One Dashboard Application Services Hub server.

- One Network Manager installation running one domain with failover.
- One instance of the NCIM topology database.

The following figure shows the architecture for this deployment.

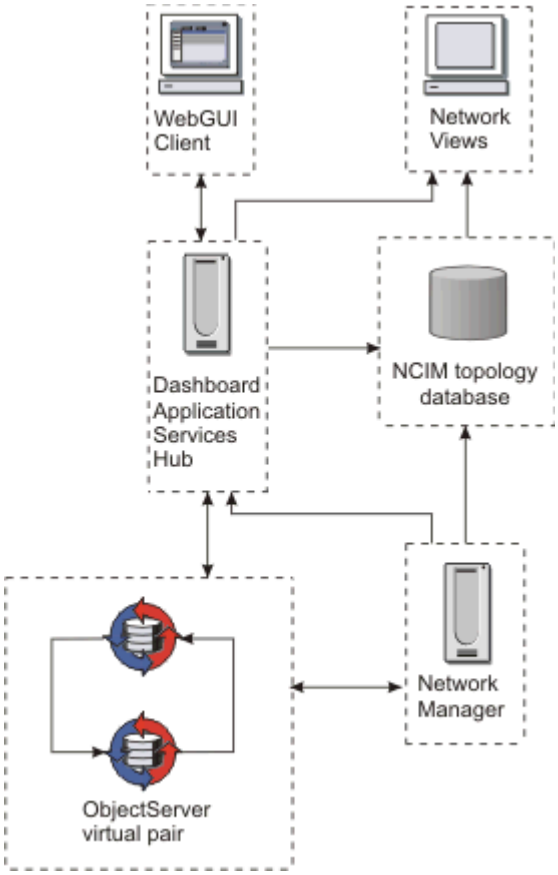

Figure 15. Simple deployment architecture

Allocation of host workstations

The following figure shows an example allocation of host workstations for this deployment.

Note: If you have a particularly large topology, you might want to install the topology database on its own server. This decision depends on the specification of your machines and how you want to spread the load between them.

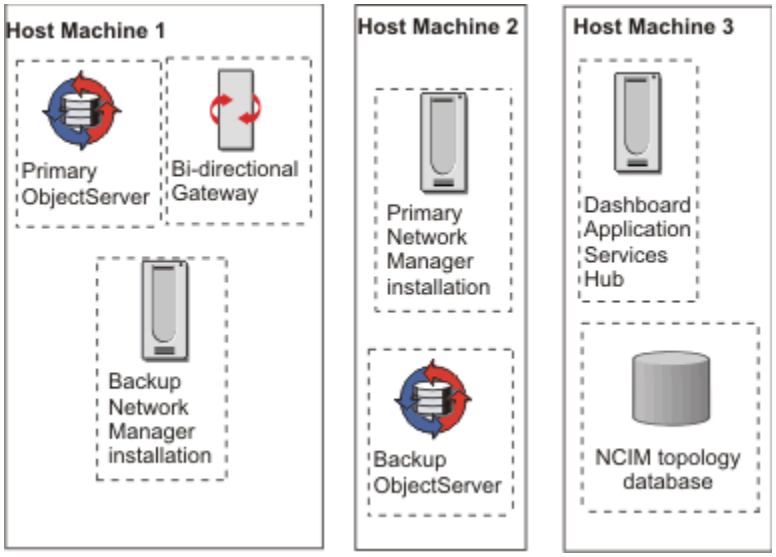

Figure 16. Simple deployment host machine allocation

Steps to install a simple deployment

The following steps provide an overview of the tasks required for this deployment, and help plan for a similar deployment. .

To install the deployment described above, perform the following steps:

1. Install the topology database on host machine 3, create the necessary tables, and start the database.

   Note: The topology database must be installed and started before you start the Network Manager core components so that discovery data can be saved.
2. Install the following ObjectServers and related components:

   a. Install the primary ObjectServer and the Bi-directional Gateway on host machine 1.

   b. Install the backup ObjectServer on host machine 2.
3. Configure and run the ObjectServers.

   Note: The ObjectServers must be running before the Network Manager core components are started.
4. Install the primary Network Manager core components on host machine 2.
5. Install the backup Network Manager core components on host machine 1.
6. Install the Network Manager GUI framework on host machine 3. The GUI framework includes the following software:

   - WebSphere Application Server
   - Dashboard Application Services Hub
   - Network Manager GUI components
   - Tivoli Netcool/OMNIbus Web GUI
   - Cognos Analytics

   Tip: If you install the Dashboard Application Services Hub on a machine with no other products, performance is likely to be better than if you install it on a machine with other products.

   Note: The Network Manager core components must be installed before the Network Manager GUI framework.
7. Configure the primary Network Manager for failover and start it.
8. Configure the backup Network Manager for failover and start it.

Example large deployment architecture

Use this example to familiarize yourself with the architecture of a large Network Manager deployment.

Components

This example deployment consists of:

- One ObjectServer and one Network Manager installation in London. The London domain sends events and topology to San Francisco.
- One ObjectServer and one Network Manager installation in New York. The New York domain also sends events and topology to San Francisco.
- One ObjectServer and one Dashboard Application Services Hub installation in San Francisco. The ObjectServer in San Francisco consolidates the events from London and New York. The Dashboard Application Services Hub server in San Francisco can access topology from both London and New York, but does not consolidate the topologies. Clients anywhere in the world can connect to the Dashboard Application Services Hub server, and view topology from London and New York.

The following figure shows the architecture for this deployment.

Note: For a large deployment of this sort, network latency across the WAN should be taken into account. This is especially important if if the poller is expected to store a lot of historical data. .

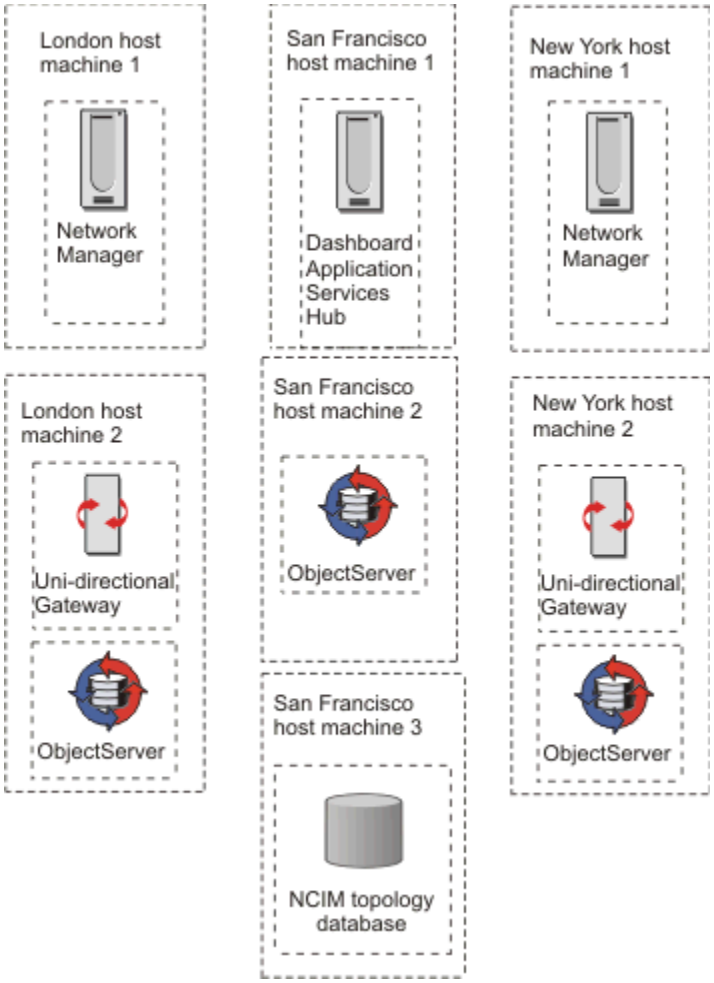

Figure 17. Large deployment architecture

Allocation of host workstations

The following figure shows an example allocation of servers for this deployment.

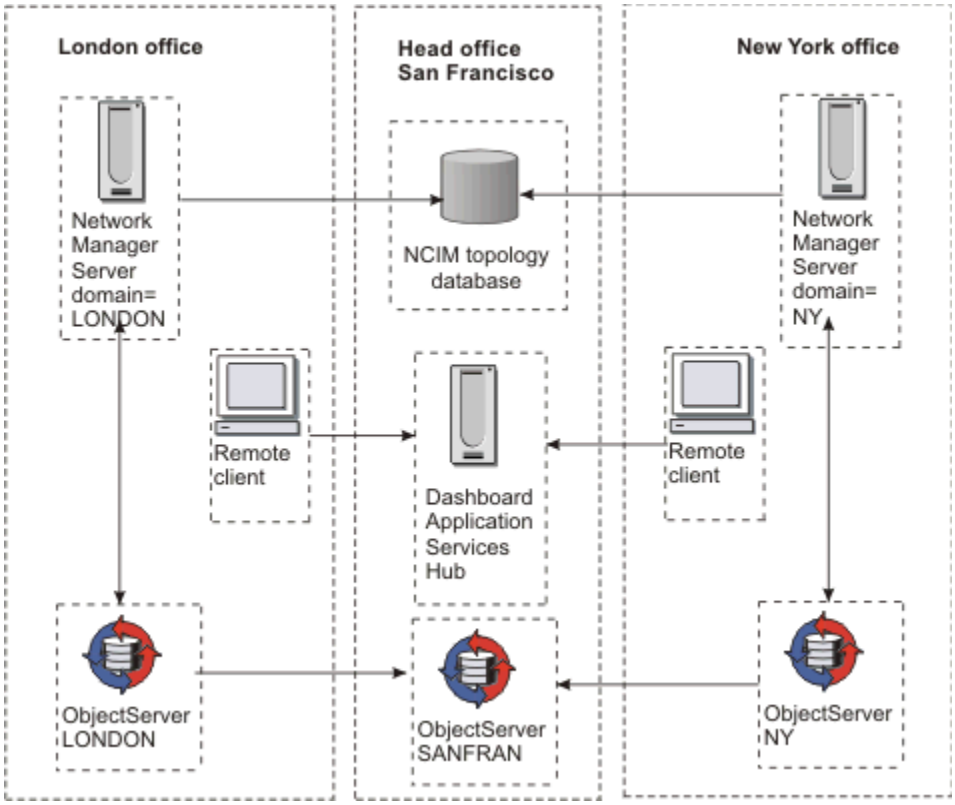

Figure 18. Large deployment host machine allocation

Steps to install a large deployment

The following steps provide an overview of the tasks required for this deployment, and help plan for a similar deployment. .

Note: If you are installing distributed Network Manager core component and Web application servers with different time zones, then you should set the same time zone on all servers which includes the database server as well as the core and GUI servers. This ensures that Network Manager is able to perform accurate timestamp comparisons from processes on different servers. You should also advise end users, such as network operators, that the system might display times that are different to the time in their location.

To install this deployment, perform the following steps:

1. Install the topology database on San Francisco host machine 3, and create the necessary database tables.

   Note: The topology database must be installed and started before you start the Network Manager core components so that discovery data can be saved.
2. Install the following ObjectServers and related components:
   - Install the ObjectServer on San Francisco host machine 2.
   - Install the ObjectServer and the uni-directional gateway on London host machine 2.
   - Install the ObjectServer and the uni-directional gateway on New York host machine 2.
3. Configure and run the ObjectServers.

   Note: The ObjectServers must be running before the Network Manager core components are started.
4. Install the Network Manager core components on London host machine 1.

   Note: The Network Manager core components must be installed before the Web applications.
5. Install the Network Manager core components on New York host machine 1.

6. Install the Network Manager GUI framework on host machine 3. The GUI framework includes the following software:
   - WebSphere Application Server
   - Dashboard Application Services Hub
   - Network Manager GUI components
   - Tivoli Netcool/OMNIbus Web GUI
   - Cognos Analytics

   Tip: If you install the Dashboard Application Services Hub on a machine with no other products, performance is likely to be better than if you install it on a machine with other products.

   Note: The Network Manager core components must be installed before the Network Manager GUI framework.

Part 2. Getting started

After you have installed Network Manager, start the product, make sure it is running correctly, and discover your network.

About this task

After configuring a first discovery, verify the results, and configure a production discovery. Schedule further discoveries to keep the network topology up to date. Once you have an up-to-date network topology, you can make the network topology available to Network Operators, and monitor the network for problems.

Chapter 4. Network Manager architecture

The Network Manager architecture can be divided into three layers: network layer, data layer, and visualization layer.

Network
The network layer interacts directly with the network. This layer contains network discovery and polling functionality. Network discovery retrieves topology data and network polling retrieves event data.

Data
The data layer stores the topology data retrieved by network discovery and the event data retrieved by network polling. Network polling also includes storage of polled SNMP and ICMP data for reporting and analysis. This layer also provides root cause analysis functionality that correlates topology and events to determine the source of network faults, and event enrichment functionality that adds topology data to events.

Visualization
The visualization layer provides the tools operators and administrators need to view topology, view events, and run network troubleshooting tools.

The following figure shows a conceptual overview of the Network Manager functional layers. Please note the following points when consulting the figure:

- It is possible to configure the Network Manager to include failover. This is not shown in the figure.
- Network Manager is designed to be installed with Tivoli Netcool/OMNIbus to enhance fault management, including root cause analysis, and correlation of alerts with the network topology.

  This figure depicts a standard Network Manager installation, and shows Tivoli Netcool/OMNIbus handling the storage and management of network events and the Tivoli Netcool/OMNIbus Web GUI handling visualization of network events.

  Note: Tivoli Netcool/OMNIbus is a separate product. If you do not already have OMNIbus then you must get a copy and install it. For more information, see the Network Manager installation documentation. Note also that Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis.
- The Dashboard Application Services Hub GUI framework is an application that runs GUIs from different Tivoli products, including Network Manager. The GUIs represented in the following figure, including the topology visualization GUIs and the event visualization GUIs all run within the Dashboard Application Services Hub GUI framework.
  - The topology visualization GUIs include single-widget views, such as the Hop View, Network Views, and Structure Browser. Default topology views also include multi-widget views, such as the Fault-Finding View and the Network Health View.
  - The Tivoli Netcool/OMNIbus Web GUI event visualization GUIs include the **Event Viewer**.
  - Network administrators can also build their own multi-widget views, which customize combinations of the single widget views.

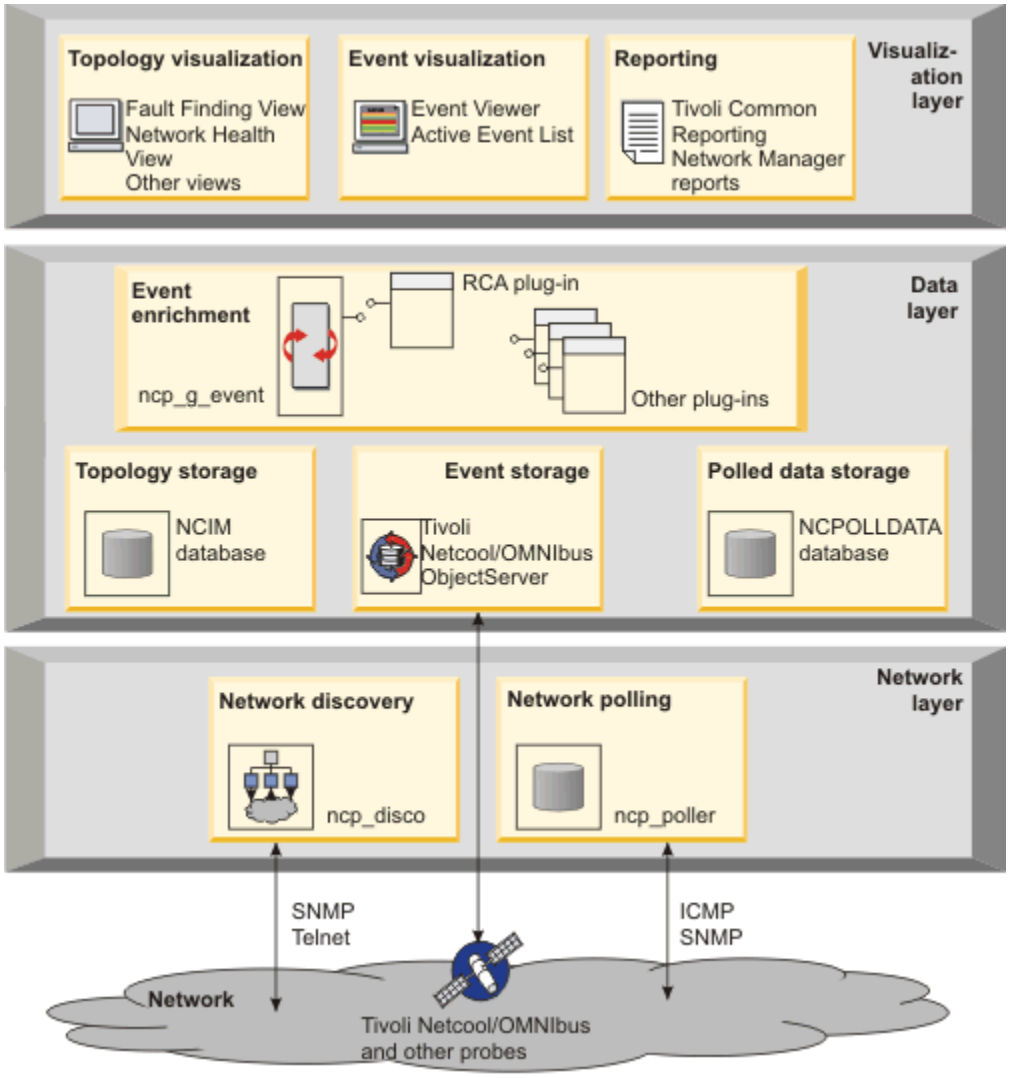

Figure 19. Network Manager functional layers

Network discovery

Network discovery involves discovering your network devices, determining how they are connected (network connectivity), and determining which components each device contains (containment). The complete set of discovered devices, connectivity, and containment is known as a network topology. You build your network topology by performing a discovery and then ensuring that you always have an up-to-date network topology by means of regular rediscoveries.

Network polling

Network polling determines whether a network device is up or down, whether it has exceeded key performance parameters, or whether links between devices are faulty. If a poll fails, Network Manager generates a device alert, which operators can view in the **Event Viewer**.

Topology storage

Network topology data is stored in the Network Connectivity and Inventory Model (NCIM) database. The NCIM database is a relational database that consolidates topology data discovered by Network Manager.

Event enrichment

Event enrichment is the process by which Network Manager adds topology data to events, thereby enriching the event and making it easier for the network operator to analyze. Examples of topology data that can be used to enrich events include system location and contact information.

Root-cause analysis

Root cause analysis is the process of determining the root cause of one or more device alerts. Network Manager performs root cause analysis by correlating event information with topology information. The process determines cause and symptom events based on the discovered network device and topology data.

Event storage

Event data is generated by Network Manager polls and also by Tivoli Netcool/OMNIbus probes installed on network devices. A probe is a protocol or vendor specific piece of software that resides on a device, detects and acquires event data from that device, and forwards the data to the ObjectServer as alerts. Event data can also be received from other event sources.

Event data from all of these event sources is stored in the Tivoli Netcool/OMNIbus ObjectServer.

Note: Tivoli Netcool/OMNIbus is a separate product. If you do not already have OMNIbus then you must get a copy and install it. For more information, see the Network Manager installation documentation.

Polled data storage

At any time a network administrator can set up polling of specific SNMP and ICMP data on one or more network devices. This data is stored in the NCPOLLDATA historical polled data database. Operators can then use the Cognos Analytics viewer to run performance reports to interpret the data.

Topology visualization

Network operators can use several topology visualization GUIs to view the network and to examine network devices. Using these GUIs operators can switch between topology views to explore connectivity or associations, and to see alert details in context. Operators also have access to diagnostic tools such as SNMP MIB Browser, which obtains MIB data for devices.

Event visualization

Operators can view event lists and use alert severity ratings to quickly identify high-priority device alerts. Operators can switch from event lists to topology views to see which devices are affected by specific alerts. They can also identify root cause alerts and list the symptom alerts that contribute to the root cause.

Reporting

Network Manager provides a wide range of reports, including performance reports, troubleshooting reports, asset reports, and device monitoring reports. Right click tools provide immediate access to reports from topology maps.

Related concepts

Network layer
The network layer consists of network discovery and polling tools.

Data layer
The data layer consists of topology storage, event storage, performance reporting data storage, and root cause analysis tools.

Visualization layer
This layer consists of topology visualization and event visualization tools.

Chapter 5. Getting started

After you have installed Network Manager, start the product, make sure it is running correctly, and discover your network.

About this task

After configuring a first discovery, verify the results, and configure a production discovery. Schedule further discoveries to keep the network topology up to date. Once you have an up-to-date network topology, you can make the network topology available to Network Operators, and monitor the network for problems.

Starting Network Manager

You can start the Network Manager back-end processes, using the **itnm_start** command.

About this task

From Network Manager V4.2 and above, you must start Tivoli Netcool/OMNIbus separately, using the Tivoli Netcool/OMNIbus commands.

Restriction: The **itnm_start** command is applicable only to UNIX installations, and to the server on which the Network Manager core components are installed. For more information about starting and stopping Network Manager, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Use the **itnm_start** command to start the Network Manager domain process controller, the **ncp_ctrl** process (which then starts all required Network Manager processes). Network Manager processes are responsible for network discovery, polling, root-cause analysis, network visualization and related activities.

To start Network Manager, complete the following steps.

Procedure

1. Start the Network Manager front-end processes by starting Dashboard Application Services Hub. Use the following command (where `server1` is the default name of the Dashboard Application Services Hub server):

   ```
   JazzSM_HOME/profile/bin/startServer.sh server1
   ```

2. Source the configuration file containing the Network Manager environment variables by entering the following command:

   ```
   /opt/IBM/netcool/core/env.sh
   ```

3. Change to the `$NCHOME/precision/bin` directory.
4. Type this command:`itnm_start -domain` *`domain`*

   This command starts all of the Network Manager components that are installed on the server.
5. Start the Dashboard Application Services Hub.

   For information on how to start Dashboard Application Services Hub, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

What to do next

You must now ensure that all Network Manager processes are up and running.

For more information about the **itnm_start** command, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Ensuring that all processes are up and running

You can check that processes are up and running using the itnm_status command.

About this task

On UNIX, you can check the status of Network Manager using the `itnm_status` command.

Restriction: This task only applies to UNIX installations, and to the server on which the Network Manager core components are installed. For more information about starting and stopping Network Manager, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

To check the status of all Network Manager components on the current server, complete the following steps.

Procedure

1. Change to the `$NCHOME/precision/bin` directory.
2. Type this command: `itnm_status`.

   This command displays the status of all of the Network Manager components that are installed on the server.

Results

Sample output: All processes up and running This output shows that all Network Manager processes are up and running.

```
Network Manager:
    Domain:  ITNM09
        ncp_ctrl              RUNNING  PID=7861  ITNM09
        ncp_store             RUNNING  PID=8127  ITNM09
        ncp_class             RUNNING  PID=8128  ITNM09
        ncp_model             RUNNING  PID=8261  ITNM09
        ncp_disco             RUNNING  PID=8280  ITNM09
        ncp_d_helpserv        RUNNING  PID=8129  ITNM09
        ncp_config            RUNNING  PID=8130  ITNM09
        ncp_poller(default)   RUNNING  PID=8988  ITNM09
        nco_p_ncpmonitor      RUNNING  PID=8134  ITNM09
        ncp_g_event           RUNNING  PID=8785  ITNM09
        ncp_webtool           RUNNING  PID=8135  ITNM09
        ncp_virtualdomain     RUNNING  PID=9167  ITNM09
    Apache Storm:
        supervisord           RUNNING  PID=596
        storm_number          RUNNING  PID=599
        storm_supervisor      RUNNING  PID=600
        zookeeper             RUNNING  PID=598
    Storm topologies:
        NMStormTopology       ACTIVE
```

Example

Sample output: Startup problems This shows the output of the command in the case of startup problems. In this example, the following processes have not started: The Discovery Engine, ncp_disco, and the Polling Engine, ncp_poller.

```
Network Manager:
    Domain:  ITNM09
        ncp_ctrl             RUNNING  PID=7861  ITNM09
        ncp_store            RUNNING  PID=8127  ITNM09
        ncp_class            RUNNING  PID=8128  ITNM09
        ncp_model            RUNNING  PID=8261  ITNM09
        ncp_disco            NOT RUNNING
        ncp_d_helpserv       RUNNING  PID=8129  ITNM09
        ncp_config           RUNNING  PID=8130  ITNM09
        ncp_poller           NOT RUNNING
        ncp_g_event          RUNNING  PID=8785  ITNM09
        ncp_webtool          RUNNING  PID=8135  ITNM09
        ncp_virtualdomain    RUNNING  PID=9167  ITNM09
    Apache Storm:
        supervisord          RUNNING  PID=596
        storm_number         RUNNING  PID=599
        storm_supervisor     RUNNING  PID=600
        zookeeper            RUNNING  PID=598
    Storm topologies:
        NMStormTopology      ACTIVE
```

What to do next

If you encounter startup problems, then complete the steps in the Troubleshooting startup problems procedure.

If all processes started up without any problems, then you can now log into Network Manager.

For more information about the **itnm_status** command and Network Manager processes, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Troubleshooting startup problems

Troubleshoot startup problems by examining log files for the processes that are not starting up. Use process dependencies to help identify the origin of the startup problem.

About this task

The default name of the log file is the process name followed by the domain name and then the .log or .trace file extension. Complete these steps to locate a log file for a process.

Procedure

1. Run the `itnm_status` command to determine which process or processes are failing to start.
   The `itnm_status` output might show, for example, that the ncp_disco process is failing to start.
2. Determine the process dependencies for the failing processes.

   Process dependencies are listed in the link below.

   For example, if the ncp_disco process is failing then the following dependencies apply:

   - The ncp_disco process depends on the Helper Server, ncp_d_helpserv, and the Topology Manager, ncp_model.
   - The ncp_d_helpserv process has no dependencies.
   - The ncp_model process depends on the Active Object Class manager, ncp_class.
3. Navigate to the default location for process log and trace files, *NCHOME*`/log/precision`.
4. Locate the log and trace files that correspond to the process name.
   For example, an instance of the ncp_disco process running on the NCOMS domain generates the following files.

   ncp_disco.NCOMS.log
   ncp_disco.NCOMS.trace
5. View the content of the log files for the failing process and for the process dependencies. Examine these files in reverse order of startup.
   For example, if the ncp_disco process is failing, then examine the log files in the following order

- ncp_disco.*DOMAIN*.log
- ncp_d_helpserv.*DOMAIN*.log
- ncp_class.*DOMAIN*.log

What to do next

For more information about troubleshooting the Dashboard Application Services Hub, see the Jazz for Service Management documentation.

For more information about the `itnm_status` command, troubleshooting Network Manager processes, and managing process dependencies, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related information

Jazz for Service Management welcome pageFor more information about troubleshooting the Dashboard Application Services Hub, search the Jazz for Service Management documentation.

Logging into Network Manager

Use your Web browser to access the Network Manager user interface.

Before you begin

To check the settings for local host, port, and user ID, view the application server profile.

About this task

To log into Network Manager:

Procedure

1. Open a supported browser.
2. Enter the URL of the application server: `https://`*`localhost`*`:16311/ibm/console` (secure access).

   Where *localhost* is the fully-qualified host name or IP address of the Dashboard Application Services Hub server.

   16310 is the default nonsecure port number and 16311 is the default secure port number. If your environment was configured during installation with a port number other than the default, enter that number instead.

   The default root context is `/ibm/console/`. The root context can be changed during installation.
3. On the login screen, enter your username and password as configured during installation, and click **Log in**.

   The default users are `smadmin`, `itnmadmin`, and `itnmuser`.

   Your user credentials are stored in the browser session. If you open a Dashboard Application Services Hub GUI in another window of the same browser, you can use the GUI without logging in again.

   Note: For information about the default users Network Manager provides, see the section about default users in the *IBM Tivoli Network Manager IP Edition Administration Guide*.
4. When you have finished working with any Dashboard Application Services Hub GUI, log out using the **Logout** link, or close all browser windows. This prevents another user from accessing the GUI using your stored user credentials.

What to do next

If you specified the parameters for an initial discovery during the installation, you can now view the network topology. If you did not specify the discovery parameters then you must now perform an initial discovery.

For more information about troubleshooting login problems, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Access to online help

Online help is topic-oriented, procedural, or reference information that you can access from the product installation, to assist you in the use of the product and to complete tasks.

You can search and browse within the online help to troubleshoot and find solutions for tasks you want to perform. Access to online help, as users work with the product, helps users to expand their knowledge about the product. You can access the online help from either the top-level online help or from the context-sensitive online help.

- Top-level online help. This online help displays a table of contents view of all available online help topics, for all products that are installed into your instance of Dashboard Application Services Hub.
- Context-sensitive online help. This online help links directly to documentation about the current panel. From this panel help topic, you can browse throughout the online help. After a product installation, this online help is disabled by default as the containing widget title bars are also disabled by default.

Accessing the top-level online help

The top-level online help displays a table of contents view of all online help topics.

About this task

Access to the top-level help is enabled by default. Within the **Contents** tab of the top-level help, you can expand, collapse, and select topics to browse around all topics within the online help. Complete the following steps to access the top-level online help.

Procedure

1. Within the Dashboard Application Services Hub navigation bar, select the **Help** icon  . The **Help** menu displays.
2. From the **Help** menu, select **InfoCenter**. The **Help System** window opens.
3. Within the **Help System** window, select **Using Network Manager**.

Results

The top-level online help for Network Manager is displayed.

What to do next

- Within the **Contents** tab of the top-level help, expand, collapse, and select topics to browse around all topics within the online help.
- Enter some text in the **Search** field to find any related online help.
- Use the available icons in the **Help System** toolbar to print or bookmark topics, or to move forwards and backwards between topics.

Enabling access to context-sensitive online help

An administrator can enable access to context-sensitive online help. This online help enables users to directly access documentation that is related to the current panel. From this panel help topic, users can browse throughout the online help.

About this task

After a product installation, this context-sensitive online help is disabled by default as the containing widget title bars are also disabled by default. If an administrator enables context-sensitive online help, users can directly access documentation that is related to the current panel. After access to context-sensitive online help is enabled, you can browse through all documentation topics within the online help. Complete the following steps to enable access to context-sensitive online help.

This access to context-sensitive online help might not work for some pages as the GUI might pre-date Dashboard Application Services Hub, or there might be no context-sensitive online help for the page.

Procedure

1. As the administrator user `itnmadmin`, display the view where you want to enable access to the online help. For example, if you want users to be able to access in-context online help for the Network Hop View, open the Network Hop View. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. In the views title bar, click the **Page Actions** icon  .
3. Select **Edit Page**. The view changes to show a view toolbar with a series of buttons and a widget palette.
4. Within a view, there can be one or more widgets. Select the widget for which you want to enable access to the context-sensitive online help.
5. In the view toolbar, select **Widget** > **Skin** > **Default**. The widget title bar for the widget is displayed and the **Help** icon is available within the widget title bar.
6. In the view toolbar, select **Save and Exit**.

Results

The widget title bar that contains the **Help** icon displays and access to context-sensitive online help for the selected widget is enabled for all users.

What to do next

- To access context-sensitive online help, click the **Help** icon  within the widget title bar.
- To enable access to context-sensitive online help for another widget, repeat all the steps.
- To browse to other topics within the online help, either expand the icons in the navigation pane or enter text in the **Search** field.
- To disable access to context-sensitive online help for a widget, go to the view toolbar and select **Widget** > **Skin** > **Default no title**

Getting started with discovery

Using Network Manager you can discover your network and schedule regular discoveries to ensure that your network topology stays up to date.

About this task

This is the most important task after Network Manager has been installed. Configure and verify your network discovery to produce the most complete and accurate network topology possible for the devices

and technologies in your network. An accurate network topology facilitates efficient root-cause analysis of network problems. This in turn enables your operators to troubleshoot network problems faster.

The most efficient approach to discovering your network is an iterative approach. This means beginning with a simple discovery and ensuring that the results are satisfactory. It is good practice to gradually configure more complex discoveries by adding extra scope zones to discover new regions of your network.

This information guides you through configuring and launching an initial discovery, and verifying the results. The information gives you guidance on how to identify problems with the discovered topology, and how to fix the discovery configuration in order to address these problems. Once you have a satisfactory topology that covers all regions of your network, the next step is to configure an efficient production discovery. The information shows you how to configure a production discovery, and how to schedule regular production discoveries to keep your discovered topology up to date with any network changes.

As you work through this information, you will perform the following discovery tasks:

- "Configuring initial discovery settings" on page 83
- "Launch the discovery and monitor discovery progress" on page 94
- "Verifying the topology" on page 102
- "Configuring production discovery settings" on page 110
- "Keeping topology up to date" on page 112

For complete information about discoveries, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Configuring initial discovery settings

Use this information to set up your initial discovery.

About this task

As you work through this information, you will perform the following discovery tasks:

- "Understanding scope settings" on page 83
- "Fine tuning a subnet scope zone using prediscovery filters" on page 86
- "Enabling the Ping finder and the feedback mechanism" on page 88
- "Configuring device and subnet access using SNMP community strings" on page 89
- "Ensuring all network technologies are covered" on page 93

Understanding scope settings

You can specify the boundaries of the network to discover by creating scopes that correspond to the IP addresses and subnets that you want to manage.

About this task

Let's suppose that your managed regions are made up of the following IP addresses and subnets:

- A single IP address, 10.30.1.20/32.
- The entire Class B subnet, 10.40.0.0/16, except for the Class C subnet 10.40.2.0/24.
- The first five IP addresses only in a set of subnets, 10.30.*.1-5.

Each of these regions can be defined using *scope zone*s. You can define as many scope zones as necessary for your network discovery.

On your own: Try to identify the boundaries of your own network. How would you express these boundaries using IP addresses, subnets, or formulas similar to the managed regions above?

Results
In the next steps you are going to define each of the three managed regions listed above using scope zones.

Setting a single IP address scope zone

Set a single IP address scope zone when one of your managed regions is made up of a single IP address only; for example, 10.30.1.20/32.

About this task
You can configure settings for your discovery within **Network Discovery Configuration**.

Procedure
1. Click the **Discovery** icon and select **Network Discovery Configuration**.
2. From the **Domain** list, select the required domain.

   Network Manager also offers advanced users the option of configuring discovery using text files. The Discovery Configuration GUI provides users less familiar with the discovery process with an easier way of configuring the discovery. When you save your settings in the Discovery Configuration GUI, the discovery configuration settings are written to the discovery text files.
3. Click **Scope**.
4. To add a new scope zone, click **New**  .

   The **Scope Properties** page is displayed.
5. Ensure that the **Protocol** setting is IPv4.

   Our single IP address scope zone, 10.30.1.20/32, is an IPv4 address, so this setting can stay as it is.
6. Ensure that **Scope By *Subnet** is selected, and type the IP address `10.30.1.20` in the **Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 32.
7. Ensure that the **Action** setting is set to **Include**.

   This defines the single IP address scope zone, 10.30.1.20/32 as an *inclusion zone*, an area of the network to be included in the discovery process.
8. Ensure that **Add to Ping Seed List** is checked.

   Clicking this option automatically adds the device in the scope zone to the *ping seed list*. This is a list of discovery seed devices, the locations from which to begin discovering devices. Discovery seeds can be IP addresses, as in this case, or subnet addresses. Clicking this option saves you having to separately enter the same entry in the **Seeds** tab.
9. Click **OK** to add this scope zone.
10. Click **Save**  to save your discovery configuration settings.

Results
You have now configured a single IP address scope zone consisting of the IP address 10.30.1.20/32. The next step is to configure a subnet scope zone for the entire Class B subnet, 10.40.0.0/16, but excluding the Class C subnet 10.40.2.0/24.You configured this single IP address as an inclusion zone, an area of the network to be included in the discovery process. When you configured this zone, you also added the IP address to the ping seed list. This is a set of IP addresses from which the discovery starts discovering the network.

The next step is to configure a scope zone for the managed region made up of the the entire Class B subnet, 10.40.0.0/16, but excluding the Class C subnet 10.40.2.0/24.

What to do next

Setting a subnet scope zone

Set a subnet scope zone when one of your managed regions is made up of a complete subnet.

About this task

A subnet scope zone can be an *inclusion zone*, an area of the network to be included in the discovery process, or an *exclusion zone*, an area of the network to be excluded from the discovery process. Let's suppose that your managed regions include the following subnet scope zones: the entire Class B subnet, 10.40.0.0/16 (inclusion zone), except for the Class C subnet 10.40.2.0/24 (exclusion zone). This can be represented graphically as follows. Only devices in the darker area are included in the discovery.

Note: The exclusion zone must be a subset of an inclusion zone otherwise you may find that the discovery has no boundaries. If you make the exclusion zone a subset of the inclusion zone then everything outside the exclusion zone becomes in scope.

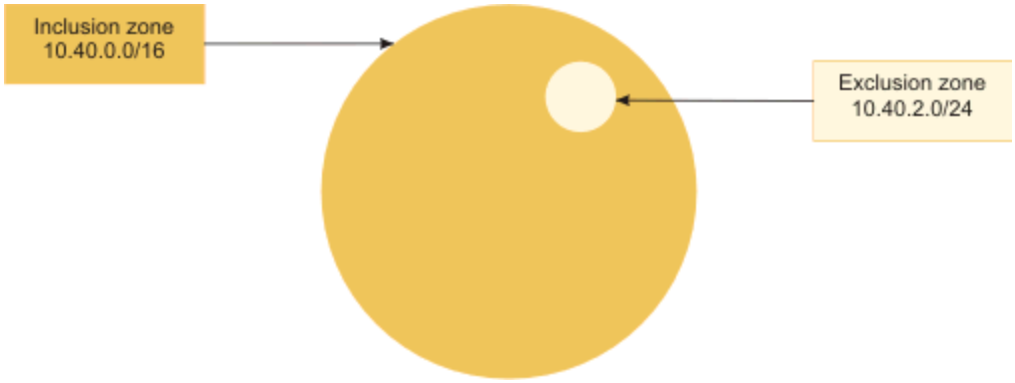

Figure 20. Exclusion zone within an inclusion zone

To create the exclusion zone within the inclusion zone, first add the Class B subnet, 10.40.0.0/16 as an inclusion zone, and then add the Class C subnet 10.40.2.0/24 as an exclusion zone.

Procedure

1. Click **Scope**.

   This takes you back to the **Scope Configuration** section of the GUI, where you can configure the subnet scopes.

2. To add a new scope zone, click **New**  .

   The **Scope Properties** page is displayed.

3. Leave the **Protocol** setting at IPv4.

   This is the required protocol setting as the Class B subnet inclusion zone 10.40.0.0/16 is an IPv4 address.

4. Ensure that **Scope By *Subnet** is selected, and type the IP address `10.40.0.0` in the **Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 16.

5. Ensure that the **Action** setting is set to **Include**.

   This defines the Class B subnet scope zone, 10.40.0.0/16 as an inclusion zone.

6. Ensure that **Add to Ping Seed List** is checked.

   Clicking this option automatically adds all the devices in the Class B subnet scope zone to the ping seed list. The discovery process will therefore attempt to ping every single device in this scope zone. This is known as *ping sweeping*.

   Ping sweeping results in long discoveries, as the discovery process has to try every single possible IP address in the subnet. Class B subnets can take up to two to three hours to ping sweep. Class A networks can take a day or more to ping sweep. However, ping sweeping takes minimal effort to configure and is useful when you are configuring initial discoveries as it enables the system to

automatically discover all devices within scope. Later, when you have successfully discovered your managed network and want to schedule more efficient production discoveries, you can generate a list of discovered IP addresses, and use this as the ping seed list rather than ping sweeping.

Restriction: The `Add to Ping Seed List` option is not available for IPv6 scope zones. This prevents ping sweeping of IPv6 subnets, which can potentially contain billions of devices to be pinged. Ping sweeping of IPv6 subnets can therefore result in a non-terminating discovery.

Ping sweeping relies on an active Ping finder. The discovery process uses the Ping finder to find devices specified in the ping seed list. You will enable the Ping finder as part of one of the next tasks.

7. Click **OK** to add this scope zone.
8. To add the Class C subnet 10.40.2.0/24 exclusion zone, click **New**  .
9. Ensure that **Scope By *Subnet** is selected, and type the IP address `10.40.2.0` in the **Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 24.
10. Under **Action** click **Exclude**.

    This defines the Class C subnet 10.40.2.0/24 as an exclusion zone.
11. Click **OK** to add this scope zone.
12. Click Save  to save your discovery configuration settings.

Results

You have now configured a subnet scope zone for the entire Class B subnet, 10.40.0.0/16, but excluding the Class C subnet 10.40.2.0/24. You did this by creating an inclusion zone and an exclusion zone. You configured ping sweeping of your Class B subnet inclusion zone. A ping sweep of this size of subnet will take up to two to three hours as every single possible IP address in the subnet has to be pinged. This is acceptable for initial discoveries as it enables the discovery process to identify all devices in scope. Later you will configure a more efficient production discovery that uses the results of your initial discoveries as ping seeds.

The next step is to configure a managed region made up of the first five IP addresses only in a set of subnets, 10.30.*.1-5.

Fine tuning a subnet scope zone using prediscovery filters

You can also restrict discovery to more complex IP address ranges. For example, you can configure your managed regions to include the first five addresses only in a set of subnets 10.30.*.1-5. The *prediscovery filter* is a mechanism that allows you to fine tune your discovery scope.

About this task

One way to do this is to first create a scope zone for the Class B subnet 10.30.0.0/16. Then restrict the discovered devices to the desired range using a *prediscovery filter*. All IP addresses within the defined scope zone are pinged initially and SNMP polled to retrieve the device sysObjectId. However, any device that does not pass the prediscovery filter is dropped from the discovery, is not queried by discovery agents, and is not included in the topology.

Test:

Procedure

1. Click **Scope**.
2. To add a new scope zone, click **New**  .

   The **Scope Properties** page is displayed.
3. Leave the **Protocol** setting at IPv4.

   This is the required protocol setting as the Class B subnet inclusion zone 10.30.0.0/16 is an IPv4 address.

4. Ensure that **Scope By *Subnet** is selected, and type the IP address `10.30.0.0` in the **Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 16.
5. Ensure that the **Action** setting is set to **Include**.

   This defines the Class B subnet scope zone, 10.30.0.0/16 as an inclusion zone.
6. Ensure that **Add to Ping Seed List** is checked.

   Clicking this option ensures that all devices in Class B subnet scope zone, 10.30.0.0/16 are pinged and SNMP polled. Data from the results of these ping and poll operations, for example the device sysObjectId is therefore available for use in prediscovery filters.
7. Click **OK** to add this scope zone.
8. Click **Filters**.

   This is the section of the GUI where you can create prediscovery filters.
9. In the **Pre-Discovery Filter** section of the panel, click **Filter Library**.
10. In the **Pre-Discovery Filter Library** window, click **Add Filter**.
11. Create a filter row to checks any devices discovered to make sure that they match one of the following:

    - 10.30.*.1
    - 10.30.*.2
    - 10.30.*.3
    - 10.30.*.4
    - 10.30.*.5

    a) In the **Name** field, type `Restrict 10.30.0.0 subnet`.

    A meaningful name of this sort helps you and others when referencing the filter later.

    b) In the **Basic** tab, select the **m_UniqueAddress** field from the **Field** list.

    The fields in this list represent data retrieved from each device during the early stages of discovery by the Details *discovery agent*. Discovery agents retrieve information about devices in the network. The Details agent is the first agent to run on each device and retrieves basic information about devices whose existence has already been verified. The fields that are presented in the **Field** list are stored in the details.returns database table. This enables you to construct filters based on a wide range of device data.

    For more information on the details.returns table, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

    c) Select **not like** from the **Comparator** list.

    d) Type `10\.30\..*\.([6-9]$)|[1-9][0-9].*$` in the **Value** field.

    The prediscovery filter allows the use of regular expressions. The regular expression that you just typed in instructs Network Manager to exclude all the unwanted devices in the 10.30.0.0 range, namely, 10.30.*.6-9 and 10.30.*.10-255. Note that you do not need to enclose the operand in single quotes. The system will do this automatically when it constructs the SQL where clause for this filter.

    Note: If the filter had been formulated using the more obvious **like** comparator, like this: `m_UniqueAddress LIKE '10\.30\..*\.[1-5]$` then no devices with management addresses outside of 10.30.*.1-5 would end up in the topology. This would therefore exclude the other scope zones that we formulated earlier, and would require the creation of extra filter rows in the filter to pass through those scopes. This example shows that it is important to design the filter logic so that you do not need to modify the prediscovery filter every time you add new scopes.

    For information on basic regular expression syntax, see the *IBM Tivoli Network Manager Reference*
12. Click **Save** to save the filter.

    The filter you defined appears in the filter list on the left of the window.
13. Click **Close**.

The filter you defined appears in the **Available Filters** list within the **Pre-Discovery Filter** section of the panel.

14. Select the filter and click **>**. The filter is applied and appears in the **Selected Filters** list.
15. Click **Save**  to save your discovery configuration settings.

Results

You have now configured your managed regions to include the first five addresses only in a set of subnets 10.30.*.1-5. You did this by creating a prediscovery filter, which uses regular expressions to filter out unwanted devices from the discovery. You created the prediscovery filter based on data collected early in the discovery by the Details agent.

The next step is to ensure that the *feedback* mechanism is switched on. Feedback is the mechanism by which data returned by discovery agents is used to find other devices. Examples of feedback data include the IP addresses of remote neighbors, or the subnet within which a local neighbor exists.

Enabling the Ping finder and the feedback mechanism

You can discover neighboring connected devices using the feedback mechanism. Feedback enables the discovery process to learn about the existence of devices as a result of querying other devices. In order for feedback to work, the Ping finder must be enabled.

About this task

By default, the Ping finder and the feedback mechanism are enabled. In this task you are going to locate these settings in the Discovery Configuration GUI and check that the settings are enabled.

Procedure

1. Click **Seed**.
2. Check that **Use Ping Finder in Discovery** is checked.

   The Ping finder is used to enable discovery to ping devices to verify existence and is used at various points in the discovery, including the following:

   - At the early stages to discover devices in the ping seed list and to perform ping sweeps of subnets.
   - Throughout the discovery to verify remote neighbors discovered as part of the feedback mechanism.
   - To identify the active interfaces on any subnets found.
3. Click **Advanced**.

   The **Advanced** tab contains a large number of configuration settings that the advanced user can set to work around unconventional network behavior.
4. In the **Advanced Discovery Configuration** section of the panel, check the setting for **Enable Feedback Control**.

   By default, feedback is set to **Feedback only on Full**, and this is the desired setting. This setting ensures that feedback is active when you are performing a *full discovery*, a discovery of your entire network. The entire network is made up of the managed areas that you defined using your discovery scopes.

   The other settings for **Enable Feedback Control** are as follows:

   No feedback
   This setting is useful when you want to strictly limit discovery to a predefined list of IP addresses, and you do not want the discovery process to discover any connected devices that are not in the predefined list. You will learn more about this setting when you set up your production discovery configuration.

   Feedback
   This setting switches on feedback for both full discovery and *partial discovery*. Partial discovery is a discovery of only a part of your network such as one or more devices or subnets. Partial discovery

is usually run in response to individual device changes: it can be run on demand, or scheduled for particularly volatile sections of the network. The main purpose of partial discovery is to quickly update topology data for a given device or devices and device connectivity is usually less of a priority when performing partial discovery. Device connectivity can be updated when the next scheduled full discovery is performed.

Typically you do not need to change any settings on the **Advanced** tab. However, it is worth noting the following settings:

Enable Ping Verification
This setting forces discovery to create network objects only for devices that respond to a ping.

Enable VLAN modelling
If you do not need to model VLANs, then disable this option to speed up discovery.

Enable ifName/ifDescr Interface Naming
Changes the default naming convention for discovered interfaces. If you change the default naming convention for discovered interfaces, you must change the BuildInterfaceName stitcher to specify your naming convention.

Discovery stitchers are pieces of code written in Network Manager's proprietary *stitcher language* that perform two main tasks within the discovery process:

Data collection stitchers
These stitchers move data collected from network devices from one database to another. These are system stitchers and are not available for customization by users.

Data processing stitchers
These stitchers 'stitch' together the data gathered by the discovery agents to generate the network topology, which can then be visualized and polled. Advanced users can modify these stitchers so that the discovery process will produce a custom topology. For example, as stated above, you can modify the BuildInterfaceName stitcher to specify a custom interface naming convention.

5. Click Save  to save your discovery configuration settings.

Results

You have now confirmed that the feedback and Ping finder are enabled.

The Ping finder is used to enable discovery to ping devices to verify existence and is used at various points in the discovery.

Feedback enables the discovery process to learn about the existence of devices as a result of querying other devices. In order for feedback to work, the Ping finder must be enabled.

Configuring device and subnet access using SNMP community strings

To enable discovery agents to access your network devices to retrieve SNMP data, you must specify SNMP community strings for the subnets and IP addresses in your network.

About this task

Community strings and Telnet access data can be *global*, which means that the discovery tries the community string for every device it encounters, or restricted to specific subnets (that is, used only on devices within a specific subnet), or even restricted to specific devices. Specifying community strings and Telnet access data by subnet results in a more efficient and faster discovery. In general, the more specific the credentials, the faster the discovery will determine the correct credentials.

Note: Speed of discovery related to community string settings in the GUI only affects the initial discoveries. Once Network Manager has identified the correct community strings, it stores this information in the NCMONITOR relational database. Subsequent discoveries access this database for SNMP community strings and other SNMP-related device access information.

When the discovery processes community strings, it always attempts to use the most specific match first. So if the discovery was attempting to query the device, 10.40.1.13, it first tries to use any community strings for that specific IP address (10.40.1.13/32). If none is available for that address, it tries to use any subnet strings specified for the Class C subnet 10.40.1.0/24 and then for the Class B subnet 10.40.0.0/16. If no subnet-specific IP addresses exists, it defaults to the global addresses in the priority order in which they are specified in the GUI.

Network Manager provides a global community string of `public`. Let's suppose that you want to keep the default `public` community string as some of your devices might use that string, but you also want to create a global community string specific to your network of `acme`, and that you want to give this `acme` community string higher priority than the default `public` community string.

In addition, you also want to define the following specific community strings:

- Class C subnet 10.40.1.0/24: give this subnet a community string of `network2`
- Class B subnet 10.40.0.0/16: give this subnet a community string of `network1`

You want the discovery process to use SNMPv2 community strings but you also want a fallback to the equivalent SNMPv1 community string if the SNMPv2 community string does not work for a particular device. To do this, you will need to create duplicate entries for each community string, one for SNMPv2 and one for SNMPv1. You must also ensure that each SNMPv2 community string is placed in the GUI so that it has a higher priority over the corresponding SNMPv1 community string.

This means that the order in which community strings will be tried for a device in the Class C subnet 10.40.1.0/24 (assuming that only the final community string works for that device will be as follows):

1. There is no community string at the device level so try the most specific subnet community string.
2. Class C subnet 10.40.1.0/24 community string `network2` using SNMPv2
3. Class C subnet 10.40.1.0/24 community string `network2` using SNMPv1
4. Class B subnet 10.40.0.0/16 community string `network1` using SNMPv2
5. Class B subnet 10.40.0.0/16 community string `network1` using SNMPv1
6. Custom global community string `acme` using SNMPv2
7. Custom global community string `acme` using SNMPv1
8. Network Manager global community string `public` using SNMPv2
9. Network Manager global community string `public` using SNMPv1

The next step is to enter these community strings into the GUI to ensure that they are tried in this order.

Procedure

1. Click **Passwords**.

   In the SNMP Community Strings section of the panel, you should see two rows in the table, showing the following information:

   Table 4. SNMP community strings

#	IP/Subnet	Community String	SNMP Version
1	null	public	Version 2
2	null	public	Version 1

   This information indicates that by default you already have two public community strings defined, with priority order being given to the SNMPv2 of this community string. Priority order is set by placing the community string higher in the table.
2. Add the global community string `acme` for SNMPv2 and SNMPv1.

   a) To add a new SNMP community string, click **New**  .

   The **SNMP Password Properties** page is displayed.

b) Type `acme` in the **Name** field.

c) The **Apply To** default setting is **All Devices**. Leave this setting as is.

This ensures that the `acme` community string is global.

d) For **SNMP Version** click **V2**.

e) Click **OK** to accept the settings.

f) Now add a second custom global community string, with the following settings:

Name
Type `acme`

Apply To
All Devices

SNMP Version
Click **V1**

Click **OK**.

At this point you have added two custom global community strings. These appear below the default public community strings in the table.

Table 5. SNMP community strings

#	IP/Subnet	Community String	SNMP Version
1	null	public	Version 2
2	null	public	Version 1
3	null	acme	Version 2
4	null	acme	Version 1

3. Assign the `acme` community string higher priority than the default `public` community string.

a) In row 3, which contains the acme community string for SNMPv2, click **Move Up** twice to move the acme SNMPv2 to the top of the table.

b) In row 4, which contains the acme community string for SNMPv1, click **Move Up** twice to move the acme SNMPv1 to the second row in the table.

The table should now appear as follows. The acme community strings appear in the first two rows in the table, and this means that the discovery process will try these strings first when attempting to gain access to devices. Also, the SNMPv2 version of acme will be tried before the SNMPv1 version.

Table 6. SNMP community strings

#	IP/Subnet	Community String	SNMP Version
1	null	acme	Version 2
2	null	acme	Version 1
3	null	public	Version 2
4	null	public	Version 1

The next step is to add the subnet-specific community strings.

4. Add community strings for the Class C subnet 10.40.1.0/24.

a) Click **New** .

The **SNMP Password Properties** page is displayed.

b) Add a subnet-specific community string with the following settings:

Name
Type `network2`

Apply To
Click ***Subnet** and type `10.40.1.0` in the ***Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 24.

SNMP Version
Click **V2**

Click **OK**.

c) Click **New**  .

The **SNMP Password Properties** page is displayed.

d) Add a second subnet-specific community string with the following settings:

Name
Type `network2`

Apply To
Click ***Subnet** and type `10.40.1.0` in the ***Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 24.

SNMP Version
Click **V1**

Click **OK**.

5. Add community strings for the Class B subnet 10.40.0.0/16.

a) Click **New**  .

The **SNMP Password Properties** page is displayed.

b) Add a third subnet-specific community string with the following settings:

Name
Type `network1`

Apply To
Click ***Subnet** and type `10.40.0.0` in the ***Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 16.

SNMP Version
Click **V2**

Click **OK**.

c) Click **New**  .

The **SNMP Password Properties** page is displayed.

d) Add a fourth subnet-specific community string with the following settings:

Name
Type `network1`

Apply To
Click ***Subnet** and type `10.40.0.0` in the ***Subnet** field. In the adjacent field following the slash sign, **/**, type the subnet mask 16.

SNMP Version
Click **V1**

Click **OK**.

The **SNMP Community String** table should now appear as follows.

*Table 7. **SNMP Community String** table following configuration and prioritization of the community strings*

#	IP/Subnet	Community String	SNMP Version
1	null	acme	Version 2
2	null	acme	Version 1
3	null	public	Version 2
4	null	public	Version 1
5	10.40.1.0	network2	Version 2
6	10.40.1.0	network2	Version 1
7	10.40.0.0	network1	Version 2
8	10.40.0.0	network1	Version 1

The subnet-specific community strings appear below the global community strings in the table. In this case the order does not matter, as the discovery process always tries specific community strings before global community strings, Also, the more specific the community string, the greater the priority, so the Class C community strings will always be tried before the Class B strings, regardless of where you place them in the table.

Results

You have now configured SNMP community strings to enable access to all the devices in your managed regions.

You have configured subnet-specific community strings for two of the subnets in your managed regions. These strings have priority.

You have also defined global community strings, which apply to all devices.

Ensuring all network technologies are covered

Network Manager discovery agents retrieve information from devices in your network. Dedicated agents such as CiscoFrameRelay retrieve specific network technology data. Check the list of full discovery agents to ensure that all the technologies in your network are covered.

About this task

In addition to the Details discovery agent, which retrieves basic information from all network devices, the discovery process also uses a set of protocol and technology-specific discovery agents to retrieve more detailed device information. By default a subset of discovery agents is enabled, and this subset usually satisfies the needs of most initial discoveries. You can use the GUI to retrieve a description of each discovery agent, and optionally enable extra discovery agents.

Procedure

1. Click **Full Discovery Agents**.
2. In the **Agents** tree, click **Agents** > **Full Layer 2 and Layer 3 Discovery** and then click the subnodes to view the full set of enabled layer 2 and layer 3 discovery agents.
3. Click an agent to see its description.

   For example, click **Agents** > **Full Layer 2 and Layer 3 Discovery** > **Layer 3** > **IpRoutingTable** to see a description of the IpRoutingTable agent. This layer 3 agent is enabled by default and learns other IP addresses and subnets to feed back into the discovery by examining each router's routing table.

   Other agents are disabled by default. For example, click **Agents** > **Entity** to see a description of the Entity agent. This agent discovers optional detailed containment information for a network entity. This

agent only needs to be enabled if you want to model physical containment and perform asset management, because the agent is resource intensive and lengthens discovery time.

4. If you made any changes to the discovery configuration, then click Save  to save your changes.

Results

You have reviewed the network protocols and technologies that will be discovered. You did this by reviewing the set of full discovery agents that are enabled. You have also seen how to use the agent tree to locate agents, how to retrieve more information on each agent, and how to enable an agent.

Configuring initial discovery settings: Summary

While working through this information, you configured initial discovery settings. You will use these settings to run a discovery.

By working through this information, you learned the following concepts and skills:

- Use of the Discovery Configuration GUI to configure key discovery settings
- Use of scope zones to include and exclude regions of your network
- How to use prediscovery filters to restrict discovery to more complex IP address ranges
- Use of ping sweeping to identify all devices in your managed regions
- How to activate the Ping finder and the feedback mechanism to enable ping sweeping
- How to configure device and subnet access using SNMP community strings
- Use of discovery agents to ensure all network technologies are covered

Launch the discovery and monitor discovery progress

Use the Discovery Status GUI to launch the discovery and to monitor discovery progress.

About this task

As you work through this information, you will perform the following discovery tasks:

- “Launching discovery” on page 95
- “Monitoring overall discovery progress” on page 96
- “Monitoring Ping finder status” on page 96
- “Monitoring discovery agent status” on page 98
- “Troubleshooting discovery issues” on page 100

Understanding discovery phases

A discovery runs through distinct phases. Use this information to understand each of the phases and to help you to monitor the discovery.

About this task

A running discovery passes through the following phases. It is possible for phases to overlap; for example, the Resolving Addresses phase (Phase 2) can start before the Interrogating Devices phase (Phase 1) has completed.

Interrogating Devices

In earlier versions of Network Manager, this phase was known as Phase 1. During this phase the discovery has found the first seed device and is finding other devices within scope. As devices are found, discovery agents proceed to interrogate the devices and retrieve device details, associated device addresses, and device connectivity.

Resolving Addresses
In earlier versions of Network Manager, this phase was known as Phase 2. During this phase the discovery maps devices in layers two and three of the OSI model.

Downloading Connections
In earlier versions of Network Manager, this phase was known as Phase 3. During this phase the discovery uses information retrieved from network switches to discover and verify device connectivity.

Correlating Connectivity
In earlier versions of Network Manager, this phase was known as Phase -1. During this phase the discovery process builds the network topology using network device information collected during the earlier phases. The work of building the topology is performed by discovery stitchers.

Launching discovery

Now that you have configured your discovery settings, the next step is to manually start your initial discoveries using the Discovery Status GUI.

About this task

You can launch a discovery in any of the following ways:

- Manually launching a discovery.
- Scheduling discovery to launch automatically on a regular basis.

Once you are satisfied with the results of your discovery, then you will probably want to schedule regular discoveries. For the moment, we are still running initial discoveries and tuning the discovery configuration based on the results, so the next step is to launch discovery manually.

Procedure

1. Click the **Discovery** icon and select **Network Discovery Status**.
2. View the **Discovery Status GUI** that displays.

   In the **Discovery Status GUI**, you can launch your discovery and monitor progress. The **Monitoring** section of the **Discovery Status GUI** displays a table with the four discovery phases:

   - Interrogating Devices
   - Resolving Addresses
   - Downloading Connections
   - Correlating Connections

   The **Discovery Type** label at the top right informs you that discovery is not running.

   Note: If you access this GUI while a discovery is running, for example, a regularly scheduled discovery, even if you did not start the discovery yourself, you would be able to monitor the running discovery.
3. From the **Domain** list, select the required domain.
4. Click **Start Discovery** 
5. Check that discovery starts okay.

   To do this, check the following:

   - The **Discovery Type** label shows the text **Discovery starting** and displays the running icon .
   - The **Last status received** label shows the text **Discovery starting**.
   - After a short time, the **Interrogating Devices** phase displays running status and the **Elapsed Time Current** column shows a time counter for this phase.

Results

You have now manually launched discovery. The next step is to monitor discovery progress.

Monitoring overall discovery progress

As discovery progresses, use the Discovery Status GUI to monitor discovery, to provide detailed information on the progress of discovery agents, and to view details of the last discovery.

About this task

You have now launched the discovery and the first phase, Interrogating Devices, has started. You can monitor the overall progress of the discovery by viewing the progress of each of the discovery phases in the Discovery Status GUI. You can sort the columns in this screen to make the viewing of data easier.

Procedure

1. Check that the **Interrogating Devices** phase is progressing without errors.

   As the phase progresses, you should see the following:

   - **Status** is **Running**  .
   - Under the **Elapsed Time** column, the **Current** value increases at regular intervals.
   - Under the **Work Completed** column, the **Current** value shows the number of IP addresses that have been found so far by the Ping finder. Based on the managed areas configured earlier as scope zones, the expectation is that the **Current Work Completed** value for **Interrogating Devices** shows the actual number of IP addresses found during the discovery. For our discovery configuration, the value will be anything from 16,000 to 65,000 IP addresses. This is based on the following estimates of the number of IP addresses in each managed area:
     - Single IP address, 10.30.1.20/32: number of IP addresses is 1.
     - The entire Class B subnet, 10.40.0.0/16, except for the Class C subnet 10.40.2.0/24. Maximum number of IP addresses is 65,536 - 255, which is just over 65,000. Assuming a sparsely populated Class B subnet, a minimum number of IP addresses might be 15,000.
     - The first five IP addresses only in a set of subnets, 10.30.*.1-5. Maximum number of IP addresses is 255 x 5 = 1275.

   You can compare the values of **Elapsed Time** and **Work Completed** in this discovery to the values in the previous discovery and this provides an extra level of verification that the discovery is running OK.
2. As the discovery moves from the **Interrogating Devices** phase into the subsequent phases, monitor the **Current Work Completed** for an idea of how far the phase has completed.

   In the **Resolving Addresses** and **Downloading Connections** phases, the percentage of work completed is calculated based on the number of IP addresses each agent has completed processing divided by the number of IP addresses the agents still have to process. Use this figure to obtain an idea of how close the phase is to completion.

Results

You now have an idea of how the overall discovery progress is progressing on a phase by phase basis. During the Interrogating Devices phase, the Ping finder pings each device within the configured scope zones The next step is to monitor the progress of the Ping finder as it pings the various IP addresses and subnets within each scope zone.

Monitoring Ping finder status

During the Interrogating Devices phase, the Ping finder pings each device within the configured scope zones. You can use the **Discovery Status GUI** to track the progress of the Ping finder through the subnets of each scope zone.

About this task

Procedure

In the **Discovery Status GUI**, click **Ping Finder Status**.

The **Ping Finder Status** section of the GUI shows the **Ping Finder Status** table. This table lists all the subnets that make up the scope zones that you configured earlier.

The **Ping Finder Status** table contains the following information:

Address
A list of IPs and subnets discovered to this point.

Netmask
For each subnet, this column indicates the netmask value.

Last Pinged
The last IP address pinged in this subnet.

Status
Indicates whether the Ping finder is still pinging this device or subnet or whether it has completed pinging.

For example, based on the scope zones that you configured, the **Ping Finder Status** table might look something like this:

*Table 8. Example of data in **Ping Finder Status** table*

Address	Netmask	Last Pinged	Status
10.30.1.20	-	-	✅
10.30.0.0	255.255.0.0	10.30.255.5	✅
10.40.0.0	255.255.0.0	10.40.39.3	➡️

This example shows that the pinging of your configured scope zones is proceeding. In particular:

- The single IP address scope zone 10.30.1.20 has been successfully pinged.
- All of the routers in the subnet 10.30.0.0 have been successfully pinged. The managed area here was made up of a complex IP address range, and to define this range you had to configure a prediscovery filter to exclude all IP addresses in the Class B subnet 10.30.0.0 outside of the range defined by 10.30.*.1-5. As you can see from the table, the last IP address to be pinged was 10.30.255.5, which is the very last IP address in this complex range.
- The Class B subnet 10.40.0.0 is still in the process of being pinged. Class B subnets can take up to two to three hours to ping sweep, because the discovery process has to try pinging every single possible IP address in the subnet. For a Class B subnet, that is 65,536 attempted IP address pings. As you can see from the table, the discovery has just pinged the IP address 10.40.39.3, so it still has a lot of pinging to do.

Note: If the Class B subnet 10.40.0.0 is a sparsely populated subnet then, when the Interrogating Devices phase completes, the Ping finder might not yet have completed pinging the subnet. By default, if, following the end of Phase 1, the Interrogating Devices phase, 90 seconds passes without the Ping finder finding any more devices, then the discovery enters what is known as the *blackout state*. During the blackout state the rest of the discovery phases progress normally but the Ping finder continues to ping sweep the sparsely populated Class B subnet 10.40.0.0, and any new IP addresses that are found are held in a special database table until the discovery phases complete for the IP addresses discovered up to the moment when the blackout state began. Once those discovery phases are complete, then the discovery process resumes for these addresses discovered during the blackout state.

Results

You have now spent some time monitoring Ping finder status and you have concluded that pinging of subnets is progressing satisfactorily. Once a device has been pinged by the Ping finder and its existence

has therefore been verified, the discovery process passes the device details to the discovery agents for information retrieval from the device. The next step is therefore to monitor the progress of the discovery agents.

Monitoring discovery agent status

As the discovery progresses, different discovery agents are called to retrieve device and connectivity data from discovered devices. This data will later be used to build the network topology. You can use the Discovery Status GUI to track overall and detailed status of the discovery agents.

About this task

Discovery agents run in the following order. Let's assume that the Ping finder has just verified the existence of the device 10.40.230.1, in our Class B subnet.

- After the Ping finder has verified the existence of IP address 10.40.230.1, the Details agent is called to retrieve basic information from this device.
- Once the Details agent has retrieved information from the IP address 10.40.230.1, the AssocAddress agent is called to retrieve all the IP addresses associated with 10.40.230.1. If the associated IP addresses have not yet been discovered and are in scope, then the IP address is passed to the Ping finder so that the device existence can be verified.
- Meanwhile other agents are called to interrogate the IP address 10.40.230.1. For example, this IP address is a router, so the IpRoutingTable agent is called to retrieve information from the routing table of router 10.40.230.1 and to feed back connected devices to the Ping finder. More precisely, 10.40.230.1 is a Cisco router within a BGP network, so the CiscoBGPTelnet agent is called to retrieve BGP-related data from the device.

This process is repeated for all devices until all relevant data has been retrieved from the devices in scope.

Note: The Details agent and the AssocAddress agent are the only discovery agents that interrogate every device in scope. The IP address counts for these agents are therefore always higher than those of the other agents.

As you monitor discovery agent progress, some of the key questions to ask are the following?

- Are all agents running okay? Have any agents crashed? If so, which IP address might have caused the agent to crash.
- Which agents are taking a long time to complete and which IP address appears to be causing this delay?
- Which agents are holding up a discovery phase and preventing the phase from completing? For example, which agents are holding up the Interrogating Devices phase?
- How many IP addresses does a particular agent, for example, the Details agent, still have to work on? How far is the agent through its work?
- Which IP addresses were found late in the discovery?

In this task we will use the **Discovery Status GUI Agents Status** table to answer these questions.

Procedure

1. In the **Discovery Status GUI**, click **Agents Status**.

   The **Agents Status** section of the GUI shows the discovery agents that are currently running and provides status information on each agent. Agents are sorted in order of state, and for each state, are sorted alphabetically.
2. Check that all agents are running okay.
   a) Check the **State** column of the Agents Status table. If any of the agents have terminated unexpectedly, then that agent will appear at the top of the list.

      The default sort order is descending order of state. Each agent state is assigned a number as follows:

Table 9. Agent states			
State	**Value**	**Icon**	**Description**
Died	5		The agent has terminated unexpectedly. This is a potential discovery problem.
Finished	4		The agent is still running but has finished processing of all the entities in its queue. The agent is still available to process any further agents placed in the queue.
Running	3		The agent is currently processing entities.
Starting	2		The agent is starting up.
Not running	1		The Agent is not running.

Let's assume that the CiscoSwitchTelnet agent has terminated unexpectedly.

b) Click the CiscoSwitchTelnet agent cell in the **Agents Status** table.

The **IP Address Status** table, which is the table below the **Agents Status** table, now displays all IP addresses for this agent.

c) Set the radio button above the table to **All**.

This ensures that the table shows all IP addresses for this agent, including IP addresses that have been processed by this agent, that are currently being processed, and that are queued for processing by the agent.

d) Sort the **IP Address Status** by **Return Time**.

Table rows with empty **Return Time** cells move to the top of the table. Look for IP addresses where the row has a value in the **Despatch Time** cell but the **Return Time** cell is empty. These IP addresses might have caused the agent to terminate unexpectedly.

Note: Further investigation is required to determine why this IP address caused the agent to crash.

3. Focus on an agent that is taking a long time to complete and to determine which IP address might be causing this delay. Let's assume that the IpForwardingTable agent is taking a long time to complete.

a) Click the IpForwardingTable agent cell in the **Agents Status** table.

The **IP Address Status** table, which is the table below the **Agents Status** table, now displays all IP addresses for this agent.

b) Set the radio button above the table to **All**.

This ensures that the table shows IP addresses that have been processed by this agent and IP addresses that are queued for processing by the agent.

c) Sort the **IP Address Status** by **Return Time**.

Table rows with empty **Return Time** cells move to the top of the table. Look for IP addresses where the row has a value in the **Despatch Time** cell but the **Return Time** cell is empty. These IP are still being worked on by the agent and might be causing the agent to take a long time to complete.

4. Determine which agents are holding up a discovery phase; for example, which agents are holding up the Interrogating Devices phase.

a) From the **Filter Agents by Phase** list just above the **Agents Status** table, select **Interrogating Devices**.

The **Agents Status** table now shows only the agents that complete in the Interrogating Devices phase.

b) Sort the **Agents Status** table by ascending order of **State**.

This brings the running agents to the top of the table, and enables you to see which agents are still running.

c) Sort the **Agents Status** table by descending order of state of **Outstanding IP Addresses**.

This brings the agents that are still processing IP addresses to the top of the table, with the agents that have the most IP addresses to process at the very top.

5. Determine how far an agent, let's say the Details agent, is through its work.
   a) Sort the **Agents Status** table by alphabetical order of **Agent**.
   b) Find the Details agent.
   c) In the Details agent row record the values for **Outstanding IP Addresses** and **Total IP Addresses**.

   You can determine a percentage of work complete using the following formula.

   Percentage work complete for an agent = (Outstanding IP Addresses / Total IP Addresses) * 100
6. Determine which IP addresses were found late in the discovery.
   a) Sort the **Agents Status** table by alphabetical order of **Agent**.
   b) Find the Details agent.
   c) Click the Details agent cell in the **Agents Status** table.

   The **IP Address Status** table now displays all IP addresses queued for the Details agent. These are the IP addresses that are in the agents despatch queue; however the agent has not yet started work on these devices.
   d) Sort the **IP Address Status** table by descending order of **Despatch Time**.

   In general, the later the agent was found during the discovery, the later its despatch time to the Details agent. This means that the agents that now appear at the top of the **IP Address Status** table were found latest during the discovery.

Results

You have now used the **Agents Status** and **IP Address Status** tables within the **Discovery Status GUI** to monitor the status of discovery agents. In particular, you have used the tables to find answers to the following queries:

- Are all agents running okay? Have any agents crashed? If so, which IP address might have caused the agent to crash.
- Which agents are taking a long time to complete and which IP address appears to be causing this delay?
- Which agents are holding up a discovery phase and preventing the phase from completing? For example, which agents are holding up the Interrogating Devices phase?
- How many IP addresses does a particular agent, for example, the Details agent, still have to work on? How far is the agent through its work?
- Which IP addresses were found late in the discovery?

Troubleshooting discovery issues

Discovery issues might arise for a number of reasons often due to malformed or inconsistent data in the network causing discovery agents to hang or crash. Before calling IBM Support, you can run a series of checks to try to narrow down the problem.

About this task

General discovery troubleshooting checks include the following:

- Check for any rogue processes running on UNIX servers.
- Check that you have sufficient memory for the Discovery process.
- Check for any discovery core files.

Procedure

1. On UNIX systems, check for any rogue processes running on the server.

a) Stop all Network Manager processes.
   Use the following command:`itnm_stop ncp -domain DOMAIN_NAME`
   Where *DOMAIN_NAME* is the name of your network domain.
   Note: If you do not specify a domain name, then the default NCOMS domain is used.
b) Check for any Network Manager processes that have not stopped.
   Use the following command:`ps -ef | grep ncp`
c) Kill any of these rogue ncp process using the Unix `kill` command.
d) Restart Network Manager.
   Use the following command:`itnm_start ncp -domain DOMAIN_NAME`
   Where *DOMAIN_NAME* is the name of your network domain.
e) Launch discovery.

2. Check that you have sufficient memory for the discovery process.
3. Check for any discovery core files.
   a) Issue the following command to recursively list out all directories that can contain core files: `ls -lR $NCHOME/precision/PD/core/`.
   b) Call IBM Support for help with debugging any core files.
      Core files are named `core.PID`, where *PID* is the ID of the process that generated the core file.
      Note: There might also be log files present in these directories. Log files are named differently to core files. The presence of log files does not indicate a problem, however, log files can be used in debugging issues.

Results

At this point you have run a series of checks to try to narrow down any possible discovery problems.

This task has covered the following activities and concepts:

- Checking for rogue processes running on the server.
- Checking that you have sufficient memory for the Discovery process.
- Checking for any discovery core files.

Launch the discovery and monitor discovery progress: Summary

While working through this information, you launched and monitored key elements of a discovery, including discovery phases, agents, and the Ping finder.

By working through this information, you learned the following concepts and skills:

- Discovery phases and what occurs in each phase
- How to use the Discovery Status GUI to launch and monitor discoveries
- How to compare the current discovery with the previous discovery
- How to determine which subnets and IP addresses the Ping finder is currently processing
- Why a discovery might enter the blackout state and consequently require more than one discovery cycle
- The order in which discovery agents and what information each discovery agent gathers
- How to interpret the Agents Status table in the Discovery Status GUI in order to answer key questions about the progress of the discovery
- General information about discovery troubleshoting

Verifying the topology

Use reports and topology views to check how well the discovery has modeled your network.

About this task

As you work through this information, you will perform the following discovery tasks:

- "Checking device access" on page 102
- "Checking for unclassified devices" on page 104
- "Checking connectivity" on page 108
- "Checking for unmanaged interfaces" on page 109

Checking device access

Use reports and SQL queries to check that all devices responded to SNMP requests during the discovery.

About this task

If you want to check that the discovery was able to access all the devices in your configured scope zones, run the Devices with no SNMP Access report. This report lists the devices that were found but for which for some reason the discovery was unable to access the device using SNMP.

Once you have identified the devices that the discovery was unable to access using SNMP, you can begin to investigate why SNMP access failed. Reasons why SNMP access might fail include the following:

Device not reachable
A firewall configuration might be blocking SNMP access. Make sure that SNMP access to the device is possible across your network's firewalls.

Device not responding
When Network Manager issues a request to a device, if the device does not respond, the request times out after a configurable time-out period and number of retries. Reasons for the timeout might include any of the following:

- If any of the devices in the configured scope zones is down at the time of discovery, then the device will not be found by the Ping finder and will not appear in the discovered network topology. You will also not be able to see these devices in the Devices with no SNMP Access report.
- The SNMP agent on the device is not running. Check the device and make sure that the SNMP agent is running.
- The SNMP agent is using a non-standard port. SNMP uses UDP protocol to communicate with the agents normally on port 161. You might need to reconfigure this on the device.
- The SNMP agent on the device is configured with a different community string than the one that you specified in Network Manager.
- If access control lists (ACLs) are being used for SNMP security, then check that the management device is on the SNMP agent ACL.

Note:

When a device fails to respond to SNMP polling a certain number of times, it is removed from the polling scope. The status of the device is then set to `NoAccessConfigured` (the value of `m_haveAccess` in the discovery returns database tables is set to `false`). The polling process cannot determine whether the device failed to respond because it is offline or because the credentials are incorrect. The next time that network discovery runs, the discovery determines whether the device has a new IP address, or the access credentials have changed.

In version 4.1 of Network Manager, the device was assumed to be offline.

To fix the case where the reason for SNMP access failure is that the SNMP agent on the device is configured with a different community string than the one that specified in Network Manager, complete the following steps:

Procedure

1. Click the **Reporting** icon and select **Common Reporting**. Within the widget, select **Network Manager**. A list of folders display. These folders contain all Cognos reports for your access.
2. Click **Troubleshooting Reports**.
3. Select the **Devices with no SNMP Access** report.

   The report displays a list of devices (the entity name and the IP address for each device) that the discovery found but the discovery agents were unable to access using SNMP.

   For more information on the **Devices with no SNMP Access** and other discovery troubleshooting reports, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
4. To check which community string Network Manager used during discovery for a given IP address, run the following SQL query on the NCMONITOR database to retrieve the SNMP access attributes for that device.

   SQL Query for SNMPv1

   ```
   SELECT v1.community, sa.version, sa.timeout, sa.retries
   FROM ncmonitor.snmpTarget st
   INNER JOIN ncmonitor.snmpV1Sec v1 on v1.accessid = st.readaccessid
   INNER JOIN ncmonitor.snmpAccess sa on sa.accessId = v1.accessid
   WHERE st.netaddr = 'ip_address';
   ```

   SQL Query for SNMPv2

   ```
   SELECT v1.community, sa.version, sa.timeout, sa.retries
   FROM ncmonitor.snmpTarget st
   INNER JOIN ncmonitor.snmpV1Sec v1 on v1.accessid = st.targetid
   INNER JOIN ncmonitor.snmpAccess sa on sa.accessid = v1.accessid
   WHERE st.netaddr = 'ip_address';
   ```

   SQL Query for SNMPv3

   ```
   SELECT v1.userid, v1.securitylevel, sa.version, sa.timeout, sa.retries
   FROM ncmonitor.snmpTarget st
   INNER JOIN ncmonitor.snmpV3Sec v1 on v1.accessid = st.readaccessid
   INNER JOIN ncmonitor.snmpAccess sa on sa.accessid = v1.accessid
   WHERE st.netaddr = 'ip_address';
   ```

   Where *ip_address* is one of the IP addresses listed in the **Devices with no SNMP Access** report.

   This query retrieves the following information:

   community
   Community string to use.

   version
   SNMP version to be used. Possible value are:

   - 0: SNMPv1
   - 1: SNMPv2
   - 3: SNMPv3

   timeout
   Number of milliseconds before retrying the SNMP request .

   retries
   Number of retries before giving up.

   For more information on the NCMONITOR database, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

5. If the community string is encrypted, you can decrypt it using the `ncp_crypt` utility.
   For example, the following command-line decrypts an encrypted password.

```
ncp_crypt -password @44:G5IhL1i2obPcXDu6uiMcse+U0qdRPojK0o6erxrfk/Y=@ -decrypt
ncp_crypt ( IBM Tivoli Network Manager Password Encryption/Decryption Tool )
Copyright (C) 1997 - 2008 By IBM Corporation. All Rights Reserved.
See product license for details.

IBM Tivoli Network Manager Version 3.9 created by fblucher at
03:38:26 Wed Nov 19 GMT 2010

@44:G5IhL1i2obPcXDu6uiMcse+U0qdRPojK0o6erxrfk/Y=@ public
```

   For more information on the `ncp_crypt` utility, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
6. Compare the SNMP community string stored in the NCMONITOR database for each device with the actual SNMP community for that device.
7. Correct the SNMP community string information for each device in the Discovery Configuration GUI.

Results

You have now checked that discovery was able to access devices and have corrected the SNMP community strings for any devices which could not be accessed. The next step is to check for any unclassified devices, that is, devices that do not have a device type classification within Network Manager.

Related tasks

Configuring device and subnet access using SNMP community strings
To enable discovery agents to access your network devices to retrieve SNMP data, you must specify SNMP community strings for the subnets and IP addresses in your network.

Checking for unclassified devices

Use reports to check that all devices found have a device type classification within Network Manager. Device type classifications are based on the MIB variable sysObjectId retrieved from the device during discovery.

About this task

Let's suppose that you want to check whether the discovery encountered any unclassified devices, that is, devices that do not have a device type classification within Network Manager. You can run the following reports to determine this:

- Devices with Unclassified SNMP Object IDs report
- Devices with Unknown SNMP Object IDs report

For any unclassified devices, you can take the following actions:

- Contact IBM Support with a list of these device types. IBM issues new device support several times a year and the latest Network Manager FixPack might include these device types. If not submit them for inclusion in a future FixPack.
- In the meantime add the sysObjectId information and mappings to Network Manager so that future discoveries are able to classify the devices. By doing this you will also enable the device to be correctly visualized in topology maps. The device class will also be available for inclusion in poll policies.

Note: The Network Manager team updates device support throughout the year. Contact IBM Support to find out when your unclassified devices will be added. In the meantime, this task describes how you can configure new device classifications.

In this task you will learn how to add the sysObjectId information and mappings to Network Manager.

Procedure

1. Click the **Reporting** icon and select **Common Reporting**. Within the widget, select **Network Manager**. A list of folders display. These folders contain all Cognos reports for your access.

2. Click **Troubleshooting Reports**.
3. Select the **Devices with Unclassified SNMP Object IDs** report.

   The report displays a list of devices with sysObjectId values that are unrecognized by Network Manager. The data in the report is grouped by sysObjectId. Let's assume you see data in the report similar to the following, under the sysObjectId 1.3.6.1.4.1977.1.6.1279.1.

Table 10. Unclassified device data for the sysObjectId 1.3.6.1.4.1977.1.6.1279.1

Entity Name	IP Address	System Description	CLASSNAME
group-1-b2.class.example.org	10.40.15.113	Hardware: x86 Family 15 Model 2 Stepping 8 AT/AT COMPATIBLE - Software; Microsoft Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)	NetworkDevice

   The report shows that the device with IP address 10.40.15.113 has the generic classification of NetworkDevice. The device has been assigned this generic classification because the system does not recognize the sysObjectId. Network Manager uses a class hierarchy to model and organize network devices. The *Network Device* class is a superclass for all device types, and contains a hierarchy of subclasses such as Cisco and Juniper that group network devices by manufacturer and then by device type and model.

   For more information on the class hierarchy, see the *IBM Tivoli Network Manager Reference*.

   In order to correctly classify the device with IP address 10.40.15.113, the first step is to determine the manufacturer of the device. You can determine the device manufacturer by identifying the manufacturer associated with the sysObjectId. The sysObjectId is an SNMP MIB variable, and includes information within it that identifies the device manufacturer.
4. Click the **Incident** icon and select **Network Availability** > **SNMP MIB Browser**.

   The SNMP MIB Browser enables you to browse the SNMP MIB tree. Each SNMP MIB variable, such as the sysObjectId, corresponds to a node on the tree. The SNMP MIB Browser opens with the MIB tree in the top left panel. By default, the MIB tree is open to the **iso** > **org** > **dod** > **internet** node.
5. Click the **internet** node in the MIB tree.

   The **MIB Variable Information** panel at the bottom left now displays the OID value for the internet node as **1.3.6.1**. You are now going to "walk" the MIB tree until you get to the sysObjectId value of 1.3.6.1.4.1.1977, which is the sysObjectId that contains the manufacturer of the unclassified device from the **Devices with Unclassified SNMP Object IDs** report.
6. Click the **private** node in the MIB tree.

   The **MIB Variable Information** panel at the bottom left now displays the OID value for the internet node as **1.3.6.1.4**. The number 4 at the end of this sysObjectId value refers to the fourth subnode (**private**) within the **internet** node.
7. Expand the **private** node.

   The **private** node expands to display a single **enterprises** node.
8. Click the **enterprises** node.

   The **MIB Variable Information** panel at the bottom left now displays the OID value for the internet node as **1.3.6.1.4.1**. The number 1at the end of this sysObjectId value refers to the first (and only) subnode (**enterprises**) within the **private** node.
9. Expand the **enterprises** node.

   The **enterprises** node expands to display a list of device manufacturers.
10. Click each manufacturer node in turn.

    Review the resulting OID value in the **MIB Variable Information** panel. You get results similar to the information in the following table:

Table 11. Enterprises and their sysObjectIds	
enterprise	**OID (sysObjectId)**
synernetics	1.3.6.1.4.1.114
bicc	1.3.6.1.4.1.170
wellfleet	1.3.6.1.4.1.18
alteon	1.3.6.1.4.1.1872
extremenetworks	1.3.6.1.4.1.1916
networkharmoni	1.3.6.1.4.1.1977
foundry	1.3.6.1.4.1.1991
alliedTelesyn	1.3.6.1.4.1.207

The enterprise corresponding to the sysObjectId `1.3.6.1.4.1977` is Network Harmoni. This means that the manufacturer of the unclassified device from the **Devices with Unclassified SNMP Object IDs** report is Network Harmoni.

Device classifications are created using active object class (AOC) files. The next step is to check whether any AOC files exist for NetworkHarmoni devices.

For more information on AOC files, see the *IBM Tivoli Network Manager Reference*.

11. Go to the directory that contains the AOC files:

```
cd $NCHOME/precision/aoc/
ls Net*
```

A listing of the files in this directory with filenames starting with the letters `Net` shows no AOC files for NetworkHarmoni devices.

12. Run the following command to see if the NetworkHarmoni enterprise number is used in any of the AOC files:

```
grep 1977 *.aoc
```

This search retrieves two files: `EndNode.aoc` and `EndNode.NCOMS.aoc`.

Note: The `EndNode.NCOMS.aoc` file is a domain-specific version of the `EndNode.aoc` file. The `EndNode.NCOMS.aoc` file starts off as an exact copy of `EndNode.aoc`. The domain-specific version is created to enable domain-specific class hierarchy settings. Network Manager always looks for a domain-specific version of the file first. If it can't find a domain-specific version, then it uses the generic version.

13. Let's assume that we ran our discovery in the NCOMS domain. Open the NCOMS domain-specific AOC file `EndNode.NCOMS.aoc` .
14. Search for the text 1977 in the file. This retrieves a line that reads: `EntityOID = '1.3.6.1.4.1.1977'`

A review of the code around that line shows the following:

```
active object 'EndNode'
{
super_class = 'Core';
instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.2021\.' OR
                    EntityOID = '1.3.6.1.4.1.2021' OR
                    EntityOID = '1.3.6.1.4.1.1575' OR
                    EntityOID like '1 \.3\.6\.1\.4\.1\.11\.2\.3\.9\.' OR
                    EntityOID = '1.3 .6.1.4.1.11.2.3.9' OR
                    (EntityType = 1 AND EntityOID IS NULL)OR
                    ... OR
                    EntityOID = '1.3.6.1.4.1.1977' OR
                    EntityOID like '1\.3\.6\.1\.4\.1\.2136\.' OR
                    ...
```

The following table explains this code.

Table 12. Description of the query

Line numbers	Description
1	Name of the class is EndNode
3	The parent of this class is the Core class.
4-13	The instantiate_rule performs a series of matches for each device it encounters. If the relevant device MIB data (in this case each match is attempted with the EntityOID, which is the same as the sysObjectId) matches any of these lines, then the device is assigned to the EndNode class.

Line 11 shows that this AOC file is looking for an *exact* match to the sysObjectId `1.3.6.1.4.1.1977`, which is the sysObjectId for the Network Harmoni enterprise. However, this does not match our original unclassified device, because that device has a sysObjectId of `1.3.6.1.4.1977.1.6.1279.1`.

This is an error in the regular expression syntax in this AOC file. Line 11 should read:

```
EntityOID like '1\.3\.6\.1\.4\.1\.11\.2\.3\.9\.'
```

This regular would ensure that any devices that has a sysObjectId that begins with `1.3.6.1.4.1.1977` would be classified as an EndNode device. Instead of doing this, you can create a new AOC file that is specific to devices with sysObjectId `1.3.6.1.4.1977.1.6.1279.1` and that classifies this device type as Network Harmoni end node device.

15. Create a new AOC file in the `$NCHOME/precision/aoc/` directory. Name this file `EndNodeNetHarmoni.aoc`.
16. Add the following text to the `EndNodeNetHarmoni.aoc` file.

```
//************************************************************
//
// File : EndNodeNetHarmoni.aoc
//
//************************************************************
active object 'EndNodeNetHarmoni'
{
  super_class ='EndNode';

  instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.1977\.1\.6\.1279\.'";

  extension for Fault = {
  rules = [] ,
  poll_list = [] };

  visual_icon = 'EndNode';
}
```

For more information on classifying network devices, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

17. Save the `EndNodeNetHarmoni.aoc` file.
18. Restart Network Manager using the following commands. This forces the AOC file to be read into the system.

```
itnm_stop ncp
itnm_start ncp
```

19. Run the following command to check that the Active Object Class manager, ncp_class, has restarted correctly.

```
itnm_status
```

The Active Object Class manager manages the AOCs and distributes them to any Network Manager process that needs them.

- If ncp_class started OK, then it means that new AOC file was set up correctly.
- If ncp_class does not start, check the following log file for any errors: `$NCHOME/log/precision/ncp_class.NCOMS.log`.

20. Specify entries in the NCIM topology database `deviceFunction` and `mappings` ncim database tables to provide the vendor, model, and function for the Network Harmoni end node device classification.

    See these two files for the appropriate data and syntax.

    - `$NCHOME/precision/scripts/sql/data/populateDeviceFunction.sql`
    - `$NCHOME/precision/scripts/sql/data/populateMappings.sql`

    For more information on these NCIM topology database tables, see the *IBM Tivoli Network Manager Reference*.

Results

You have now checked for unclassified devices and made the necessary modifications to the AOC files. that discovery was able to access devices and have corrected the SNMP community strings for any devices which could not be accessed. The next step is to check for device connectivity.

Checking connectivity

Use reports and topology views to check for missing connections between devices.

About this task

Procedure

1. Click the **Reporting** icon and select **Common Reporting**. Within the widget, select **Network Manager**. A list of folders display. These folders contain all Cognos reports for your access.
2. Click **Troubleshooting Reports**.
3. Select the **Devices with no connections** report.

   The report displays a list of devices for which connectivity was not discovered properly.

   For more information on the **Devices with no connections** and other discovery troubleshooting reports, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
4. For each device in the list, try to resolve the problem by doing one of the following:

   - Ensure that Network Manager has been added to the access control list for the device.
   - Check that all the appropriate discovery agents were configured.
   - Check whether the device that you expected to be connected is out of scope.

   Another possible reason for missing connectivity is that the device that you expected to be connected was not discovered due to incorrect seeding of the discovery. In the case of the discovery configuration that was configured earlier, that should not be a problem because you configured ping sweeping on all of the scopes, so each device in scope was individually pinged. However, this is another area to investigate if you configured individual device seeds

   .

Results

You have now checked for device connectivity and taken action to fix the discovery configuration. The next step is to check for unmanaged interfaces.

Related tasks

Ensuring all network technologies are covered

Network Manager discovery agents retrieve information from devices in your network. Dedicated agents such as CiscoFrameRelay retrieve specific network technology data. Check the list of full discovery agents to ensure that all the technologies in your network are covered.

Checking for unmanaged interfaces

Use SQL queries to check that devices marked as permanently unmanaged are really meant to be marked as permanently unmanaged.

About this task

During discovery, the `PopulateDNCIM_ManagedStatus` discovery stitcher is used to mark specific interfaces as permanently unmanaged for the purposes of monitoring. This means that the specified interface types are not polled by Network Manager. Interfaces are set to permanently unmanaged on an interface type basis, based on the value of various interface attributes, including the `ifDescr` attribute. You can check which types of interfaces are marked permanently unmanaged by default and you can change the settings if necessary. By default, interfaces which are virtual or dial up are marked permanently unmanaged, because it costs money to poll these interfaces.

In addition to being marked unmanaged, any events generated on these interfaces will be tagged so that they can be filtered out of event lists by network operators.

Procedure

1. Use the following SQL command to retrieve a list of interfaces that have been marked as permanently unmanaged by the discovery.

```
SELECT     mnode.entityName AS DeviceName,
           i.entityName AS Interface,
           i.ipAddress AS IPAddress,
           i.ifDescr AS ifDescr,
           m.status AS Status
FROM       ncim.interfaces i
INNER JOIN ncim.entity mnode on mnode.entityId = i.mainNodeEntityId
INNER JOIN ncim.managedStatus m on m.entityId = i.entityId and m.status = 2;
```

2. Check each IP address returned by the query and note any IP addresses that you want to be able to poll and monitor.

   Let's assume that the results of the query show a number of interfaces that need to be monitored. Let's also assume that each of these IP addresses has the text `Vlan` in their `ifDescr` MIB variable, and you want to monitor them.

3. Edit the `$NCHOME/precision/disco/stitchers/DNCIM/PopulateDNCIM_ManagedStatus.stch` file.
4. Remove the VLAN interface type from the filter at the end of the file.

   To do this you must remove the following two lines from the filter:

```
OR
ExtraInfo->m_IfDescr like 'Vlan'
```

5. Save the file.

Results

You have now checked for unmanaged interfaces. You noted that VLAN interfaces had been set to permanently unmanaged. This was not a desired setting, and so you modified the settings in the `PopulateDNCIM_ManagedStatus.stch` stitcher file so that VLAN interfaces are discovered as managed interfaces.

You have performed a number of topology checks. You can perform more topology checks by running other discovery troubleshooting reports.

Assuming that you are now satisfied with the changes that you have made to the discovery configuration, you can run another discovery to check the results of your changes.

Related tasks

Launching discovery
Now that you have configured your discovery settings, the next step is to manually start your initial discoveries using the Discovery Status GUI.

Verifying the topology: Summary

While working through this information, you used reports, topology views, and SQL queries to check how well the discovery modeled your network. You used the results of these verification activities to adjust the discovery configuration settings.

By working through this information, you learned the following concepts and skills:

- An understanding of why discovery was unable to access devices using SNMP
- How to correct SNMP community string discovery configuration settings for individual devices
- The use of active object class (AOC) files to classify network devices
- How to modify AOC files in order to fix device classification problems
- An understanding of why the topology might be missing connections between devices
- How to identify permanently unmanaged interfaces
- How to modify the assignment of permanently unmanaged interfaces

Configuring production discovery settings

Configure an efficient production discovery by generating a list of the discovered devices and using this list to seed discoveries.

About this task

As you work through this information, you will perform the following discovery tasks:

- “Generating a list of discovered devices” on page 110
- “Specifying IP addresses to find using the File finder” on page 111

Generating a list of discovered devices

After successfully discovering your managed network, generating a list of discovered IP addresses can make subsequent discoveries more productive.

About this task

Your initial discoveries used ping sweeping to try every single possible IP address in the subnet. This method is useful when you are configuring initial discoveries as it takes minimal effort to configure and it enables the system to automatically discover all devices within scope. Now, however, you have successfully discovered your managed network and want to schedule more efficient production discoveries. You can do this by generating a list of discovered IP addresses, and using this list as the ping seed list rather than ping sweeping.

Procedure

Run the `BuildSeedList.pl` Perl script to write the IP addresses discovered by your previous discovery to a file.

Issue the following command to do this:

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
BuildSeedList.pl -domain NCOMS -outFile seedfile.txt
```

This command builds a device seed list based on the IP addresses discovered by your previous discovery. The command looks in the NCOMS domain, which is the domain in which the previous discovery was run.

The file that is output by this script is stored in the following location: `$NCHOME/etc/precision/seedfile.txt`.

Results

You have now generated a device seed list that contains all the devices (and only the devices) in your topology. You will now use this consolidated device seed list to configure a more efficient production discovery.

Specifying IP addresses to find using the File finder

Use the File finder with feedback to configure an efficient discovery that can be used on an ongoing basis in production.

About this task

You have now created a seed list containing just the devices in your discovered topology. You are now going to configure the File finder to use this file as your seed list. You must also make the following changes to your discovery configuration to ensure that you have an efficient production discovery that completes more quickly than your initial discoveries:

- Switch off ping sweeping of your scope zones.
- Ensure that the Ping finder is still enabled. You need the Ping finder to verify the existence of devices in your File finder seed list and to ping newly discovered devices connected to your seed devices.
- Ensure that feedback is switched on. You need feedback on in order to discover new devices connected to your seed devices.

Procedure

1. Click the **Discovery** icon and select **Network Discovery Configuration**.
2. From the **Domain** list, select the required domain.
3. Switch off ping sweeping of your scope zones.
   a) Click **Scope**.
   b) For each include scope in the **Scope Configuration** table, click on the **Address** field.
   c) In the Scope Properties window, uncheck the **Add to Ping Seed List** option.
   d) Repeat this for each include scope in the **Scope Configuration** table.
4. Ensure that the Ping finder is still enabled.
   a) Click **Seed**.
   b) Check that **Use Ping Finder in Discovery** is checked.
5. Configure the File finder.
   a) Check the **Use File Finder in Discovery** option.
   b) In the File finder section of the GUI. click **New** 
   c) In the **Filename** field of the **File Seed Properties** window, type the path to the device seed list that you generated.
      The path to this file is:
      ```
      $NCHOME/etc/precision/seedfile.txt
      ```
   d) In the **Delimiter** field, type `[\t]+`.
   e) Ensure that the **IP Column** is set to 1 and that the **Name Column** is set to 2.
   f) Click **OK**.
6. Ensure that feedback is switched on.
   a) Click **Advanced**.

b) In the **Advanced Discovery Configuration** section of the panel, check the setting for **Enable Feedback Control**.

By default, feedback is set to **Feedback only on Full**, and this is the desired setting. This setting ensures that feedback is active when you are performing a *full discovery*, a discovery of your entire network. The entire network is made up of the managed areas that you defined using your discovery scopes.

7. Click Save  to save your discovery configuration settings.

Results

Now that you have configured a more efficient discovery using the File finder, you can schedule regular discoveries to run with these settings.

Configuring production discovery settings: Summary

While working through this information, you configured production discovery settings. You will use these settings to schedule future production discoveries.

By working through this information, you learned the following concepts and skills:

- Use of a ping seed list, instead of ping sweeping, to configure an efficient discovery
- How to use the `BuildSeedList.pl` Perl script to capture IP addresses discovered by your previous discovery
- How to use the File finder to use file containing a list of IP addresses to seed a discovery

Keeping topology up to date

You can keep the discovered topology up to date by configuring a discovery schedule for your entire network.

About this task

As you work through this information, you will perform the following discovery task: “Scheduling discovery” on page 112

Scheduling discovery

Schedule ongoing production discoveries to keep your discovered topology up to date.

About this task

Now that you have configured an efficient discovery using the File finder, you can schedule discovery to run on a regular basis. This ensures that any new devices or devices changes are identified and added to the topology.

Let's suppose you want to set up a scheduled discovery to run every night at 3:00 AM.

Procedure

Run the `scheduleDiscovery.pl` Perl script to schedule a full discovery.

Issue the following command to do this:

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/scheduleDiscovery.pl
-domain NCOMS -time 03:00
```

This command instructs Network Manager to run a full discovery on the NCOMS domain every night at 3 AM.

In addition to using the `scheduleDiscovery.pl` Perl script to schedule a daily full discovery, you can also use this script to perform other tasks related to discovery scheduling:

- Display the current discovery schedule.
- Schedule a weekly or monthly discovery.
- Schedule discovery to occur at a specified interval; for example, every 48 hours.

For more information on the `scheduleDiscovery.pl` Perl script, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

The `scheduleDiscovery.pl` Perl script uses the scheduling parameters configured in the command line and uses these to update the `FullDiscovery.stch` discovery stitcher. The discovery daemon checks for changed discovery stitchers every 60 seconds. When it sees that the `FullDiscovery.stch` stitcher has been modified, it sets up the next scheduled discovery.

It is also possible to configure a discovery schedule by editing the `FullDiscovery.stch` stitcher directly. The stitcher is located at:

```
$NCHOME/precision/disco/stitchers/
```

For more information on the `FullDiscovery.stch` stitcher, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Keeping topology up to date: Summary

While working through this information, you configured a discovery schedule for your entire network. You will use these settings on an ongoing basis to keep the discovered topology up to date.

By working through this information, you learned the following concepts and skills:

- How to use the `scheduleDiscovery.pl` Perl script to schedule regular discoveries
- Use of stitchers, pieces of code written in Network Manager's proprietary stitcher language and that perform tasks within the discovery process
- The role of the FullDiscovery.stch in scheduling discoveries.

Viewing the network

Following an initial network discovery, use the following options to view the discovered network: browse the network using the **Network Views** or search for specific network devices using the **Network Hop View**.

Browsing the network

Browse the network using the **Network Views** to visualize the network based on geographical or other groupings. For example, you can browse discovered subnets or device classes. **Network Views** also highlights discovery issues by showing you devices that the discovery was unable to access or unable to classify.

Before you begin

Before you can work with network views, the first network discovery must have successfully completed, either as part of the installation or immediately following installation.

Restriction: The Administrator user, itnmadmin, has network views assigned by default, so that when you log in with this user, you can view the topology. By default, itnmuser has OOB network views assigned, but other user profiles may not have any network views assigned by default.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. In the **Network Views** tree on the left of the widget, browse the network by expanding network view nodes of interest.
   Here are some examples:

- To browse subnets, click the + symbol next to the Subnets node.
- To browse VLANs, click the + symbol next to the Global VLANs node.
- To browse device classes and see devices grouped into categories such as Linux, Sun, and Cisco, click the + symbol next to the Device Classes node.

  Note: Devices which the discovery process could not access using SNMP appear in the NoSNMPAccess sub-node, under the Device Classes node.

3. Click a network view.

   The network map displays subnets and devices in that network view. Faulty devices are displayed with an associated event icon.

Searching for network devices

You can search for a specific device in the discovered network topology using the **Network Hop View**.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. Select a network domain from the **Domain** list.
3. Check or uncheck the **Search all domains** checkbox to constrain the search to a particular domain or to search across all domains.

   If the **Search all domains** checkbox is checked, the **Domain** list is disabled. The default state of the **Search all domains** checkbox is controlled by the `topoviz.entitySearch.allDomains` property in the `topoviz.properties` file.

4. Click **Search for Seed Device**  to specify the device to search for.
5. In the **Entity Search** window, ensure that the **Basic** tab is selected and complete the search criteria fields.

   Domain
   Select the domain in which you want to search.

   Note: If you opened the Entity Search window from the Path Views GUI, then you cannot change domain. This is done to prevent cross-domain path traces.

   IP Address
   Specify the IP address of the device. You can specify all of the address, or only the first part of the address. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets.

   Device Name
   Specify the name of the device. You can specify all of the name, or only the first part of the name. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets. Device names are not case-sensitive. If you specify both an IP address and a device name, the IP address takes precedence.

6. Click **Find**.

   The **Results** list box displays the devices resulting from your search, as a listing of IP addresses or entity names, along with the domain in which the devices exist.

7. Select the device you want from the **Results** list box, and click **Select & Close** to return to the **Network Hop View** main window.

   The **Seed device** field in the **Network Hop View** toolbar is populated with the seed device IP address or host name.

8. Select the maximum number of hops displayed from the seed device from the **Hops** list.

   This setting shows more or less devices connected to the seed device.

9. Specify how to display connectivity:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

10. Click **Apply Changes**  .

    The topology you selected is displayed in the network map. Faulty devices are displayed with an associated event icon.

    Note: If you have configured cross-domain discovery, the **Network Hop View** results might include devices from a different domain to the domain in which the seed device is located. Hover the cursor over a device to see which domain it is located in.

Network map icons and symbols

The **Network Hop View** and the **Network Views** show icons representing discovered devices and subnets and the event status associated with a device.

Devices and subnets

The following tables describe the device and device connectivity icons used in the network map and network tree. Within the network map solid line indicates a connection between devices and pale dashed line indicates membership; for example, membership of a subnet or of a BGP autonomous system.

The following table describes general icons used in network maps.

Table 13. Icons used in network maps: general		
Icon	**Name**	**Description**
	Cell icon	Represents a device that is designated as a radio area network cell.
	Element management system (EMS) icon	Represents an EMS.
	End node icon	Represents end-node devices, including Windows, Linux, and Solaris workstations and printers.
	Generic logical collection icon	Represents a Generic logical collection.
	Geographical location icon	Represents a geographical location.
	Geographical region icon	Represents a geographical region.
	Manually added device or connection between devices	Used to indicate that the associated device or connection was added manually using the **Topology Management** right-click options.
	Probe icon	Used to represent a network probe.
	Radio area network (RAN) router icon	Represents a device that is designated as a radio area network router.
	Radio area network (RAN) switch icon	Represents a device that is designated as a radio area network switch.
	Router icon	Represents a device that is designated as a router.
	Subnet icon	Represents a subnet
	Switch icon	Represents a device that is designated as a switch.
	Unknown device icon	System is unable to identify the correct icon to use for this device. The most likely reason is failed SNMP access to the device.

Table 13. Icons used in network maps: general (continued)		
Icon	**Name**	**Description**
[4]	Number of connections indicator	This indicates either of the following: • In the case of a connection relationship between two devices, which is indicated by a solid line, this number indicates the number of interfaces participating in the connection between the devices. • In the case of a membership relationship, which is indicated by a pale dashed line, this number indicates the number of interfaces participating in membership, for example, of a subnet or OSPF area. The number of connections displayed is specific to the connectivity layer being displayed.
	Completely unmanaged device	The entire device, including all its interfaces, is unmanaged.
	Partially unmanaged device	Only certain components of this device are unmanaged.

The following table describes LTE icons used in network maps.

Table 14. Icons used in network maps: LTE		
Icon	**Name**	**Description**
	Antenna icon	Represents an antenna.
	Equipment Identity Register (EIR) icon	Represents an Equipment Identity Register (EIR).
	Evolved NodeB (eNodeB) icon	Represents an Evolved NodeB (eNodeB) device.
	eUtranCell icon	Represents a eUtranCell.
	Home Subscriber Server (HSS) icon	Represents a Home Subscriber Server (HSS).
	LTE pool icon	Represents an LTE pool.
	LTE sector icon	Represents an LTE sector.

Table 14. Icons used in network maps: LTE (continued)		
Icon	**Name**	**Description**
	LTE tracking area icon	Represents an LTE tracking area.
	Mobility Management Entity (MME) icon	Represents a Mobility Management Entity (MME) device.
	Policy and Charging Rules Function (PCRF) icon	Represents a Policy and Charging Rules Function (PCRF).
	Packet Data Network Gateway (PGW) icon	Represents a Packet Data Network Gateway (PGW) device.
	Serving Gateway (SGW) icon	Represents a Serving Gateway (SGW) device.

Event status

The following table shows the default event status icons.

Table 15. Default event status icons		
Severity or meaning	**Color in the Event Viewer**	**Default icon in the Network Views**
5 (critical)	Red	
4 (major)	Orange	
3 (minor)	Yellow	
2 (warning)	Blue	
1 (indeterminate)	Purple	
0 (clear)	Green	
No status has been retrieved for this device. If this persists, there may be an error.	Not displayed in the **Event Viewer**	
There are no events for this device. This icon appears in the **Network Views tree** only.	Not displayed in the **Event Viewer**	

Table 15. Default event status icons (continued)		
Severity or meaning	**Color in the Event Viewer**	**Default icon in the Network Views**
This icon appears next to unmanaged devices in the Network Views and Hop View network map. This icon also appears next to the unmanaged components in the **Structure Browser**.	Not displayed in the **Event Viewer**	
This icon appears in the Network Views and Hop View network map next to devices that contain unmanaged components.	Not displayed in the **Event Viewer**	

For more information about visualizing the network, see the *IBM Tivoli Network Manager User Guide*.

Creating user profiles for Network Operators

Create user profiles for your Network Operators and assign them to the Network_Manager_User group. This automatically assigns all the required roles to the user.

Procedure

1. Click the **Console Settings** icon and select **WebSphere Administration Console**.
2. Log in with a WebSphere Application Server administrative user.
3. Select **Users and Groups** > **Manage Users**.
4. Click the **Create** button.
5. In the **User ID** field, type a unique name to identify the user. This user ID is added to the user registry and is also used as the login account name. For example, you might type `dlucas`
6. Click **Group Membership** and then follow the steps in "Assigning user profiles to the Network_Manager_User group" on page 121 to add the user as a member of one or more existing groups.
7. In the **First name** field, type the given or first name of the user. For example, you might type `Diana`.
8. In the **Last name** field, type the family or last name of the user. For example, you might type `Lucas`.
9. Optional: In the **E-mail** field, type an e-mail address for the user. For example, you might type `dlucas@tivoli.com`.
10. In the **Password** field, type a unique password. For example, you might type `d4lucas`.
11. In the **Confirm password** field, type the same password again.
12. Click **Create**. If successful, a message displays that indicates that the user has been created. Also, the user ID and other user information is added to the user registry, and a new login account is created for the user.
13. To create another user, click **Create Another**.
14. Repeat the process until you have created all the new users.

Assigning user profiles to the Network_Manager_User group

Automatically assigns all the required roles to a Network Operator by assigning a user to the Network_Manager_User group.

About this task

The Network_Manager_User group provides all the necessary Network Manager roles for a network operator.

Procedure

1. During the process of "Creating user profiles for Network Operators" on page 120, click **Group Membership**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, the results are displayed in two lists: one list is for groups that matched the search criteria and one list, named **Current Groups**, is for groups that the user is already a member of.
6. To add the user to one or more groups, highlight the groups from the matching groups list to select them. For example, to assign users to the Network_Manager_User group, highlight `Network_Manager_User` and then click **< Add**.
7. Optional: To undo or remove the user as a member, highlight the groups from the **Current Groups** list and then click **Remove >**.
8. Return to the process of "Creating user profiles for Network Operators" on page 120 to complete the steps.

Network Manager user roles

Network Manager defines a number of default roles, which provide users with the ability to perform a predefined set of activities within Web applications.

Access to the Web applications and to functions within the Web applications depends on the roles that are assigned to users. Network Manager roles are usually assigned to users by using groups. Users can also have roles assigned to them from other products. After the administrator adds or removes roles, the revised function is not available to users until users log out and log back in to the Dashboard Application Services Hub.

Note: For information about the user roles that are defined by Cognos Analytics see the Cognos Analytics Knowledge Center at the following web address: https://www.ibm.com/support/knowledgecenter/SSEP7J.

The following table lists all the default roles that are defined by Network Manager.

Table 16. Network Manager roles

Role	Assigned to group	Description
`ncp_bookmark_admin`	`Network_Manager_IP_Admin`	User can modify network view bookmark permissions.
`ncp_config`	`Network_Manager_IP_Admin`	User can save any configuration changes that they have made.

Table 16. Network Manager roles (continued)

Role	Assigned to group	Description
ncp_config_editor	Network_Manager_IP_Admin	User can edit the following widgets. Network Discovery Configuration Configure NCIM Database Access
ncp_disco_config	Network_Manager_IP_Admin	User can view and edit the discovery configuration settings.
ncp_disco_config_alter_domain	Network_Manager_IP_Admin	User can change the domain for which they are configuring a discovery.
ncp_disco_editor	Network_Manager_IP_Admin	User can edit the Network Discovery Status widget.
ncp_disco_status	Network_Manager_IP_Admin	User can view the status of a discovery as it is running.
ncp_disco_status_control	Network_Manager_IP_Admin	User can start or stop the discovery, or run a discovery with same configuration settings. This role is ineffective without the role Network Manager IP Discovery Status.
ncp_disco_status_alter_domain	Network_Manager_IP_Admin	User can change the domain from which they are getting discovery status. **Note:** Do not remove this role from discovery administrators.
ncp_event_analytics	Not assigned to a group by default.	Enables Event Analytics right-click tools on devices in the topology graph.
ncp_gis	Not assigned to a group by default.	User can open geographical views.
ncp_gis_admin	Not assigned to a group by default.	User can edit portlet layout preferences in geographical views.
ncp_hopview	Network_Manager_User	User can access the Hop View.
ncp_hopview_editor	Network_Manager_IP_Admin	User can edit the Network Hop View widget.
ncp_manage_unmanage	Network_Manager_IP_Admin	User can set devices to managed and unmanaged status.
ncp_mibbrowser	Network_Manager_User	User can access the MIB Browser.
ncp_mibbrowser_config	Network_Manager_User	User can access the MIB Browser for configuration purposes.
ncp_mibbrowser_editor	Network_Manager_IP_Admin	User can edit the SNMP MIB Browser widget.

Table 16. Network Manager roles (continued)

Role	Assigned to group	Description
ncp_mibgraph_default_properties_config	Network_Manager_IP_Admin	User can change the MIB graph default properties. This role is ineffective without the following Network_Manager_User group roles: ncp_mibgraph_user, ncp_mibgraph_config, ncp_mibbrowser.
ncp_mibgraph_config	Network_Manager_IP_Admin, Network_Manager_User	Enables access to the SNMP MIB Graph widget and right-click tools.
ncp_mibgraph_editor	Network_Manager_IP_Admin	User can edit the SNMP MIB Graph widget.
ncp_mibgraph_user	Network_Manager_User	User can access SNMP MIB Graph.
ncp_monitor_policy	Network_Manager_IP_Admin	Enables access to the Configure Poll Policies widget, as well as access to the Create Poll Policy right-click tool.
ncp_monitor_editor	Network_Manager_IP_Admin	User can edit the following widgets. Configure Poll Definitions Configure Poll Policies
ncp_monitor_policy_alter_domain	Network_Manager_IP_Admin	User can select a domain other than the default for poll policies.
ncp_monitor_template	Network_Manager_IP_Admin	User can create a new poll policy definition.
ncp_networkhealth_dashboard	Network_Manager_User	User can access the Network Health Dashboard.
ncp_networkhealth_dashboard_admin	Network_Manager_IP_Admin	User can edit Network Health Dashboard widgets.

Table 16. Network Manager roles (continued)

Role	Assigned to group	Description
ncp_networkview	Network_Manager_User	User can access the Network Views and to display any of the following views: • User Views: Network views that are created by the user. • Group Views: Views that are assigned to the group or groups that this user belongs to. • Global Views: Views accessible to all users regardless of the group to which they belong. Users with this role can not change the view layout, unless the administrator gives them access to the Hierarchichal, Symmetric, Circular, and Tabular layout buttons. To enable users to change (but not save) the layout, set the topoviz.networkview.readonly.enablelayout=true option in the $NMGUI_HOME/profile/etc/tnm/topoviz.properties file. To grant more permissions to users, assign a different role, such as ncp_networkview_admin_user.
ncp_networkview_admin_global	Network_Manager_IP_Admin	User can create, edit, partition, and delete Global Views. These are views accessible to all users regardless of the group to which they belong. User can also perform Move operations on network views within the global views.
ncp_networkview_admin_group	Network_Manager_IP_Admin	User can create, edit, partition, and delete Group Views. These are views assigned to the group or groups that this user belongs to. This role also allows the user to perform Move operations on network views within a group view collection.

Table 16. Network Manager roles (continued)

Role	Assigned to group	Description
ncp_networkview_admin_user	Network_Manager_User	User can create, edit, partition, and delete their own set of network views. This role also allows the user to perform Move operations on network views within a user view.
ncp_networkview_admin_all_users	Network_Manager_IP_Admin	User can create, edit, partition, and delete Private Views. These are private views created by users who have the Network Manager IP Network View - Administer views for user role. This role also allows the user to perform Move operations on network views within a group view collection.
ncp_networkview_editor	Network_Manager_IP_Admin	User can edit the Network Views widget.
ncp_oql	Network_Manager_IP_Admin	User can perform and display the results of select type operations using the Management Database Access page.
ncp_oql_editor	Network_Manager_IP_Admin	User can edit the Management Database Access widget.
ncp_oql_update	Network_Manager_IP_Admin	User can perform and display the results of update type operations using the Management Database Access page.
ncp_pathview	Network_Manager_IP_Admin, Network_Manager_User	User can create, edit, and delete path views.
ncp_pathview_editor	Network_Manager_IP_Admin	User can edit the Path Views widget.
ncp_reporting_user	Network_Manager_IP_Admin, Network_Manager_User	Adds the Cognos Reporting menu item.
ncp_reporting_admin	Not assigned to a group by default.	This role is not currently used.
ncp_rest_api	Network_Manager_IP_User	Required for access to GUI elements that use RESTful APIs. Leave this role assigned to all users.
ncp_structurebrowser	Network_Manager_User	User can use the Structure Browser.
ncp_structurebrowser_editor	Network_Manager_IP_Admin	User can edit the Structure Browser widget.
ncp_structureview_entitysearch	Network_Manager_User	User can search entities in the Structure Browser.

Table 16. Network Manager roles (continued)		
Role	**Assigned to group**	**Description**
ncp_structureview_ interport_navigation	Network_Manager_User	User can navigate from a port on one device to a port on another device in the Structure Browser.
ncp_topo_mgmt	Network_Manager_IP_Admin	User can add and remove devices and connections to the topology using the topology management functionality available within the **Network Hop View**.
ncp_webtools	Network_Manager_User	User can use the WebTools.
ncp_webtools_editor	Network_Manager_IP_Admin	User can edit Web Tools, which is a set of GUIs available form the right-click menu on a device in the topology map.
netcool_rw	Not assigned to a group by default.	User can use the Management Database Access and Network Polling widgets.
noi_npi	Network_Manager_User	User can view the **Device Dashboard** and, in particular, the **Performance Insights** widget used in this dashboard.
Fix Pack 1 Fix Pack 1 noi_npi_admin	Network_Manager_IP_Admin	User can edits the **Device Dashboard** and, in particular, the **Performance Insights** widget used in this dashboard.

User roles for charting

Users must have the user IDs assigned to a chart role before they can see and work with the charting functions.

The main administrator of Jazz for Service Management already has the chartAdministrator role, and can assign users to any of the three chart roles that are available. Logged in users will have no access privileges to the charting features if their user ID has not been assigned to a chart role. These are the capabilities of the chart roles:

chartAdministrator
Users with this role can create and delete charting connections to data sources, upload charts, and can clear the charting cache (useful for troubleshooting).

chartCreator
Users with this role can upload charts, view, and edit them. They cannot create or delete chart connections nor can they clear the charting cache.

chartViewer
Users assigned to this role can select and view charts, but cannot modify them or their preferences. They cannot upload charts, create connections, or clear the charting cache.

Roles are assigned through **Users and Groups > Administrative User Roles**.

Making the network topology visible to Network Operators

To enable Network Operators to view the discovered topology, add network views to the view collections that are associated with the users or user groups of the Operators.

Before you begin

A network discovery must have run, so that it is possible to view the generated topology. Also, the required users must have been created and assigned to the Network_Manager_User user group.

About this task

By default, the itnmadmin user has access to the the network topology through the Network Views. This is because Network Manager is configured to automatically deploy an initial network view that displays all the IP network entities on the network for a domain.

Unlike the itnmadmin user, newly-created users, for example Network Operators, do not have any access to the network topology through the Network Views. You must associate views of the network with the Operators' users or with their user groups. You do this in one of the following ways:

Creating new network views
Assign a new network view to a user or user group.

Copying existing network views
Copy a network view from the itnmadmin user and assign it to a user or user group.

The itnmadminuser has access to the network views that are assigned to each user and user group. For example, to access the network views of the user group "Public", select **Public Views.** from the list. To access the views of a user called "dlucas ", select **dlucas Views**.

Procedure

- To copy a network view from the itnmadmin user to other user or groups:
  a) Click the **Incident** icon and select **Network Availability** > **Network Views**.
  b) From the list, select **itnmadmin Views**.
  c) Click **Copy or Move View**  .
  d) Select **Copy**.
  e) From the **To** list, select the network view collection to which to add the network view.

  Tip: To make the network view available to all users, select **Global**.
- To create an initial network view that displays all the subnets on a domain:
  a) Click the **Incident** icon and select **Network Availability** > **Network Views**.
  b) From the list, select the network view collection for the required user or user group and click **New View**  .

  Tip: To make the network view available to all users, select **Global**.
  c) Type a name for the network view.
  d) In the **Parent** list, select `NONE`.
  e) In the **Type** list, select `Dynamic Views - Subnet`.
  f) In the remaining fields, specify the layout and style, and the icons that represent the network view.
  The map icon is used to represent the network view in the right display panel, whereas the tree icon is used to represent the network view in the left navigation panel.
  g) Click **Filter**.
  h) Select the domain.
  i) In the **Subnet Classes** field, select **A & B** or **A, B & C**.

If you select **A, B & C**, a large number of subnets is created, because most networks contain large numbers of class C subnets.

j) Click **OK**.

- To create an initial network view that displays all the entities on the network for a domain:

a) Click the **Incident** icon and select **Network Availability** > **Network Views**.

b) From the list, select the network view collection for the required user or user group and click **New View**  .

Tip: To make the network view available to all users, select **Global**.

c) Type a name for the network view.

d) In the **Parent** list, select `NONE`.

e) In the **Type** list, select `Dynamic Views - Template`.

f) In the remaining fields, specify the layout and style, and the icons that represent the network view.

The map icon is used to represent the network view in the right display panel, whereas the tree icon is used to represent the network view in the left navigation panel.

g) Click **Filter**.

h) Select the domain.

i) In the **Template** field, select `IP Default`.

Warning: Do not use the `ip_default.xml` template if you have large or very large networks. The `ip_default.xml` template is intended mainly for educational purposes to demonstrate how the topology can be displayed. Running this template against a large or very large production topology could have a serious impact on the memory and performance of your Network Manager installation, particularly on displaying and using network views. If you have large or very large networks, create network view templates that enable operators to generate a limited set of network views or create network views manually. For more information on creating network views and network view templates, see the *IBM Tivoli Network Manager User Guide*. For more information about network sizes, see the section on deployment scenarios in the *IBM Tivoli Network Manager User Guide*.

j) Click **OK**.

Results

When Network Operators log in with their users and open the **Network Views**, they can click the network views that you created or copied for them to begin visualizing the network.

What to do next

To verify that the Operators can now display network views, select from the list a user or user group for which you have created or copied network views. For example, select **Global** if you created or copied network views for all users. The navigation tree now contains network views.

Alternatively, log out of Network Manager, and log back in as a user that now has network views assigned.

Now that the Operators have access to the topology, and can work, you can create additional network views that are designed around the access concept that you want to develop for the network. If you then want to revise Operators' access you can delete these initial network views.

For more information on administering network views, see the *IBM Tivoli Network Manager IP Edition Administration Guide*. For more information about visualizing the network, see the *IBM Tivoli Network Manager User Guide*.

Viewing network events

When you have discovered your network and given access to your operators, you can configure what events are raised on the network, and then view those events in a simple list or in the context of the network topology.

About polling the network

To poll the network, Network Manager periodically sends queries to the devices on the network. These queries determine the behavior of the devices, for example operational status, or the data in the Management Information Base (MIB) variables of the devices.

Network polling is controlled by poll policies. Poll policies consist of the following:

- Poll definitions, which define the data to retrieve.
- Poll scope, consisting of the devices to poll. The scope can also be modified at a poll definition level to filter based on device class and interface.
- Polling interval and other poll properties.

Note: Network Manager does not poll non-IP entities, such as layer 1 optical devices and radio access network devices. These devices are automatically set to unmanaged status.

Network Manager uses the IBM Tivoli Netcool/OMNIbus SNMP trap probe and the Syslog probe to monitor the network. To run Tivoli Netcool/OMNIbus probes, use Tivoli Netcool/OMNIbus process control.

For more information about how to use Tivoli Netcool/OMNIbus process control, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

The polling process is controlled by the ncp_poller process. The ncp_poller process stores SNMP information in the ncmonitor database; other data is stored in-memory.

Network Manager has a multiple poller mechanism to distribute the load. If the default pollers cannot handle the polling demands for your network, you might need to confgure additional pollers.

Enabling polls

To generate network events, you must enable some of the default poll policies.

About this task

By default, only a few poll policies are enabled. Enabling poll policies creates network traffic. Only enable those poll policies that will give you useful information about your network.

Which poll policies to enable depends on what network technologies you are using, what device types are in your network, and what kind of information you want to monitor. As an example, we will enable some poll policies and later we will view events generated by these policies.

Procedure

1. Click the **Administration** icon and select **Network** > **Network Polling**.
2. Select the check box next to the **Default Interface Ping** poll policy. This poll policy uses the Default Interface Ping poll definition to ping all interfaces on every main node with a valid IP address. Because in a typical network many interfaces might be in an administratively down state, this policy is likely to generate significant traffic and some network events.
3. Select the check box next to the **cpuBusyPoll** poll policy. This poll policy uses the cpuBusyPoll poll definition to generate an event when the average CPU usage of a Cisco device exceeds 80%.
4. Select the check box next to the **ciscoEnvMonTemperatureState** poll policy. This poll policy uses the ciscoEnvMonTemperatureState poll definition to generate an event when the temperature of a Cisco device is reported as anything other than normal.
5. Click **Enable Selected Policies** to enable these policies.

6. Click **OK**.

What to do next

Each poll runs at certain intervals. After half an hour or so, check whether any events can be seen in the network views and **Event Viewer**.

Viewing events in the network views

You can use the network views to check that certain sections of the network or certain kinds of devices are free of problems.

Before you begin

To perform this task you must be logged in as the administrator, or the administrator must have given you access to the relevant network views.

About this task

In the Enabling Polls task, you enabled some poll policies that monitor Cisco routers for various error conditions. Now you can use the network views to see if any of the routers on your network have events associated with them.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the **All Routers** network view nodes.

   All routers that have been discovered are displayed.
3. Any routers with any events against them are displayed with an event status icon next to them.
4. Right-click on any device to see the tools available for working with the device.

Related reference

Default event status icons

The **Structure Browser** in table mode, the **Network Views**, and the **Network Hop View** show the severity of events affecting a device or other network entity such as a card, by showing an alert icon adjacent to the entity.

Viewing events in the Event Viewer

You can use the **Event Viewer** to see all network events.

About this task

In the Enabling Polls task, you enabled some poll policies that poll device interfaces, and others that monitor Cisco routers. Additionally, all devices in the network (except end nodes such as printers) are pinged by default. Now you can use the **Event Viewer** to see if any events have been raised on the network. You can also see the network context in which an event appears using the **Network Hop View**

The **Fault-Finding View** page appears with the **Event Viewer** widget above and the **Network Hop View** widget below.

Note: When you first open the **Fault-Finding View** page, the **Event Viewer** widget displays all events in the ObjectServer and the **Network Hop View** widget is empty.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Fault-Finding View**.
2. Select an event of interest in the **Event Viewer**, or right-click an event and then click **Broadcast Topology Context**.

The **Network Hop View** GUI now displays the network topology related to the selected event.

Restriction: Results vary if you select multiple events in the **Event Viewer**.

- If all the selected events occurred on the same network device, then the **Network Hop View** widget only displays the network topology related to that device.
- If the selected events occurred on different devices, then the **Network Hop View** widget does not display any network topology .

What to do next

Now you can investigate the events. You can investigate the root cause of events, view the structure of devices related to an event, and perform other tasks by right-clicking on an event.

Related tasks

Investigating events

Use features of the **Event Viewer** to support network troubleshooting. You can use the **Event Viewer** to show affected network devices, identify root-cause events, and identify events that have a major service impact.

Part 3. Setting up network visualization

To set up network visualization, you can set up Network Views for your operators, and configure users, roles and groups.

Related tasks

Configuring GUIs

You can change the appearance and functionality of the Hop Views; update MIB information; and configure the presentation of events from unmanaged devices.

Chapter 6. Administering the GUI framework

Use the functions of the Dashboard Application Services Hub within Jazz for Service Management to administer pages, folders, views, widgets, and console preference profiles.

About this task

The Dashboard Application Services Hub is a GUI container used by Network Manager and by other products.

For information about working with Dashboard Application Services Hub, including working with the console, pages, and folders, see the Jazz for Service Management Knowledge Center, at https://www.ibm.com/support/knowledgecenter/SSEKCU.

Network Manager requires Dashboard Application Services Hub Version 3.1.3.9 or later.

Network Manager requires Jazz for Service Management V1.1.3.9 or later.

See the following topics for information about portlets that are specific to Network Manager and for information about accessing online help.

Access to online help

Online help is topic-oriented, procedural, or reference information that you can access from the product installation, to assist you in the use of the product and to complete tasks.

You can search and browse within the online help to troubleshoot and find solutions for tasks you want to perform. Access to online help, as users work with the product, helps users to expand their knowledge about the product. You can access the online help from either the top-level online help or from the context-sensitive online help.

- Top-level online help. This online help displays a table of contents view of all available online help topics, for all products that are installed into your instance of Dashboard Application Services Hub.
- Context-sensitive online help. This online help links directly to documentation about the current panel. From this panel help topic, you can browse throughout the online help. After a product installation, this online help is disabled by default as the containing widget title bars are also disabled by default.

Accessing the top-level online help

The top-level online help displays a table of contents view of all online help topics.

About this task

Access to the top-level help is enabled by default. Within the **Contents** tab of the top-level help, you can expand, collapse, and select topics to browse around all topics within the online help. Complete the following steps to access the top-level online help.

Procedure

1. Within the Dashboard Application Services Hub navigation bar, select the **Help** icon  . The **Help** menu displays.
2. From the **Help** menu, select **InfoCenter**. The **Help System** window opens.
3. Within the **Help System** window, select **Using Network Manager**.

Results

The top-level online help for Network Manager is displayed.

What to do next

- Within the **Contents** tab of the top-level help, expand, collapse, and select topics to browse around all topics within the online help.
- Enter some text in the **Search** field to find any related online help.
- Use the available icons in the **Help System** toolbar to print or bookmark topics, or to move forwards and backwards between topics.

Enabling access to context-sensitive online help

An administrator can enable access to context-sensitive online help. This online help enables users to directly access documentation that is related to the current panel. From this panel help topic, users can browse throughout the online help.

About this task

After a product installation, this context-sensitive online help is disabled by default as the containing widget title bars are also disabled by default. If an administrator enables context-sensitive online help, users can directly access documentation that is related to the current panel. After access to context-sensitive online help is enabled, you can browse through all documentation topics within the online help. Complete the following steps to enable access to context-sensitive online help.

This access to context-sensitive online help might not work for some pages as the GUI might pre-date Dashboard Application Services Hub, or there might be no context-sensitive online help for the page.

Procedure

1. As the administrator user `itnmadmin`, display the view where you want to enable access to the online help. For example, if you want users to be able to access in-context online help for the Network Hop View, open the Network Hop View. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. In the views title bar, click the **Page Actions** icon  .
3. Select **Edit Page**. The view changes to show a view toolbar with a series of buttons and a widget palette.
4. Within a view, there can be one or more widgets. Select the widget for which you want to enable access to the context-sensitive online help.
5. In the view toolbar, select **Widget** > **Skin** > **Default**. The widget title bar for the widget is displayed and the **Help** icon is available within the widget title bar.
6. In the view toolbar, select **Save and Exit**.

Results

The widget title bar that contains the **Help** icon displays and access to context-sensitive online help for the selected widget is enabled for all users.

What to do next

- To access context-sensitive online help, click the **Help** icon  within the widget title bar.
- To enable access to context-sensitive online help for another widget, repeat all the steps.
- To browse to other topics within the online help, either expand the icons in the navigation pane or enter text in the **Search** field.
- To disable access to context-sensitive online help for a widget, go to the view toolbar and select **Widget** > **Skin** > **Default no title**

Network Manager widgets

Use this reference information to help you configure customized Network Manager pages.

The following topics provide more information on Network Manager widgets.

List of Network Manager widgets

You can use Network Manager widgets for creating pages.

The following Network Manager widgets are available to add to a page.

- Configure NCIM Database Access
- Configure Poll Definitions
- Configure Poll Policies
- Management Database Access
- Network Discovery Configuration
- Network Discovery Status
- Network Hop View
- Network Views
- Path Views
- Path View Administration
- SNMP MIB Browser
- SNMP MIB Graph
- Structure Browser
- Reporting (configures Tivoli Common Reporting)

You might also see widgets from other products;.for example, the Tivoli Netcool/OMNIbus Web GUI **Event Viewer**.

Editable widget parameters

Use this information to understand which parameters are associated with each Network Manager widget and how each of these parameters affects the appearance of the widget.

To modify widget parameters, refer to the information about customizing a Dashboard Application Services Hub widget in the Jazz for Service Management information center at https://www.ibm.com/support/knowledgecenter/SSEKCU.

Important: The Network Views, Hop View, and Structure Browser widgets refresh themselves. There is no need to set a global refresh on these widgets.

The editable parameters for the Network Manager widgets are as follows.

"Database Configuration" on page 138
"Discovery Configuration" on page 138
"Discovery Status" on page 138
"MIB Browser" on page 138
"Monitor Configuration Poll Policy" on page 138
"Monitor Configuration Template" on page 138
"Management Database Access" on page 138
"Structure Browser" on page 138
"Topology HopView" on page 139
"NetworkViews" on page 139
"Path Views" on page 139

Database Configuration

There are no editable parameters for this widget.

Discovery Configuration

There are no editable parameters for this widget.

Discovery Status

There are no editable parameters for this widget.

MIB Browser

MIB Browser

Domain
Name of the domain that the widget presents as default

Object ID
SNMP Object ID of the node for which MIB information is requested

Host
Name of the host that has where the Helper Server is running

Show Results Only?
Indicates whether only the results of the MIB query are displayed. The default value is False.

Monitor Configuration Poll Policy

There are no editable parameters for this widget.

Monitor Configuration Template

There are no editable parameters for this widget.

Management Database Access

Management Database Access

Domain
Name of the domain that the widget presents as default

Query
SQL query

Service
Name of management database on which the query is run

Show Results Only?
Indicates whether only the results of the query are displayed. The default value is False.

Structure Browser

Structure Browser

Entity ID
Entity ID of the device whose structure is being requested.

View Mode
Specifies which mode the widget loads: tree or table.

Note: Table mode is only available when the Structure Browser is displayed as a widget.

Table Mode
Select the type of information to display within the table.

Topology HopView

Topology HopView

Domain
Name of the domain that the widget presents as default

Seed device
Pivot device around which the Network Hop View must be displayed

Hops
Number of hops to display from the pivot device

Connectivity
Type of connectivity to display in the network map; options are IP Subnets, Layer1, Layer 2, Layer 3, PIM, and IPMRoute

Default value: IP Subnets

Layout
Layout style of the network map; options are Symmetric, Hierarchical, Orthogonal, and Circular

Default value: Symmetric

Show End Nodes?
Indicates whether to display end nodes in the map. The default value is False.

NetworkViews

Topology Network Views

Network Views Properties

Show Network Views Tree
Indicates whether to display the network view navigation tree.

Choose Default Tab
Indicates whether to show the **Bookmarks** or **Libraries** tab as the default tab.

Libraries Treetable Properties

Map ID
ID of a specific network view to be displayed in the treetable.

Bookmarks Treetable Properties

Width
Specifies the width of the columns in the **Bookmarks** treetable.

Hidden Columns
Provides the option to hide the **Max** column, which shows the maximum alert status for all devices within a network view.

Locked Columns
Provides the option to lock the **Max** column.

Sort Column
Specifies which column to sort on.

Sort Order
Specifies the sort order.

Path Views

Topology Path Views

Path View Properties

Show Path Views Tree
Indicates whether to display the path views navigation tree.

Path View ID
ID of the path view to be displayed.

Treetable Properties

Width
Indicates the width of the column.

Hidden Columns
Indicates whether a column should be hidden. Master columns can not be hidden.

Locked Columns
Prohibits scrolling. Master columns can not be locked.

Sort Column
Specifies how the master column is to be sorted.

Sort Order
Indicates whether columns should be sorted in ascending or descending order. Parent rows are sorted first, then child rows.

Related information

Customizing a widget Depending on how a widget was configured when it was created and any shared settings applied by your administrator, you can customize a widget's setting.

Event information for Network Manager widgets

Refer to this table to get information about the publish events and subscribe events for Network Manager widgets. Use this event information when you create a new custom widget and you want to wire your custom widget with an existing Network Manager widget.

Table 17. Event information for Network Manager widgets

Widget name	Event type	Event name	Event description
Dashboard Network Views	Publish event	`NodeClickedOn`	Left-clicking a node on the widgets topology canvas publishes a `NodeClickedOn` event that contains the Network Manager *ViewId*.
Network Hop View	Publish event	`NodeClickedOn`	Left-clicking a node on the widget's topology canvas publishes a `NodeClickedOn` event that contains the Network Manager `entityId` .
	Subscribe event	`NodeClickedOn`	Internally, this `NodeClickedOn` event that contains `entityId` converts to a `showDevice` event (which contains `NmosObjInst`, `NmosEntityId`, and so on) and displays the device as a node on the widget's topology canvas based on the `entityId`
	Subscribe event	`showEntity`	Similar to the description for the **Network Hop View** subscribe event, for `NodeClickedOn`.
	Subscribe event	`Showdevice`	Similar to the description for the **Network Hop View** subscribe event, for `NodeClickedOn`.

Table 17. Event information for Network Manager widgets (continued)

Widget name	Event type	Event name	Event description
Network View	Subscribe event	`NodeClickedOn`	Subscribes to a `NodeClickedOn` event and displays device structure based on the events `entityId` attribute.
	Publish event	`showEvents`	Right-clicking a node on the widget's topology canvas and choosing **Show Events** publishes a `showEvents` event that contains *Transient Events Filter name* and the Network Manager *ViewId*.
	Publish event	`showEntity`	Right-clicking a node on the widget's topology canvas and choosing **Show Device Structure** publishes a `showEntity` event that contains the Network Manager *Entity Id*.
Network Views	Not applicable. This widget does not publish or subscribe to events.		
Path Views GUI	Not applicable. This widget does not publish or subscribe to events.		
SNMP MIB Grapher	Not applicable. This widget does not publish or subscribe to events.		
SNMP MIB Browser	Not applicable. This widget does not publish or subscribe to events.		
Structure Browser	Subscribe event	`NodeClickedOn`	Subscribes to a `NodeClickedOn` event and displays device structure based on the events *Entity Id* attribute.
	Subscribe event	`showEntity`	Subscribes to a `showEntity` event and displays device structure based on the *Entity Id*.
	Publish event	`showPerformanc e`	Within the **Structure Browser**, when you open a node and choose the **Show Interface** tab, the `showPerformance` event publishes the *deviceId* and the *interfaceId*.

Chapter 7. Administering network views

Network Views shows logical groupings of devices that you may need to monitor within your network. Create new views or change existing views to help network operators visualize devices.

About network views

Use this information to understand what a network view is, the different types of network view, and the types of user access to network view collections.

Use a network view to create a custom grouping of any set of devices, sub-nets, VLANs or other device collections for monitoring.

Network views can also be created based on device events. For example, you can create a network view that displays all devices on which a Critical severity event has occurred.

Standard network views

Create a standard network view to group any set of devices, sub-nets, VLANs or other device collections for monitoring. Standard network views are also referred to as *network views*.

For example, if you need to monitor the status of two specific sub-nets, you can group them in a standard network view. Once created, this network view appears in the Navigation Panel, with a name and in a position in the navigation tree that you specify.

For example you can create a new `My Views` container node in the navigation tree, name your new network view `My Subnets` and place this new view in the `My Views` container.

As the network changes and the topology is updated following discoveries, the content of the network view changes accordingly. For example, if new devices are added to the subnet, then these devices are automatically added to the network view after they have been discovered.

Usage considerations

Standard network view are useful for operators who monitor a part of the large network and need to focus on the devices, subnets or other device collections within their part of the network.

Create a standard network view if:

- You want to create views of particular device collections only, rather than all device collections of a specific type.
- You want to create a view that contains more than one device collection, rather than one view for each device collection.

Related tasks

Creating standard network views
Network Manager has two types of views: standard and dynamic. You can create these standard views.

Dynamic network views

Dynamic network views are based on the devices or collections that you specify and based on all the network topology data. Dynamic network views are also referred to as *dynamic views*

If you create a dynamic view of VLANs, multiple VLAN network views are created, one for each VLAN. The result is therefore a node in the **Navigation Panel** for each VLAN in the network.

As the network changes and the topology is updated following discoveries, the VLAN nodes in the **Navigation Panel** might appear or disappear. For example, if any VLANs are removed from the network, then after another discovery, the corresponding VLAN network views automatically disappear.

Usage considerations

The dynamic view option is useful for keeping track of all the devices and device collections in your network. This option is therefore of greater use to an administrator who needs to keep track of device changes across the entire network. This option is also useful for operators of smaller networks who monitor an entire network.

Do not create a dynamic view if:

- You want to create views of particular device collections only, rather than all device collections of a specific type.
- You want to create a view that contains more than one device collection, rather than one view for each device collection.

If you want to achieve either of the above results, create a standard network view.

Related tasks

Creating dynamic network views
Network Manager has two types of views: standard and dynamic. You can create these dynamic views.

Access configuration for network view collections

Use groups and role assignments to administer read-write and read-only access to network view collections, and administer privileges to copy and move network views between network view collections.

Network view collections

A network view collection is a grouping of network views accessible to a single user, a restricted set of users, or all users. You configure user access to network view collections by assigning roles to users and assigning users to groups.

Types of network view collection

TopoViz categorizes network view collections as follows:

Group views
Network views that are assigned to the group or groups to a user belongs. For example, divide users into geographical groups. Access to network views can then be restricted based on membership of the groups.

User views
Network views created by a user. Only the user and certain administrators can see these views.

Global views
Network views that are accessible to all users regardless of the group or groups to which they belong.

Types of user access to network view collections

User access to network views falls into the following two categories:

Read-write access
Enables the user to create, edit, delete, and partition network views. A user with this type of access can also copy and move network views between group, user and global view collections. Administrator access also enables users to display network views. To give users read-write access, you must assign the user the `netcool_rw` role, in addition to the Network Views administrative roles.

Read-only access
Enables the user to only display network views.

Example

The following table shows an example of assignment of roles to enable read-write or read-only access for different users within the "London" and "New York" groups.

The user "bob" is a member of both the "London" and "New York" groups and has read-write access across both groups. In addition to the group views, user can access their own user views and the global views.

Table 18. Configuring user access to network view collections

Group	Users	Roles	Accessible view collections	Access Level
London	ben (London)	ncp_networkview netcool_ro	London Views Global Views	read-only
	betty (London)	ncp_networkview netcool_rw ncp_networkview_admin_user	betty Views	read-write
			London Views Global Views	read-only
New York	barbara (London)	ncp_networkview netcool_rw ncp_networkview_admin_user ncp_networkview_admin_group	barbara Views London Views	read-write
			Global Views	read-only
	bob (London and New York)	ncp_networkview netcool_rw ncp_networkview_admin_all_users ncp_networkview_admin_group ncp_networkview_admin_global	ben Views, betty Views, barbara Views bob Views jerry Views, judy Views, jonas Views London Views New York Views Global Views	read-write
	jerry (New York)	ncp_networkview netcool_rw ncp_networkview_admin_user ncp_networkview_admin_group	jerry Views New York Views	read-write
			Global Views	read-only
	judy (New York)	ncp_networkview netcool_rw ncp_networkview_admin_user	judy View	read-write
			New York Views Global Views	read-only
	jonas (New York)	ncp_networkview netcool_ro	New York Views Global Views	read-only

Creating network view containers

Create a container to group together network views and store them in a single node in the **Network View** navigation panel.

About this task

Restriction: Starting with Network Manager Version 4.2, you can not use a filtered view to contain other network views. You can only set containers as Network View parents. This restriction is intended to avoid performance issues with large or complex views.

To create a network view container:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Container`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Background Image

   Click **Browse**  to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.
4. Click **OK**.

Results

The new container node is displayed in the **Network View Tree**.

What to do next

Now, create new view within the container, or move existing views to the container.

Related tasks

Creating network views

Create network views to show only those parts of the network that you need to monitor. There are two types of network views: standard views and dynamic views.

Copying or moving views

Move network views if you want to make private views available on a group-wide or global basis. Copy network views into your private collection if you want to change a group or global view without any impact on the original view.

Creating network views

Create network views to show only those parts of the network that you need to monitor. There are two types of network views: standard views and dynamic views.

About this task

Both standard views and dynamic views provide a custom grouping of any set of devices, sub-nets, VLANs or other device collections for monitoring.

Certain types of network view can be created based on device events. For example, you can create a network view that displays all devices on which a Critical severity event has occurred. To create network views based on device events, you must create a network view with an event filter.

Creating standard network views

Network Manager has two types of views: standard and dynamic. You can create these standard views.

About this task

Certain types of network view can be created based on device events. For example, you can create a filtered network view that displays all devices on which a Critical severity event has occurred.

Creating dependency network views

Dependency network views show devices that are dependent on specified independent entities. For example, within a radio access network (RAN), base stations are modeled as being dependent on base station controllers. You can create a dependency network view to display all of the base stations dependent on one or more base station controllers.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

To create a dependency network view:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

Name
Type a name for the network view, dynamic view, or network view container.

Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent
Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

Type
Select `Dependency`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Complete the tab as follows:

Domain
Select your network domain.

Class
This drop-down lists the classes of independent entity in your network. Select a class from the list. For example, to create a network view that shows all the devices that are dependent on specified RAN base station controllers, select `RAN Base Station Controller`.

Connectivity
Select `Default`. The network view is displayed using the most appropriate connectivity for the type of collection you selected. You also have the option of specifying one of the other following connectivity options:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

Available independent entities
Select the independent entities for which you want to display dependent devices and click **Select**  to move them to the **Selected independent entities** list.

5. Click **OK**.
   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Creating network views of device collections

To monitor collections of devices, such as subnets, VPNs, and MPLS VPNs, in a part of a large network, create a standard network view of a device collection. Standard views of device collections are changed automatically as the topology changes after a discovery.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

You can create the following device collections:

- Border Gateway Protocol (BGP) Autonomous Systems (AS), clusters, and networks
- Data Centers
- Element Management System (EMS) systems
- Generic collections
- Geographic locations
- Geographic regions
- Global Virtual Local Area Networks (VLANs)

- Hot Standby Routing Protocol (HSRP) groups
- Internet Group Membership Protocol (IGMP) groups
- Internet Protocol (IP) paths
- IPM Route Multicast Distribution Trees (MDT)
- ITNM Services
- Logical collections
- LTE pools
- LTE public land mobile networks (PLMNs)
- LTE tracking area collections
- MPLS Traffic Engineered (TE) tunnels
- Open Shortest Path First (OSPF) areas and routing domains
- Port Groups
- Protocol Independent Multicast (PIM) groups
- Radio Access Network (RAN) circuit core, GSM cells, location areas, packet core, routing areas, and UTRAN cells
- Stacks
- Subnets
- Virtual Private Networks (VPNs)
- VLAN Ports
- VLAN Trunking Protocol (VTP) domains
- VTP domains
- WLAN 802.11
- WLAN Channel
- WLAN SSID

To create a standard network view of one or more device collections in your network:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Collection`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Complete the tab as follows:

Domain
Select your network domain.

Type
Select the required device collection. The **Available Collections** list is automatically populated based on your selection.

Connectivity
Select `Default`. The network view is displayed using the most appropriate connectivity for the type of collection you selected. You also have the option of specifying one of the other following connectivity options:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

SubGraph
If the visualization of logical groups has been enabled by the administrator, this menu is available. Select **Enable** to display entities in logical groups surrounded by a boundary (cloud), which can be expanded and collapsed. Select **Disable** to display entities in logical groups connected to a ring, which cannot be expanded or collapsed.

Available Collections

Select the device collections that you want to display in the network view and click **Select** to move them to the **Selected Collections** list.

5. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Related tasks

Creating dynamic views of subnets
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

Creating dynamic views of MPLS VPNs
To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

Creating network views of MPLS VPNs

To have the option of showing or hiding CE (customer edge) devices, create a network view of MPLS VPNs.

About this task

You can also create an MPLS VPN view by creating a network view of device collections. However, you do not have the option to show or hide CE devices.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View** .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `MPLS VPN`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Complete the tab as follows:

Domain
Select your network domain.

CE Devices
Select the `Hide` or `Show`.

Available MPLS VPNs

Select the MPLS VLANs that you want to display in the network view and click **Select**  to move them to the **Selected MPLS VPNs** list.

5. Click **OK**.

The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Creating network views of VPLS VLANS

To monitor Virtual Private LAN Service Virtual Private Networks (VPLS VPNs), you can create network views of specific VPNs.

About this task

VPLS VPN network views are created automatically. You can also create them manually. To create a network view of a particular VPLS VPN, complete the following steps.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. In **Network Views**, within the **Libraries** tab, click **New View**  .
3. Complete the **General** tab as follows:

Name
Type a name for the network view, dynamic view, or network view container.

Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent
Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select NONE.

Type
Select VPLS VPN.

Layout
Select Orthogonal, Circular, Symmetric, Hierarchical, or Tabular layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Complete the tab as follows:

Domain
Select your network domain.

CE Devices
Select Hide or Show.

Available VPLS VPNs

Select the VPLS VLANs that you want to display in the network view and click **Select**  to move them to the **Selected VPLS VPNs** list.

5. Click **OK**.
The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Creating custom network views

The custom view groups any set of devices, sub-nets, VLANs or other device collections in a domain for monitoring. Create a custom view to manually add devices. Custom views are empty when they are first created. Devices can be added from any network view in the domain for which the custom view was created.

About this task

Custom views do not use SQL filters. The view is updated as you add and remove devices.

Note: When you add an unassigned device to a custom view, the Unassigned view is automatically updated to remove the device.

An administrator can set the value of the **topoviz.customview.enable** property in the $NMGUI_HOME/profile/etc/tnm/ file to enable or disable custom views. This property is also used to enable or disable Unassigned views.

Complete these steps to create a custom view.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click the **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select NONE.

   Type
   Select Custom.

   Layout
   Select Orthogonal, Circular, Symmetric, Hierarchical, or Tabular layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Background Image

   Click **Browse**  to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.
4. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

What to do next

Add devices, including unassigned devices, to the custom view.

Adding devices to a custom view

You can group any set of devices, subnets, VLANs, or other device collections in one domain in a custom view.

About this task

After you create a custom view, the view is empty. Devices can be added to a custom view from any network view in the domain for which the custom view was created. The devices are copied, that is, they also remain in their original view. If you add an unassigned device to a custom view, the device is automatically removed from the unassigned view.

Complete these steps to add one or more devices to a custom view.

Procedure

1. From an existing view, select one or more devices.
2. Right-click the selected device or devices and select **Add To View** from the context menu.
3. From the **Add View** window, under **Add devices to custom view**, specify a value for these fields:**To** and **View**.
4. First, choose a view from the **To** drop-down menu.

   This designates the category of view, for example `itnmadmin` views, to add the device to.
5. Next, click the **View Tree** button.

   A tree is displayed that contains the custom views that are available for the **Type** you selected. The custom views in the tree are highlighted in bold and italics.
6. Select a custom view from the tree, and then click **OK**.

   Note: You must click **OK** below the tree, before clicking **OK** for **Add selected nodes to**. If you do not click **OK** below the tree, an error message is displayed.
7. Click **OK** to add the selected devices to the custom view.

Removing devices from a custom view

Remove one or more devices from a custom view if you no longer want the device to be assigned to the custom view.

About this task

Network Manager automatically updates network views to add or remove devices. The custom view is the only view that is not automatically updated. If you want to remove a device from a custom view, you must remove the device. Complete these steps to remove one or more devices from a custom view.

Note: If an unassigned view exists for a domain, any devices removed from the custom view are automatically added to the unassigned view if they do not exist in any other network view.

Procedure

1. Navigate to the custom view from which you want to remove one or more devices.
2. From the custom view, select the devices.
3. Right-click to access the context menu and then select **Remove from view**.
4. When the confirmation window displays, click **Yes** to remove the selected devices from the custom view.

Creating network views for unassigned devices

Create a network view for unassigned devices. The Unassigned view groups all devices in a domain that are not currently assigned to a network view. The view is updated dynamically as devices are added and removed from views in the domain.

About this task

The Unassigned view acts as a placeholder for network devices that do not belong to other views. From the Unassigned view, an operator can assign devices to a network view.

Unassigned views do not use SQL filters because they are automatically created by querying the network for unassigned devices. The view is updated dynamically as devices are added and removed from views in the domain.

An administrator can set the value of the **`topoviz.customview.enable`** property in the `etc/tnm/topoviz.properties` file to enable or disable unassigned views. This property is also used to enable or disable custom views.

Complete these steps to create an Unassigned view.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Unassigned`.

   Layout
   Select Grid or Tabular.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Background Image

   Click **Browse**  to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Results

The Unassigned view is created when devices that are not in another view are automatically added to the unassigned view.

What to do next

You can select an unassigned device and right-click to add the device to a network view.

Creating filtered views

Use a filtered view to view parts of the network based on topology database filters; for example, a network view showing all Cisco devices on a given subnet.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. Click the **Libraries** tabe and click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Filtered`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style

Specify whether the background image is to be centered or tiled.

Line Status

Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Set up the filter.

   You have the following options:

   - Click the **Filter** tab, and select a domain. Select the attribute table that you want to use in the filter and type an SQL WHERE clause in the **Filter** field.
   - Click the **Filter** tab and click **Edit**  to use the Filter Builder GUI. The Filter Builder has basic and advanced modes:
     - In basic mode, select a field, comparator, and value from the lists. Use the radio buttons to create Boolean relationships that combine multiple filters. To add more filters, click **Add new row**  .
     - In advanced mode, type the SQL WHERE clause into the field. Prefix each column name from the table that you query with the table alias `t.`. For example, `t.entityName like 'rtr%'`

   The SQL syntax differs depending on which database you use to store topology. See the documentation for your database type.

5. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
6. From the **Connectivity** list, select the required connectivity:

Layer 1

Displays all physical connections.

Layer 2

Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3

Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets

Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

7. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Sample filters

The following examples show the different ways to build a typical filter. The filter retrieves all Cisco devices on subnet 172.20.10.

To build a filter by typing SQL WHERE statements:

1. On the **Filter** tab, from the **Table** list, select `ipEndPoint`. In the **Value** field, type `subnet like '172.20.10.%'`.
2. Click **Add new row**  .
3. From the **Table** list, select `chassis`. In the **Value** field, type `className like 'Cisco'`.
4. Click **OK**.

To build a filter by using the **Filter Builder**:

1. On the **Filter** tab, from the **Table** list, select `ipEndPoint`. Click  . The **Filter Builder** is displayed.
2. On the **Basic** tab, select `subnet` from the **Field** list.
3. From the **Comparator** list, select =.
4. In the **Value** field, type `172.10.10.6` and click **OK**.
5. On the **Filter** tab, from the **Table** list, select `chassis`. Click  . The **Filter Builder** is displayed.
6. Click **Add new row**  .
7. From the **Field** list, select `className`.
8. From the **Comparator** list, select =.
9. In the **Value** field, type `Cisco`.
10. Click **OK**.

Example topology filter: main node filter

This example shows you how to create a network view that filters based on main node IP addresses only.

Before you begin

Before you begin this task, you need to follow the instructions described in the task "Creating filtered views". When you reach the step in which you set up the filter for the network view, perform the following steps.

About this task

In this example you will create a network view that filters on main node IP addresses that meet the following criteria: any IP address that has 172.18, 172.19, or 172.20 as the first two octets.

Procedure

1. Click the **Filter** tab.
2. From the **Domain** list, select your network domain.

3. In the **Table** column, select mainNodeDetails.
4. Open the **Filter Builder**, by clicking **Open Filter Builder**  .
5. In the Filter Builder, under **Basic**, use the lists and fields to build the required query: First create the part of the query that filters for any IP address that has 172.18 as the first two octets.
   a) From the **Field** list select ipAddress.
   b) From the **Comparator** list select like.
   c) In the **Value** field type 172.18%
      The percent sign (%) is a wildcard.
6. Next, create the part of the query that filters for any IP address that has 172.19 as the first two octets.
   a) Click **Add new row**  to add a new row to the Filter table.
   b) From the **Field** list select ipAddress.
   c) From the **Comparator** list select like.
   d) In the **Value** field type 172.19%
7. Next, create the part of the query that filters for any IP address that has 172.20 as the first two octets.
   a) Click **Add new row**  to add a new row to the Filter table.
   b) From the **Field** list select ipAddress.
   c) From the **Comparator** list select like.
   d) In the **Value** field type 172.20%
8. Ensure that the Boolean relationship used to combine the three filters that you just defined is **Any**.
9. Click **OK** to complete the definition of the filter.

What to do next

Now, complete the remaining steps in the task "Creating a filtered network view".

Example topology filter: all Cisco devices on a subnet

When creating a filtered network view, create a topology filter to filter the parts of the topology to show in the network view. For example, as part of the filtered network view you can create a filter to show all Cisco devices on a given subnet.

Before you begin

This task shows you how to create an example topology filter for a filtered network view.

About this task

Before you begin this task, you need to follow the instructions described in the task "Creating filtered views". When you reach the step in which you set up the filter for the network view, perform the following steps.

Procedure

1. Click the **Filter** tab.
2. From the **Domain** list, select your network domain.
3. Set up the subnet part of the filter. In the **Table** column, select the ipEndPoint NCIM topology table.
4. Open the Filter Builder, by clicking **Open Filter Builder**  .
5. In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a) From the **Field** list select subnet.
   b) From the **Comparator** list select like.
   c) In the **Value** field type a subnet identifier.

For example, to specify the subnet 172.20.100.0, type the text 172.20.100%. The percent sign (%) is a wildcard.

d) Click **OK** to complete the definition of the subnet part of the filter.

The **Filter** column value for ipEndPoint now reads as follows: subnet like '172.20.100%'.

6. Set up the part of the filter that filters by device type. Click **Add new row** to add a new row to the Filter table.
7. In the **Table** column, select the chassis NCIM topology table.
8. Open the Filter Builder, by clicking **Open Filter Builder**.
9. In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a) From the **Field** list select className.
   b) From the **Comparator** list select like.
   c) In the **Value** list type Cisco%.
   d) Click **OK** to complete the definition of the device type part of the filter.

   The **Filter** column value for chassis now reads as follows: className like 'Cisco%'.
10. Ensure that the Boolean relationship used to combine the two filters that you just defined is **All**.

What to do next

Now, complete the remaining steps in the task "Creating a filtered network view".

Example event filter: all devices with Critical events

When creating a filtered network view, create an event filter to filter topology based on events. For example, as part of the filtered network view you can create a filter to show all devices with events of Critical severity.

Before you begin

This task shows you how to create an example event filter for a filtered network view.

About this task

Before you begin this task, you need to follow the instructions described in the task "Creating a filtered network view". When you reach the step in which you set up the filter for the network view, perform the following steps.

Procedure

1. Click the **Filter** tab.
2. From the **Domain** list, select your network domain.
3. In the **Table** column, select the activeEvent table.
4. Open the Filter Builder, by clicking **Open Filter Builder**.
5. In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a) From the **Field** list select Severity.
   b) From the **Comparator** list Select =.
   c) From the **Value** list select Critical.
   d) Click **OK** to complete the definition of the filter.

   The **Filter** column value for the activeEvent table now reads as follows: Severity = Critical.

Note: The activeEvent table contains a subset of fields from the Tivoli Netcool/OMNIbus alerts.status table. For information on the fields in the alerts.status table, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

What to do next

Now, complete the remaining steps in the task "Creating a filtered network view".

Creating filtered views using variables

Use a variable in a filtered view to create complex views. For example, create a view of all devices with events older than one hour.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

You can use a variable in the filter. The variable is replaced by the appropriate value retrieved from the server. The variable name must be in the form *{%variable}*.

Restriction:

The only variable supported is {%serverTime}. The {%serverTime} variable is replaced with the current time on the Network Manager server, expressed as a UNIX epoch time (seconds after midnight on 1 January 1970 UTC).

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Filtered`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Background Image

   Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Set up the filter:
   a) Click the **Filter** tab.
   b) From the **Domain** list, select your network domain.
   c) In the **Table** column, select the database table that contains the variable you want to use. For the `{%serverTime}` variable, select the **activeEvent** table.
   d) In the **Filter** column, type an SQL WHERE clause that includes the variable you want to use. For example, to create a view that contains devices with events older than one hour, use the following clause:

```
{%serverTime} - FirstOccurrence > 3600
```

5. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
6. From the **Connectivity** list, select the required connectivity:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

7. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Creating IP filtered views

You can create network views for IP-addressable entities based on IP filter criteria. For example, you can create a network view for all IP-addressable entities that either have a specific IP address or contain a specific fragment of an IP address. You can specify multiple IP filters.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

To create an IP-filtered network view:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `IP Filter`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Background Image

   Click **Browse**  to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. From the **Domain** list, select your network domain.
5. In the **Address Patterns** field, specify an IP address pattern that you want to match.

   An IP filtered network view filters based on the accessible IP address for any IP addressable entity within the selected domain. IP addressable entities include main node devices, such as switches and routers, but also include device components such as interfaces, loopback interfaces, and VLANs. An IP filtered network view therefore does not only filter on main node IP addresses; instead it returns all main nodes that meet the following criteria:

   - Main nodes, where the accessible IP address of the main node matches the range specified in the IP filter. Examples of main nodes returned using this criterion include switches where the IP address of the switch corresponds to the accessible IP address.
   - Main nodes, where at least one interface or other IP addressable component within the main node matches the range specified in the IP filter. Examples of main nodes returned using this criterion include routers where the device typically contains many IP interfaces routing traffic. The management address of the device is often on a separate management network. As the device might be named by its management address this returned address might not match the filter specified; for example, an IP filter view of with a filter criterion such as 1.1.1.* returns a device with the name 2.2.2.2.

   If you want to filter on main node IP addresses only, you can create a filtered network view.

   Tip: You can specify as many IP address patterns as you want. The resulting network view shows the union of all IP address retrieved by the different address patterns.
6. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
7. From the **Connectivity** list, select the required connectivity. The **Connectivity** list displays some of the options listed below:

   Layer 1
   Displays all physical connections.

   Layer 2
   Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

   Layer 3
   Shows routers and the connections between routers. Switches are not normally displayed.

   Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

   The connections between devices are displayed as follows:

   - Connections between two layer 3 interfaces are shown as normal.
   - Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
   - Connections between two layer 2 interfaces are not shown.

   IP subnets
   Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

   - **Layer 1** for transmission layer connections.
   - **Layer 2** for data link connections.

- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

8. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Sample IP address patterns

To match all IP addresses that begin with 192.168, type the address pattern `192.168`.
To match IP addresses that begin with 172.18, 172.19, and 172.20, type the address pattern `172.18-20`.

Related tasks

Example topology filter: main node filter
This example shows you how to create a network view that filters based on main node IP addresses only.

IP filter syntax

Use this reference information to understand how to model the syntax of an IP filter.

When searching for specific IP addresses, you can use ranges for the last octet. You can also assume wildcards for the last octet.

See the following examples to understand the use of ranges and wildcards.

The following examples show different options for using ranges and wildcards to filter for IP addresses:

- `172.18-20` matches any IP address that has 172.18, 172.19, or 172.20 as the first two octets.
- `172.20.36-38` matches any IP address that has 172.20.36, 172.20.37, or 172.20.38 as the first three octets.
- `192.168` matches all IP addresses that have the value of 192.168 as the first two octets.

  Note: When used in the last octet, the asterisk (*) wildcard is optional. For example, entering 192.168 and 192.168.* produce the same results. However, the asterisk can be used to filter within octets, for example 192.0.2.1* only matches addresses that have 192.0.2.1* as their first characters.

Creating standard cross-domain network views

You can create standard network views of different types, that show devices from all discovered domains.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

Before creating a cross-domain network view, you must configure and run cross-domain discoveries for each domain that you want to aggregate.

About this task

To create standard network views across domains, complete the following steps:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select a standard network view type. Because the resulting network view will contain all devices from all discovered networks, consider the size of the network views so as not to create unnecessary load on the server.

   Fill in the other fields as appropriate for that type of network view.
4. Click the **Filter** tab. Complete the tab as follows:

   Domain
   Select the **AGGREGATION** domain.

   Fill in the other fields as appropriate for that type of network view.
5. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Creating dynamic network views

Network Manager has two types of views: standard and dynamic. You can create these dynamic views.

About this task

Certain types of network view can be created based on device events. For example, you can create a dynamic distinct network view that categorizes devices by location, and within each location, categorizes the devices by the event severity on each device.

If the system contains a large number of views, this can adversely affect performance. The administrator can restrict the number of child views that a dynamic view is allowed to contain when a user creates or edits a dynamic view. If the number of child views that a dynamic view would contain is greater than the `topoviz.tree.size.warning` property in topoviz.properties, the GUI displays a warning, but allows the user to proceed. If the number of child views that a dynamic view would contain is greater than the `topoviz.tree.size.limit`property in topoviz.properties, the GUI will not allow the user to proceed. By default, there is no warning and no limit, and so a dynamic view can contain any number of child views.

`topoviz.tree.size.warning` and `topoviz.tree.size.limit` apply only when a user is creating or editing a dynamic view in the GUI. They do not apply to network views created through the auto-provisioning mechanism. Refer to *Creating and deploying network views from templates automatically* in the *IBM Tivoli Network Manager User Guide* for more information about Creating and Deploying Network Views. They also do not apply if the discovery causes new child views to be created under a dynamic view.

Creating dynamic views of device collections

To view and keep track of changes to device collections in your network, create dynamic views of device collections. Use dynamic network views to monitor changes to the network. If the topology has changed after a discovery, the nodes in the **Navigation Panel** are updated automatically.

Before you begin

Use a dynamic network view to monitor which devices have been added to the network, and which devices have been removed. If the topology has changed after a discovery, the nodes in the **Navigation Panel** are updated automatically.

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

You can create the following device collections:

- Border Gateway Protocol (BGP) Autonomous Systems (AS), clusters, and networks
- Data Centers
- Element Management System (EMS) systems
- Generic collections
- Geographic locations
- Geographic regions
- Global Virtual Local Area Networks (VLANs)
- Hot Standby Routing Protocol (HSRP) groups
- Internet Group Membership Protocol (IGMP) groups
- Internet Protocol (IP) paths
- IPM Route Multicast Distribution Trees (MDT)
- ITNM Services
- Logical collections
- LTE pools
- LTE public land mobile networks (PLMNs)
- LTE tracking area collections
- MPLS Traffic Engineered (TE) tunnels
- Open Shortest Path First (OSPF) areas and routing domains
- Port Groups
- Protocol Independent Multicast (PIM) groups
- Radio Access Network (RAN) circuit core, GSM cells, location areas, packet core, routing areas, and UTRAN cells
- Stacks
- Subnets
- Virtual Private Networks (VPNs)
- VLAN Ports
- VLAN Trunking Protocol (VTP) domains
- VTP domains
- WLAN 802.11
- WLAN Channel

- WLAN SSID

The following table describes specific requirements for which a dynamic view of device collections is not suitable. In each case, follow the alternative course of action:

Table 19. Strategies for creating dynamic views of device collections

Requirement	Action
You want a dynamic view of subnets and want to avoid creating large numbers of view of class C subnets.	Create a dynamic view of subnets. Typically, networks contain large numbers of class C subnets, which result in large numbers of views. By creating a dynamic view of subnets, you can restrict the number of views to class A and class B subnets.
You want a dynamic view of MPLS VPNs but want to restrict the views to customer VPNs only, and want the option of showing customer-edge (CE) devices in those views.	Create a dynamic view of MPLS VPNs. For MPLS VPNs, a dynamic view of device collections results in views for both the customer VPNs and the MPLS core network. Additionally, the customer VPNs do not show customer edge (CE) devices.

To create a dynamic view of one or more device collections in your network:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View** .
3. Complete the **General** tab as follows:

Name
Type a name for the network view, dynamic view, or network view container.

Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent
Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

Type
Select `Dynamic Views – Collection`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse** to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse** to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Complete the tab as follows

Domain
Select your network domain.

Type
Select the required device collection. The **Preview** list is automatically populated based on your selection.

Connectivity
Select `Default`. The network view is displayed using the most appropriate connectivity for the type of collection you selected. You also have the option of specifying one of the other following connectivity options:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

SubGraph
If the visualization of logical groups has been enabled by the administrator, this menu is available. Select **Enable** to display entities in logical groups surrounded by a boundary (cloud), which can be expanded and collapsed. Select **Disable** to display entities in logical groups connected to a ring, which cannot be expanded or collapsed.

Subtree Structure
For selected dynamic network view device collections, this option enables you to view the network view as a hierarchical structure. The flag takes one of the following values: **Hierarchical** (present the collections in a hierarchy), or **Flat** (present the collections in a flat list).

Note: The schema allows collections of any type to exist in a hierarchy, but this option is expected to be most useful for geographic location and geographic region collections. Note also that the geographic hierarchy will not appear automatically; the ability to display a geographic hierarchy requires stitcher customization to identify the relevant parts of the postal address where a device is located. You will need to perform this stitcher customization for your deployment, or possibly for each country that you display in the network views.

5. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Related tasks

Creating dynamic views of subnets
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

Creating dynamic views of MPLS VPNs
To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

Creating dynamic views of subnets

To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

Typically, networks contain large numbers of class C subnets, which result in large numbers of views. By creating a dynamic view of subnets, you can restrict the number of views to class A and class B subnets.

Tip: If you want to create network views that contain more than one subnet, then do not create a dynamic view. Instead, create a *standard network view* for device collections.

To create a dynamic view of the subnets in your network:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not

supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent
Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

Type
Select `Dynamic Views – Subnet`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Select your network domain from the **Domain** list.
5. Select the required option from the **Subnet** list:

Option	Description
A & B	Creates network views for each of the class A and class B subnets in your network
A, B & C	Creates network views for each of the class A , class B, and class C subnets in your network. Typically, this option automatically creates a large number of subnet network views because most networks contain many class C subnets.

The **Preview** list is automatically populated based on your selection.

6. Click **OK**.

The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

What to do next

Related tasks

Creating dynamic views of subnets
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

Creating dynamic views of MPLS VPNs
To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

Creating dynamic views of device collections

To view and keep track of changes to device collections in your network, create dynamic views of device collections. Use dynamic network views to monitor changes to the network. If the topology has changed after a discovery, the nodes in the **Navigation Panel** are updated automatically.

Creating network views of device collections
To monitor collections of devices, such as subnets, VPNs, and MPLS VPNs, in a part of a large network, create a standard network view of a device collection. Standard views of device collections are changed automatically as the topology changes after a discovery.

Creating dynamic views of MPLS VPNs

To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

About this task

Restriction: The dynamic view of MPLS VPNs does not create a network view for the MPLS core network. To create a view for the core network, create a dynamic view of device collections.

Tip: If you want to create a view that contains more than one customer VPN, do not create a dynamic view. Instead, create a network view of MPLS VLANs.

To create a dynamic view of the customer VPNs in your network:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Dynamic Views – MPLS – VPN`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. Complete the tab as follows:

Domain
Select your network domain.

CE Devices
Select `Hide` or Show. The **Preview** list is automatically populated based on your selection.

5. Click **OK**.

The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

What to do next

Related tasks

Creating dynamic views of device collections
To view and keep track of changes to device collections in your network, create dynamic views of device collections. Use dynamic network views to monitor changes to the network. If the topology has changed after a discovery, the nodes in the **Navigation Panel** are updated automatically.

Creating network views of device collections
To monitor collections of devices, such as subnets, VPNs, and MPLS VPNs, in a part of a large network, create a standard network view of a device collection. Standard views of device collections are changed automatically as the topology changes after a discovery.

Creating dynamic views of subnets
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

Creating distinct dynamic views

To create a network view that has custom categories and subcategories, create a *distinct dynamic view*.

About this task

For example, you can use the distinct dynamic view to categorize devices by location and within each location organize by the network administrator who is responsible for maintaining the devices. For example, you can use this option to categorize devices by location, and within each location, list the different device classes, such as Cisco 2600 devices or 3ComSuperStack devices.

To create an IP-filtered network view:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

Name
Type a name for the network view, dynamic view, or network view container.

Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent
Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

Type
Select `Dynamic Views – Distinct`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

Background Image

Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. Click the **Filter** tab. From the **Domain** list, select your network domain.
5. In the **Fields** list, select the topology database tables and fields that correspond to the categories and subcategories that you want to define. Make sure you define the categories and subcategories in the correct order.
   a) Click **Add...**.
   b) From the **Table** list, select the required database table.
   The **Field** list is automatically populated based on your selection.
   c) Select the required field from the **Field** list.
   d) Repeat steps "5.a" on page 182 to "5.c" on page 182.

   See "Sample topology database fields for categories" on page 184 for more information on how to specify the fields.

   As you select fields, the **Preview** list is updated to show the relationships between the categories that you selected.
6. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
7. From the **Connectivity** list, select the required connectivity:

   Layer 1
   Displays all physical connections.

   Layer 2
   Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

8. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Sample topology database fields for categories

The following example helps you complete the fields in step "5" on page 182.

To categorize devices by location, and within each location categorize by the responsible network administrator, define the following categories, in the following order:

1. Location of the device: This data is held in the sysLocation field of the chassis database table.
2. Contact person associated with the device: This data is held in the sysContact field of the chassis database table.

This order ensures that location is the main category and contact person is the subcategory.

Creating template-based dynamic views

Use a template-based dynamic view to generate a pre-configured set of dynamic views that are predefined by the network administrator.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

The required templates must have been defined and stored in the `$NMGUI_HOME/profile/etc/tnm/dynamictemplates/` directory. If a template is not stored in this directory, it cannot be selected for generating dynamic views.

About this task

A template is a set of preconfigured views that are defined in an XML file. The network administrator can preconfigure different sets of views for different network operators by defining these preconfigured views in separate templates. The network operators select the template that is relevant to them and generate the views.

To create a template-based dynamic view:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. Click the **Libraries** tab and click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select `NONE`.

   Type
   Select `Dynamic Views - Template`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Tree Icon

   If you want a different icon than the default icon to represent the view, click **Browse**  to browse for an icon.

   Background Image

   Click **Browse**  to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated **Event Viewer** event with the highest severity, and can appear with an additional severity icon.
4. Click the **Filter** tab. From the **Domain** list, select your network domain.
5. From **Template**, select the template that want to use to generate the dynamic view.
   The **Preview** list is automatically populated with the list of network views based on your selection.
6. Click **OK**.
   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Creating dynamic cross-domain network views

You can create dynamic network views of different types, that show devices from all discovered domains.

Before you begin

If you want to store the view in a custom container, you must create the container before you begin this task.

Before creating a cross-domain network view, you must configure and run cross-domain discoveries for each domain that you want to aggregate.

About this task

To create dynamic network views across domains, complete the following steps:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Click **New View**  .
3. Complete the **General** tab as follows:

   Name
   Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select NONE.

   Type
   Select a dynamic network view type. Because the resulting network view will contain all devices from all discovered networks, consider the size of the network views so as not to create unnecessary load on the server.

   Fill in the other fields as appropriate for that type of network view.
4. Click the **Filter** tab. Complete the tab as follows:

   Domain
   Select the **AGGREGATION** domain.

   Fill in the other fields as appropriate for that type of network view.
5. Click **OK**.

   The new view is added to the navigation tree in the **Navigation Panel**. If you added the view to a container, expand the container node to see the new view in the tree.

Example: Small network or Proof of Concept (POC)

If you want to check whether two or more domains have been discovered and joined together as you expect, you could recreate all the network views that are usually created automatically after a discovery finishes. Do this only if you are sure that the total of the resulting network views will not have an adverse performance impact. For example, you might want to do this while testing cross-domain discovery, on a non-production system. To create all the usual network views, complete the following steps:

1. Create a new network view of type **Dynamic Views - Template**.
2. Select the domain **AGGREGATION**.
3. Select the template **IP Default**.

Changing network views

You can change any of the properties of an existing view.

About this task

To edit a view, complete the following steps:

Procedure

1. In the navigation panel, navigate to the view you want to edit and click the**Edit view**  button.
   A dialog box is displayed.
2. Edit the properties of the view. When you have finished, click **OK** to apply your changes.
3. Click **Save**  .

Deleting network views

Delete existing network views if they are no longer required.

About this task

To delete an existing view:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. Navigate to the required network view and select the view. Then click **Delete View**  .
   The **Delete View** dialog is displayed.
3. Select one of the following options:

Option	Description
Delete view and all its sub-views	Deletes both the selected view and any subviews that it might have.
Delete view and move sub-views to new parent	Deletes only the selected view and moves any sub-views to the node that you select from the list. To move the subviews to the top level of the hierarchy, select NONE.

4. Click **Delete** > **OK**.

Copying or moving views

Move network views if you want to make private views available on a group-wide or global basis. Copy network views into your private collection if you want to change a group or global view without any impact on the original view.

Before you begin

To copy or move views to a container, you must be a member of that contain, or you must have administration rights for the container.

To move a view, you must have the appropriate administration rights. If you do not have the administration rights to move a view, you can only copy a view. For many of these operations you must have read-write access.

About this task

For the available options when copying or moving views, see "Possible copy and move actions" on page 188.

To copy or move a view:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. Navigate to the required view, select the view, and click **Copy or Move View**  .
3. Under **Action**, select an option:
   - **Copy**: Creates a copy of the view in the selected target.
   - **Move**: Moves the view to the selected target.
4. Complete the other fields as follows:

   To
   Select the view collection to which you want to copy or move the view.

   Parent
   Select the node under which the view appears in the hierarchy in the **Navigation Tree**. To display the view on the top level, select NONE.
5. Click **OK**.

Possible copy and move actions

The following table describes the copy and move operations that you can perform, and shows source and target view collections for these copy and move operations.

Table 20. Copying and Moving Network Views between Network View Collections

Source	Target	Result
Own user view collection	Within same user view collection	Places the network view in a required position within the user view collection
Own user view collection	Group view collection	Makes a private network view available on a group-wide basis
Own user view collection	Global view collection	Makes a private network view available on a global basis
Group view collection	Own user view collection	Enables you to copy a group view into your own user view collection and modify the view there
Group view collection	Within same group view collection	Places the network view in a required position within the group view collection
Group view collection	Another group view collection	Enables sharing of network views between groups
Group view collection	Global view collection	Makes a network view formerly available only to users within a single group available on a global basis
Global view collection	Own user view collection	Enables you to copy a global view into your own user view collection and modify the view there

Table 20. Copying and Moving Network Views between Network View Collections (continued)		
Source	**Target**	**Result**
Global view collection	Group view collection	Enables you to copy a global view into a group view collection where group members can display the view and modify it if they have read-write access
Global view collection	Another point within the Global view collection	Places the network view in a required position within the global view collection

Related reference

Access configuration for network view collections
Use groups and role assignments to administer read-write and read-only access to network view collections, and administer privileges to copy and move network views between network view collections.

Roles required to copy and move network views

To enable users to copy and move network views between network view collections you must assign the users to certain roles and groups.

The ability to copy and move network views between view collections varies depending on which roles are assigned to a user and which group or groups of which the user is a member.

The following table describes that you must assign to users so that they can copy and move views.

Table 21. Roles for copying and moving network views between network view collections				
Operation	**From**	**To**	**Roles required**	**Group membership required**
Copy or move	Own user view collection	Within same user view collection	ncp_networkview ncp_networkview_admin_user netcool_rw	None
Copy	Own user view collection	Group view collection	ncp_networkview ncp_networkview_admin_group netcool_rw	Must be member of the target group
Move view collection	Own user view collection	Group view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_group netcool_rw	Must be member of the target group
Copy	Own user view collection	Global view collection	ncp_networkview ncp_networkview_admin_global netcool_rw	None

Table 21. Roles for copying and moving network views between network view collections (continued)

Operation	From	To	Roles required	Group membership required
Move	Own user view collection	Global view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_global netcool_rw	None
Copy	Group view collection	Own user view collection	ncp_networkview ncp_networkview_admin_user netcool_rw	Must be member of the source group
Move	Group view collection	Group view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_group netcool_rw	Must be member of the source group
Copy or move	Group view collection	Within same group view collection or to another group view collection	ncp_networkview ncp_networkview_admin_group netcool_rw	Must be member of the source and target groups
Copy	Group view collection	Global view collection	ncp_networkview ncp_networkview_admin_global netcool_rw	Must be member of the source group
Move	Group view collection	Global view collection	ncp_networkview ncp_networkview_admin_global ncp_networkview_admin_group netcool_rw	Must be member of the source group
Copy	Global view collection	Own user view collection	ncp_networkview ncp_networkview_admin_user netcool_rw	None
Move	Global view collection	Own user view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_global netcool_rw	None

Table 21. Roles for copying and moving network views between network view collections (continued)				
Operation	**From**	**To**	**Roles required**	**Group membership required**
Copy or move	Global view collection	Another point within the Global view collection	ncp_networkview ncp_networkview_admin_global netcool_rw	None
Copy	Global view collection	Group view collection	ncp_networkview ncp_networkview_admin_group netcool_rw	Must be member of the target group
Move	Global view collection	Group view collection	ncp_networkview ncp_networkview_admin_global ncp_networkview_admin_group netcool_rw	Must be member of the target group

Deploying pre-configured network views

To configure network views for use by network operators, create a template that specifies pre-configured network views. The template can be deployed either by the operators, or globally for specific sets of operators.

About this task

The network views in the template can be created in two ways:

- Network operators generate the network views from the **Network Views** GUI by create a new template-based dynamic network view and specifying the template.
- You generate the network views specified in the template and assign the generated views to a specific user or group.

Results

Making a pre-configured template available to operators

Provide a template of pre-configured network views to network operators so that they can use the template to generate dynamic network views from the **Network Views** GUI themselves.

About this task

To provide the template:

Procedure

1. Define the template in an XML file.

   Give the XML file the following name:

   template_name`.xml` , where *template_name* is the name of the template on which network operators base their dynamic network views.
2. Save the template to the `/opt/ibm/netcool/gui/precision_gui/profile/etc/tnm/dynamictemplates` directory.

Related concepts

About network view templates
A network view template is a set of preconfigured network views that is defined in an XML file. Network administrators use templates to automatically generate network views.

Creating and deploying network views from templates automatically

Create network views from templates and assign them to groups or users automatically using auto-provision scripts.

About this task

To deploy the templates, you must create an auto-provision script. This script performs the following tasks:

- Creates a top-level dynamic view node in the Network Views Navigation Panel, using a specified name
- Generates a set of network views using a specified template, and puts the template in the top-level dynamic view node in the **Navigation Panel**
- Assigns the network views generated to a specified user or user group.
- Uses a specified domain.

Every 60 seconds the `$NMGUI_HOME/profile/etc/tnm/autoprovision/` directory is monitored for new auto-provision scripts. When a new auto-provision script is found, the script is read and processed, and the dynamic network view referenced in the script is created and assigned to the specified user or user groups.

When a script is processed, the suffix `.processed` is added to the file name, whether or not any network views were created. Files which end in `.processed` are not processed again. If you want to rerun a script, remove the `.processed` from the end of the file name, so that the file name ends in `.xml`.

Note: Auto-provisioned network views are created only when the `tnm.database.createDefaultNetworkView` parameter in `tnm.properties` is set to `true`. By default, this parameter is set to false. The default setting can be overridden during installation by selecting the `Create default Network Views` in selected database check box in Topology Database panel.

To deploy preconfigured network views automatically:

Procedure

1. Define the template as an XML file and save the template to the `$NMGUI_HOME/profile/etc/tnm/dynamictemplates/` directory.
2. Create the auto-provision script in XML and copy it into the `$NMGUI_HOME/profile/etc/tnm/autoprovision/` directory.
   See "Sample auto-provision script" on page 193 for an example.

   The script is automatically processed within 60 seconds and the specified network views are created in the specified domain for the specified users and groups.
3. If a network topology exists for the specified domain, the new network views are automatically populated with devices. If no discovery has been run, the network views are populated when a discovery has been run in the appropriate domain.

   Restriction: If the domain referenced in the auto-provision script does not exist at the time that the script is processed, no network views are created. You need to first create the domain, and then create the network views. This is true even if you create a script that references all domains using a wildcard "*".

Sample auto-provision script

The following sample auto-provision script creates a view called `NCOMS View` and creates a set of views underneath using the dynamic view template `ipdefault`. These views are assigned to the `itnmadmin` user and use the domain `NCOMS`.

```
<autoProvision name="NCOMS View" domain="NCOMS" accessLevel="user"
accessId="itnmadmin">
        <dynamicViewTemplate id="ipdefault" />
</autoProvision>
```

Network view templates

Read about network view templates and use this reference information to create new network view templates for Network Manager.

About network view templates

A network view template is a set of preconfigured network views that is defined in an XML file. Network administrators use templates to automatically generate network views.

The XML files that are used to define the templates are stored in the `$NMGUI_HOME/profile/etc/tnm/dynamictemplates/` directory.

Network administrators create templates based on the needs of network operators. The templates can be made available to operators in the following ways:

By saving the templates to a specified location
The operator can then choose to generate the preconfigured set of network views from the **Network Views** GUI, as one of the options available when creating a network view.

By assigning the templates to specified users or user groups
The administrator deploys the preconfigured views defined in one or more templates and assigns these views to a specific user, group or at a global level. Depending on how the templates have been assigned, operators find the preconfigured views automatically available in their **Network Views Navigation Panel**.

Related tasks

Creating template-based dynamic views
Use a template-based dynamic view to generate a pre-configured set of dynamic views that are predefined by the network administrator.

Making a pre-configured template available to operators
Provide a template of pre-configured network views to network operators so that they can use the template to generate dynamic network views from the **Network Views** GUI themselves.

Creating and deploying network views from templates automatically
Create network views from templates and assign them to groups or users automatically using auto-provision scripts.

Related reference

Description of IP network view template

The IP network view template `ip_default.xml` defines dynamic network views for a wide range of IP network classes and collections.

Default network view templates

Network Manager is shipped with templates containing dynamic views for each item available on the network.

IP network view template

Network Manager is shipped with the IP network view template, `ip_default.xml`. This template consists of dynamic network views for each item available on the IP network.

Description of IP network view template

The IP network view template `ip_default.xml` defines dynamic network views for a wide range of IP network classes and collections.

Warning: Do not use the `ip_default.xml` template if you have large or very large networks. The `ip_default.xml` template is intended mainly for educational purposes to demonstrate how the topology can be displayed. Running this template against a large or very large production topology could have a serious impact on the memory and performance of your Network Manager installation, particularly on displaying and using network views. If you have large or very large networks, create network view templates that enable operators to generate a limited set of network views or create network views manually. For more information on creating network views and network view templates, see the *IBM Tivoli Network Manager User Guide*. For more information about network sizes, see the section on deployment scenarios in the *IBM Tivoli Network Manager User Guide*.

Dynamic views are created for the following items:

- Alert views. The following alert views are presented:
  - All devices with PingFailRootCause events
  - All devices with SnmpLinkInDiscards events
  - Alert views based on event severities
  - Monitoring views: network views resulting from Network Manager polling and used by the adaptive polling scenarios
- ASMs running on devices. An ASM agent running on a device corresponds to a commercial server or database product running on that device. These network views group devices within a network based on the commercial server or database products running on those devices.
- BGP networks
- Customer MPLS VPNs
- Device classes
- HSRP groups
- IGMP
- IPMROUTE
- NAT address spaces
- OSPF routing domains
- Subnets
- VLANs
- VPLS
- VTP domains

No dynamic view is created for an item if no item of that type exists on the network. For example, if your network has no HSRP groups, then no dynamic view is generated for HSRP groups.

IP network view template XML code

This template example uses all of the elements available from the IP template hierarchy. It includes network views based on user-defined filters and dynamic views.

Example

The following sample template XML file is provided for illustration purposes and uses all of the elements available from the template hierarchy.

```
<dynamicViewTemplate id="complete_template" label="Complete Template" manager="PrecisionIP">

<!--  "Classic" Class Partition -->

<!-- VPLS -->
<container id="vpls" label="VPLS">
    <dynamicMplsVpn id="vpls_vpns" label="VPLS VPNs" ceDevices="true"/>
</container>

<!-- IP Multicast Routing View -->
    <dynamicCollection id="ipMRoutingMdts" label="Multicast Routing MDTs" entityType="46" connectivity=”ipMRoute”/>

<!-- IGMP View -->
    <dynamicCollection id="igmpGroups" label="IGMP Groups" entityType="121"/>

<dynamicDistinct id="device_classes" label="Device Classes" connectivity="ipsubnets" endNodes="false">
        <tableField table="chassis" field="className" />
    </dynamicDistinct>

<!--  BGP Networks -->
    <collection id="bgp_networks" label="BGP Networks" entityType="30">
        <entity name="BGP Networks" />
    </collection>

<!-- PIM Network -->
    <collection id="pim_network" label="PIM Network" entityType="42">
        <entity name="PIM Network"/>
    </collection>

<!-- Unassigned view-->
    <unassigned id="unassigned_view" label="Unassigned_View" />

<!-- Custom view (previously known as a manual view)-->
    <custom id="custom_view" label="Custom_View" connectivity="ipsubnets"/>

<!--  VLAN Port Collections -->
    <dynamicCollection id="vlan_port_collection" label="Vlan Ports" entityType="113" connectivity="layer2" />

<!--  HSRP Groups -->
    <dynamicCollection id="hsrp_groups" label="HSRP Groups" entityType="18" />

<!--  OSPF Routing Domains -->
    <dynamicCollection id="ospf_routing_domains" label="OSPF Routing Domains" entityType="21" />

<!--  VTP Domains -->
    <dynamicCollection id="vtp_domains" label="VTP Domains" entityType="24" />

<!--  Subnets -->
    <dynamicSubnet id="subnets" label="Subnets" classes="ab" />

<!--  MPLS -->
    <container label="mpls" label="MPLS">
        <collection id="mpls_core" label="MPLS Core" entityType="17">
            <entity name="VPN_CONTAINER_MPLS Core" />
        </collection>
        <dynamicMplsVpn id="mpls_vpns" label="MPLS VPNs" ceDevices="false" />
    </container>

<!-- MPLS TE -->
    <dynamicCollection id="mpls_te" label="MPLS TE" entityType="36"/>

<!-- Static MPLS -->
    <mplsVpn id="mpls_vpn" label="Static MPLS VPN" ceDevices="true">
        <entity name="VPN_CONTAINER_1104"/>
    </mplsVpn>

<!--  NAT Address Spaces -->
    <dynamicDistinct id="nat_address_spaces" label="NAT Address Spaces" connectivity="ipsubnets" endNodes="false">
        <tableField table="ipEndPoint" field="addressSpace" />
    </dynamicDistinct>

<!--  Discovered ASMs -->
    <dynamicDistinct id="discovered_asms" label="Discovered ASMs" connectivity="ipsubnets" endNodes="false">
       <tableField table="netcoolAsmsRunning" field="ASMName" />
    </dynamicDistinct>

<!-- Wildcard IP Filter -->
    <ipFilter id="ipfilter1" label="Filtered IPs 1" endNodes="true">
       <addressPattern pattern="192.*.*.*"/>
    </ipFilter>

<!-- Ranged IP Filter -->
    <ipFilter id="ipfilter2" label="Filtered IPs 2">
      <addressPattern pattern="192.168.3-4"/>
    </ipFilter>

<!-- Filtered for two class names -->
    <filtered id="filtered1" label="Network Devices/Linux Machines" endnodes="true" condition="or">
      <filter table="chassis" filter="className = 'NetworkDevice'"/>
      <filter table="chassis" filter="className = 'Linux'"/>
    </filtered>
```

```
<!-- Filtered for particular network devices -->
    <filtered id="filtered2" label="Network Devices: Main Node < 2000" endnodes="true" condition="and">
      <filter table="chassis" filter="className = 'NetworkDevice'"/>
      <filter table="chassis" filter="mainNodeEntityId < 2000"/>
    </filtered>

<!-- Devices that have been manually added with the topology editor -->
<!-- connectivity defaults to IP subnets -->
  <filtered id="ManuallyAdded" label="Manually Added Devices" endNodes="true">
    <filter schema="ncim" table="entity" filter="manual = 1" />
  </filtered>

<!-- All routers -->
  <filtered id="AllRouters" label="All Routers" connectivity="layer3">
    <filter schema="ncim" table="classMembers" filter="classId in (select classId from {%schema_ncim}entityClass where
classType='Router')" />
  </filtered>

<!-- All switches -->
<filtered id="AllSwitches" label="All Switches" connectivity="layer2">
  <filter schema="ncim" table="classMembers" filter="classId in (select classId from {%schema_ncim}entityClass where
classType='Switch')" />
  </filtered>

<!-- default event filtered type views based on severities -->
    <container id="alert_views" label="Alert views">

        <container id="acknowledged_alerts"  label="Acknowledged Alerts">
            <filtered id="Critical" label="Critical" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=5 and Acknowledged=1"/>
            </filtered>

            <filtered id="Major" label="Major" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=4 and Acknowledged=1"/>
            </filtered>

            <filtered id="Minor" label="Minor" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=3 and Acknowledged=1"/>
            </filtered>
        </container>

        <container id="Unacknowledged_alerts"  label="Unacknowledged Alerts">
            <filtered id="Critical" label="Critical" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=5 and Acknowledged=0"/>
            </filtered>

            <filtered id="Major" label="Major" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=4 and Acknowledged=0"/>
            </filtered>

            <filtered id="Minor" label="Minor" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=3 and Acknowledged=0"/>
            </filtered>
        </container>

<!-- Filter using the current time as a variable -->
  <filtered id="OldCriticalPingFail" label="Critical Ping Fail Events at least 1 hour old" connectivity="ipsubnets" endNodes="true">
    <filter schema="ncmonitor" table="activeEvent" filter="EventId = 'NmosPingFail' and Severity=5 and {%serverTime} - FirstOccurrence
&gt;= 3600"/>
  </filtered>

<!-- default event filtered type view -->
    <filtered id="ping_fail_root_cause" label="PingFailRootCause" connectivity="ipsubnets" endNodes="true">
        <filter schema="ncmonitor" table="activeEvent" filter="EventId='NmosPingFail' and NmosCauseType='Root Cause'"/>
    </filtered>
<filtered id="snmppollfail" label="SNMP Poll Fail" connectivity="ipsubnets" endNodes="true">
  <filter schema="ncmonitor" table="activeEvent" filter="EventId='NmosSnmpPollFail'" />
  </filtered>

<!-- default event filtered type view -->
    <filtered id="SnmpLinkInDiscards" label="SnmpLinkInDiscards" connectivity="ipsubnets" endNodes="true">
        <filter schema="ncmonitor" table="activeEvent" filter="EventId='NmosSnmpLinkInDiscards'"/>
    </filtered>

<!-- Monitoring views -->
        <container id="Monitoring_views"  label="Monitoring Views">

            <filtered id="InitialPingFail" label="Initial Ping Fail Events" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="EventId = 'NmosPingFail' and Tally <= 18"/>
            </filtered>

            <filtered id="HighDiscardRate" label="Devices that have at least one interface event for HighDiscardRate"
connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="EventId = 'Poll-HighDiscardRate'"/>
            </filtered>
        </container>

    </container>

</dynamicViewTemplate>
```

LTE network view template

Network Manager is shipped with the LTE network view template, `lte_default.xml`. This template consists of dynamic network views for each item available on the LTE network.

Description of LTE network view template

The LTE network view template `lte_default.xml` defines dynamic network views for a wide range of LTE network classes and collections.

Views are created for the following items:

- Control Plane by Tracking Area: Lists network views containing sections of the control plane associated with a given tracking area. Each of these network views is given the name of the associated tracking area.
- EPC network: Lists all devices in the evolved packet core (EPC) network.
- EPC Control Plane: Provides a fully connected network view showing all control plane devices in the Evolved Packet Core section of the LTE network.
- EPC by Vendor: Lists all vendors for devices in the evolved packet core (EPC) network. Clicking a vendor name lists the devices of that vendor type in the EPC.
- EPC User Plane: Provides a fully connected network view showing all user plane devices in the Evolved Packet Core section of the LTE network.
- E-UTRAN network: Lists all eNodeB devices in the evolved UMTS Terrestrial Radio Access network (EUTRAN).
- E-UTRAN by Vendor: Lists all vendors for the eNodeB devices in the evolved UMTS Terrestrial Radio Access network (EUTRAN). Clicking a vendor name lists the eNodeB devices of that vendor type in the EUTRAN
- LTE Network Geography: Shows devices in the LTE hierarchy grouped geographically. The geographical groupings vary depending on how the geographical locations and regions are defined in your system.
- LTE Pools: Shows all pools in the LTE hierarchy. If you have no LTE pools then this node does not appear. Because the LTE Pools view is a dynamic distinct view, it will contain child views for whatever types of LTE pools exist in the NCIM topology database; for example, MME pools, PGW pools, SGW pools.
- PLMN: Lists all public land mobile networks (PLMN) in the LTE hierarchy.
- Tracking Areas: Lists all tracking areas in the LTE hierarchy.
- User Plane by Tracking Area: Lists network views containing sections of the user plane associated with a given tracking area. Each of these network views is given the name of the associated tracking area.
- Vendor: Lists all vendors in the LTE hierarchy. Clicking a vendor name lists network views corresponding to the device types from that vendor in the LTE hierarchy.

No dynamic view is created for an item if no item of that type exists on the network. For example, if your network has no LTE pools, then no dynamic view is generated for LTE pools.

LTE network view template XML code

This template example uses all of the elements available from the LTE template hierarchy. It includes network views based on user-defined filters and dynamic views.

Example

The following sample template XML file is provided for illustration purposes and uses all of the elements available from the template hierarchy.

```
<dynamicViewTemplate id="lte_default" label="LTE Default" manager="PrecisionIP" >

    <container id="lte_network_drilldown" label = "LTE Network Drilldown" layout="tabular">
        <filtered id="eutran" label="E-UTRAN" endNodes="true" connectivity="noconnections">
                <filter schema="ncim" table="entityClass" filter="classType = 'ENODEB'"/>
        </filtered>

        <dynamicDistinct id="eutranByVendor" label="E-UTRAN by Vendor" endNodes="true"
connectivity="noconnections">
```

```
           <tableField table="enbFunction" field="vendorName"/>
        </dynamicDistinct>

        <filtered id="epc" label="EPC" condition="OR" endNodes="true" connectivity="noconnections">
                <filter schema="ncim" table="entityClass" filter="classType = 'EIR'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'MME'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'HSS'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'PCRF'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'PGW'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'SGW'"/>
        </filtered>

        <dynamicDistinct id="epcByVendor" label="EPC by Vendor" endNodes="true"
connectivity="noconnections">
           <tableField table="epcLteFunction" field="vendorName"/>
        </dynamicDistinct>

        <dynamicCollection id="plmn" label="PLMN" entityType="158" useCollectionHierarchy="true"
connectivity="noconnections"/>

        <dynamicCollection id="tracking_areas" label="Tracking Areas" entityType="153"
useCollectionHierarchy="false"
endNodes="true" connectivity="noconnections"/>

        <dynamicDistinct id="vendor" label="Vendor" endNodes="true" connectivity="noconnections">
           <tableField table="lteFunction" field="vendorName"/>
           <tableField table="lteFunction" field="lteFunctionType"/>
        </dynamicDistinct>
    </container>

    <dynamicCollection id="lte_network_geography" label="LTE Network Geography" entityType="112"
connectivity="lteuserplane"
useCollectionHierarchy="true" subgraph="true" endNodes="true" />
    <!-- entityType 112 is Geographic Region -->

    <container id="lte_network_topology" label = "LTE Network Topology">
        <dynamicCollection id="controlplane" label="Control Plane by Tracking Area" entityType="163"
connectivity="ltecontrolplane" useCollectionHierarchy="true" subgraph="true" endNodes="true"/>
        <dynamicCollection id="userplane" label="User Plane by Tracking Area" entityType="164"
connectivity="lteuserplane"
useCollectionHierarchy="true" subgraph="true" endNodes="true"/>
        <filtered id="epc_control_plane" label="EPC Control Plane" connectivity="ltecontrolplane"
condition="OR"
endNodes="true">
                <filter schema="ncim" table="entityClass" filter="classType = 'EIR'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'MME'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'HSS'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'PCRF'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'PGW'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'SGW'"/>
        </filtered>
        <filtered id="epc_user_plane" label="EPC User Plane" connectivity="lteuserplane" condition="OR"
endNodes="true">
                <filter schema="ncim" table="entityClass" filter="classType = 'PGW'"/>
                <filter schema="ncim" table="entityClass" filter="classType = 'SGW'"/>
        </filtered>

    </container>

     <dynamicDistinct id="lte_pools" label="LTE Pools" connectivity="ltecontrolplane" endNodes="true">
        <tableField table="ltePoolDevices" field="ltePoolType"/>
        <tableField table="ltePoolDevices" field="ltePoolName"/>
     </dynamicDistinct>

</dynamicViewTemplate>
```

Network view template elements

Use this information to understand the elements that are used to create an XML template for a network view.

The following table describes the elements that are used to create a template.

Note: Each element can take the attributes `id` and `label`, in addition to the attributes listed in the table.

Table 22. Elements in the template XML		
Element	**Description**	**Attributes**
addressPattern	Specifies an address pattern to filter device IP addresses.	pattern
collection	Generates a network view of a device collection.	entityType subgraph
container	Generates a container to group network views. Containers can also group other containers.	
dynamicCollection	Generates a dynamic view of a device collection.	entityType connectivity subgraph
dynamicDistinct	Generates a distinct dynamic view.	connectivity endNodes
dynamicMplsVpn	Generates a dynamic view of MPLS VPNs.	ceDevices
dynamicSubnet	Generates a subnet dynamic view.	classes
dynamicViewTemplate	Defines a template.	manager
entity	Specifies a device collection to display in the network view.	name
filter	Specifies a custom filter on the chosen table and fields within it. The filter is performed on an inner join between the "entity" table and the specified table.	schema table filter
filtered	Generates a network view of a device collection, filtered based on other tables and fields.	endNodes connectivity condition
ipFilter	Generates a network view of a device collection, filtered by the IP address of each. A device must pass at least one child addressPattern filter to be shown.	endNodes connectivity
manual	Generates an empty manual view.	
mplsVpn	Generates a network view of MPLS VPNs.	ceDevices
tableField	Specifies a topology database table and field to use as a category.	table field
unassigned	Generates an empty unassigned view.	

Network view template attributes

Use this information to understand the attributes that are used to create an XML template for a network view.

The following table describes the attributes that are used to create a template.

Note: Attribute values must be enclosed within quotation marks; for example, `id="device_classes"`.

Table 23. Attributes in the template XML

Element	Description
ceDevices	Specifies whether to display customer-edge (CE) routers in a dynamic view of MPLS VPNs. Options are the following: • `false`: do not display CE routers • `true`: display CE routers
classes	Specifies which types of subnets to display in a subnet dynamic view. Options are the following: • `ab`: class A and B subnets • `abc`: class A, B, and C subnets
condition	The operator to combine multiple filters. Options are the following: • and • or The default option is the "and" operator.
connectivity	Specifies the type of connectivity to use to display the network views. Options include: • `ipmroute` • `ipsubnets` • `layer1` • `layer2` • `layer3` • `ltecontrolplane` • `lteuserplane` • `noconnections` • `ospf` • `pim` **Note:** If you do not want to see connections between devices, then the option is `connectivity="noconnections"`. However, in this case a tabular view showing the devices in a list might be a better choice than one of the graphical views. You can specify a tabular layout using the layout attribute, described further down in this table.
endNodes	Boolean flag that specifies whether to display end nodes, such as workstations and printers, in the network view. Options are as follows: • false: do not display end nodes (default) • true: display end nodes

Table 23. Attributes in the template XML (continued)

Element	Description
entityType	Specifies the type of the device collection to display. For example, to display VLANs, set this attribute to 16, which is the entityType field value for VLANs in the topology database.
field	Specifies a topology database field to use in a distinct dynamic view.
filter	SQL filter to use. Any strings within the SQL filter must be coded within single quotation marks. It is necessary to use XML escape sequences for certain symbols. Examples of filters are: • "className = 'NetworkDevice'" • "mainNodeEntityId > 2000" **Note:** If filtering using entityId, you must specify the corresponding table attribute as entity. The filter string can use variables in the form `{%variable}`. For example, the following filter shows events that are older than an hour: `<filter schema="ncmonitor" table="activeEvent" filter="{%serverTime} - FirstOccurrence &gt; 3600">`. In Network Manager 3.9, the only supported variable is `{%serverTime}`.
id	Contains a template identifier. If you deploy pre-configured views automatically using a template, use the id identifier to use in the auto-provision script in the dynamicViewTemplate attribute.
label	Contains the label used to identify a template in the Network Views GUI. The operator sees this label in the New View dialog box when the operator creates a template-based dynamic view.
layout	Specifies the layout to use to display the network views: Options are as follows: • circular • grid • hierarchical • orthogonal • symmetric • tabular
manager	Contains the name of the network management system that manages the devices to be visualized in the generated network views; for example, `PrecisionIP` for Network Manager.

Table 23. Attributes in the template XML (continued)

Element	Description
mapIcon	Used to represent views in the **Topology Display Panel**. The default map icon takes the form of a cloud. This attribute takes the following form: `mapIcon="icon.svg"` Where *icon* is the name of the icon to use to represent the view in the **Topology Display Panel**. **Note:** You can specify as a map icon any of the .svg icons in the directory `$NMGUI_HOME/profile/etc/tnm/resource/`. You only need to specify the filename of the icon , as this filename is automatically appended to the directory path.
name	Contains the name of the device collection to display. You can also use this attribute to specify the name of a container node and of dynamic views.
pattern	Specifies a filter pattern for IP addresses; for example, 192.*.*.8, or 192.168.3–4.
subgraph	Provides the option, within the network view, to display entities in logical groups surrounded by a boundary (cloud), which can be expanded and collapsed. This attribute can take the following values: • `subgraph = "false"`: enable display of entities in logical groups surrounded by a boundary (cloud). • `subgraph = "true"`: enable display of entities in logical groups connected to a ring, which cannot be expanded or collapsed.
schema	Specifies a database schema within the NCIM database. By default the value of the schema attribute is set to `ncim`. You do not need to specify the schema attribute if you want to reference a table in the `ncim` schema. However, if you want to reference a table in a different schema, then you must set the value of the schema attribute. For example, to reference the activeEvent table in the `ncmonitor` schema, set `schema = ncmonitor`.
table	Specifies a topology database table to use in a distinct dynamic view.

Table 23. Attributes in the template XML (continued)	
Element	**Description**
treeIcon	Used to represent views in the **Navigation Panel**. The default tree icon takes the form of a cloud. This attribute takes the following form: `treeIcon="icon.png"` Where *icon* is the name of the icon to use to represent the view in the **Navigation Panel**. **Note:** You can specify as a tree icon any of the .png icons in the directory `$NMGUI_HOME/profile/etc/tnm/resource/`. You only need to specify the filename of the icon , as this filename is automatically appended to the directory path.
useCollectionHierarchy	For selected dynamic network view device collections, this option enables you to view the network view as a hierarchical structure. The flag takes one of the following values: **Hierarchical** (present the collections in a hierarchy), or **Flat** (present the collections in a flat list).

Configuring properties of network views

You can configure how network views are displayed.

Configuring connectivity types

You can create or edit connectivity types for use in the Hop View and the Network Views.

About this task

You can display different types of connectivity in the Network Hop View and the Network Views. For example, you can display Layer 1, Layer 2, Layer 3, or IP subnets connectivity. You can also define your own connectivity types.

To configure a connectivity type, complete the following steps:

Procedure

1. On the server where the Network Manager Web components are installed, back up and edit the appropriate file:
   - For US English, edit the file `$NMGUI_HOME/profile/etc/tnm/locale/ncp_layertypes.properties`.
   - For other languages, create or edit the file `$NMGUI_HOME/profile/etc/tnm/locale/ncp_layertypes_lang_country.properties`, where *lang* is the two-letter language code, and *country* is the two-letter country code.

   For example, to define a new layer type in Brazilian Portuguese, edit the file `ncp_layertypes_pt_BR.properties`.
2. Add a line to create a new connectivity type, or edit or delete the line for an existing connectivity type. To create a new layer of type "Pseudo Wire":

```
connectivity.77:Pseudo Wire
```

In this example, the number 77 is the value of the `entityType` field from the `ncim.entityType` topology database that corresponds to Pseudo Wire Topology. You can choose a different entityType, as long as it has a metaClass of Topology. Pseudo Wire is the name that will be displayed in the **Connectivity** menu.

Important: Do not delete or modify the default connectivity types Layer 1, Layer 2. Layer 3, IP Subnets, or Converged Topology.

3. Edit or create the following file: `$NMGUI_HOME/profile/etc/tnm/locale/ncp_layertypes_`*`lang_country`*`.properties` and add a line similar to the following:

   `connectivity.`*`name`*`:`*`number`*

   Where *name* is the name by which the layer is to be referred to in dynamic templates, for example, in the `ip_default.xml` file. The name can be any combination of lowercase letters, digits and underscores. By convention, the name is the same as the name that you used in the `ncp_layertypes_`*`lang_country`*`.properties` file, converted to lowercase and with spaces removed. Refer to *IP network view template code* to see how layer names are referred to in template files, for example: `connectivity="ipsubnets"`.

   The connectivity number *number* must match the number that you added in the `ncp_layertypes_`*`lang_country`*`.properties` file.
4. Save and close the file.

Enabling custom or unassigned views

Enable custom and unassigned views if you want to create a custom or unassigned view type. You must create a custom view if you want to manually add a collection of devices to a view. Create an unassigned view to automatically collect all unassigned devices for a domain in the unassigned view.

About this task

Complete these steps to enable custom and unassigned views.

Procedure

1. Back up the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file.
2. Add or edit the following property: **`topoviz.customview.enable`**.

   Set the value to `true` to enable both custom and unassigned views.

   Note: Set the value to `false` to disable custom and unassigned views.
3. Save and close the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file.
4. Ensure that the `addToView.xml` and `removeFromView.xml` files are present in the `$NMGUI_HOME/profile/etc/tnm/tools/` directory. If they are not present, copy them from the `$NMGUI_HOME/profile/etc/tnm/tools/default/` directory.
5. Ensure that the following lines are present in the `$NMGUI_HOME/profile/etc/tnm/menus/ncp_topoviz_device_menu.xml` file:

```
<tool id="addToView"/>
<tool id="removeFromView"/>
```

Enabling visualization of logical groups

If you enable this feature, logical groups such as subnets can be expanded and collapsed in the Network Views.

About this task

If the **SubGraph** property of a Network View is disabled, membership of logical groups is shown by dashed lines connecting entities to a blank oval, which represents the logical group. If the **SubGraph**

property of a Network View is enabled, entities in logical groups are shown surrounded by a rectangular border, which can be collapsed into a cloud.

The **SubGraph** property can only be set on Network Views of type Collection.

The **SubGraph** property of a Network View can be enabled or disabled when creating or editing a network view. The option to enable or disable the **SubGraph** property only appears in the GUI if the visualization of logical groups has first been enabled by an administrator.

To enable the visualization of logical groups, complete the following tasks.

Procedure

1. Back up the `/opt/ibm/netcool/gui/precision_gui/profile/etc/tnm/topoviz.properties` file.
2. Add or edit the following line: `topoviz.collection.subgraph.enable=true`.
3. Save and close the file.

Customizing line thickness in topology maps

You can customize the thickness of the lines connecting network entities based on the speed of the connection between them.

Procedure

1. Back up and edit the file: `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`
2. Edit the following properties to enable the display of link capacity:

   topoviz.hopview.showlinkcapacity
   Set to `true` to enable link capacity display for the **Network Hop View**. Set to `false` to disable.

   topoviz.networkview.showlinkcapacity
   Set to `true` to enable link capacity display for the **Network Views**. Set to `false` to disable.
3. Edit the following properties to specify the thickness of the lines for different connection speeds:

   topoviz.pipe.1.threshold
   Specify the first connection speed threshold above which the line thickness changes. Connection speed is measured in bits/sec. You can use the following International System of Units multipliers: k, M, G, T, P, E.

   topoviz.pipe.1.thickness = 2
   Specify the thickness of a line, the connection speed of which is above the first threshold. The line thickness is specified in multiples of the default line thickness.

   topoviz.pipe.2.threshold
   Specify the second connection speed threshold above which the line thickness changes. Connection speed is measured in bits/sec. You can use the following International System of Units multipliers: k, M, G, T, P, E.

   topoviz.pipe.2.thickness
   Specify the thickness of a line, the connection speed of which is above the second threshold. The line thickness is specified in multiples of the default line thickness.

   topoviz.pipe.n.threshold
   Specify the nth connection speed threshold above which the line thickness changes, where *n* is 3, 4, or 5, in order. You can specify up to 5 thresholds. Connection speed is measured in bits/sec. You can use the following International System of Units multipliers: k, M, G, T, P, E.

   topoviz.pipe.n.thickness
   Specify the thickness of a line, the connection speed of which is above the nth threshold, where *n* is the value that you specified in the previous property. The line thickness is specified in multiples of the default line thickness.

Example

The following example specifies that connections with a capacity over 2 GBits/sec are drawn with lines that are twice as thick as the default:

```
topoviz.pipe.1.threshold = 2G
topoviz.pipe.1.thickness = 2
```

Related tasks

Monitoring links

By monitoring the links between devices, you can determine the status of the devices connected by the link. In addition, you can launch tools to diagnose the underlying problem.

Configuring Link status option

You can configure the information that is displayed on links between devices. You can choose to display information from events or poll policies.

About this task

Administrator can configure links to display event information or link status information from poll policies.

To configure **Link status options**, perform the following procedure:

Procedure

1. In the `$NMGUI_HOME/profile/etc/tnm/status.properties/` file, set the `status.link.policy.status.enabled` parameter to `true`. **Link status option** button appears on the network view toolbar.
2. To color links according to event status or the value of a poll policy, change the default by setting the `status.link.type` parameter in the `status.properties` file. The default is to display event status.

   Note: These are default settings and the user can change the settings for each network view.

Configuring column display in the tabular view

You can configure which columns are displayed in the **Network Views** table mode. You can also configure the width of columns and the horizontal alignment of displayed text.

About this task

The **Network Views** can be displayed in a tabular view, which shows information about selected devices.

To configure how columns are displayed, complete the following steps:

Procedure

1. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/ncimMetaData.xml` file.
2. Locate the following section.

```
        <columnView tableMode="topoviztable">
            <statusColumn statusColumn="severity"/>
            <statusColumn statusColumn="managedStatus"/>
            <columnName tableAlias="e" column="entityId"/>
            <columnName tableAlias="e" column="entityType"/>
            <columnName tableAlias="e" column="displayLabel"/>
            <columnName tableAlias="c" column="accessIPAddress"/>
            <columnName tableAlias="m" column="classType"/>
            <columnName tableAlias="c" column="className"/>
        </columnView>
```

   Note:

There are three topoviztable sections. You must edit each section if you make any changes. You can make the columns in each section identical.

If you choose to include different columns in different sections, the section that is associated with entity type 1 is authoritative, and the other sections must contain an initial sequence of those columns. For instance, if entity type 1 has columns A, B, C and D, the other columns can have A; or A, B; or A, B, C; or A, B, C, D. They cannot have, for instance, B, A; or A, C; or C, A, B. For the purposes of determining whether one <column Name> tag refers to the same column, only the column attribute must be the same. The tableAlias can be different.

3. Add or remove the columns that you want to display.

   Fields must come from the physicalChassis table.

   The tableAlias and column attributes must match a <dataField> tag in this <entityMetaData> section. The <listDataField> and <extraInfo> tags are not supported.

   The tabular layout displays the columns in the order specified here.

   The following columns must be present, but can be anywhere in the list:

   - entityId
   - entityType

   If you include the following columns, you must specify them by using statusColumn, as in the default example above. These columns can be anywhere in the list:

   - severity
   - managedStatus
4. Save and close the $NMGUI_HOME/profile/etc/tnm/ncimMetaData.xml file.
5. Back up and edit the $NMGUI_HOME/profile/etc/tnm/topoviz.properties file.
6. Fix Pack 5

   To change the width of a column, edit the following line, where *column* is the name of the column that you want to modify, and *width* is the width in em or px:

   ```
   topoviz.table.width.column=width
   ```

   For example:

   ```
   topoviz.table.width.severity=6em
   ```
7. Fix Pack 6

   Add or edit the following line in order to configure the horizontal alignment of text:

   ```
   topoviz.table.style.column_name=text-align: alignment
   ```

   Where column_name is the name of the column, and alignment is left, right, or center.

   By default, all text is left-aligned.
8. Fix Pack 12

   Choose the option to display the status as text or icon for severity and managedStatus columns.
9. Save and close the $NMGUI_HOME/profile/etc/tnm/topoviz.properties file.

Entity types

The entityType table contains all the entity types that are available in the NCIM topology database.

The following table lists the entity types available in the topology database.

Table 24. Network Manager entities

Entity type	Entity type name	Category	NCIM table	Description
0	Unknown	Element		
1	Chassis	Element	physicalChassis	Main node device.
2	Interface	Element	networkInterface	Interfaces with entityType 2 can be discovered and polled.
3	Logical Interface	Element	networkInterface	Interfaces with entityType 3 are inferred but are not directly accessible. Hot Standby Routing Protocol (HSRP) virtual IP interfaces are an example of logical interfaces.
4	Local VLAN	Element	localVlan	VLAN port on a main node device.
5	Module	Element	physicalCard	Card within a switch or router. The term *module* is used to avoid confusion with the term *card* which is used in layer 1 networks.
6	PSU	Element	physicalPower Supply	Power® supply unit within a main node device.
7	Logical Collection	Collection		Examples of logical collections include MPLS VPNs, global VLANs and subnets. NCIM can also model OSPF areas.
8	Daughter Card	Element		The child of a network card.
9	Fan	Element	physicalFan	Fan component within a main node device.
10	Backplane	Element	physicalBackplane	Backplane component within a main node device. Backplanes usually contain slot entities.
11	Slot	Element	physicalSlot	Slot component within a main node device. Slots usually contain module entities.
12	Sensor	Element	physicalSensor	Sensor component within a main node device.
13	Virtual Router	Element	virtualRouter	Represents a instance of a virtual router within a chassis device.
14	CPU	Element	cpu	Represents Central Processing Units (CPUs).
15	Subnet	Collection	subnet	Logical collection that lists the IP address in a class A, B, or C subnet.
16	Global VLAN	Collection	globalVlan	Collection of VLAN entities across multiple chassis devices that combine to form a virtual network.
17	VPN	Collection	networkVpn	Logical collection of IP address collected within a VPN.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
18	HSRP Group	Collection	hsrpGroup	Represents an Hot Standby Routing Protocol (HSRP) group logical collection. The Cisco HRSP implements a virtual router with its own IP and MAC addresses. This virtual router forms an HSRP group that consists of a number of real interfaces, only one of which is active at any given time. The active interface forwards IP traffic that is sent to the virtual router, and the other interfaces in the group stand by ready to become active if the active interface fails.
19	Stack	Element		Collection of chassis devices as defined by the Entity MIB.
20	VRF	Element	vpnRouteForwarding	Represents a VPN routing and forwarding table.
21	OSPF Routing Domain	Collection	ospfRoutingDomain	Represents an OSPF routing domain.
22	OSPF Service	Service	ospfService	Represents an OSPF service running on a device.
23	OSPF Area	Collection	ospfArea	Represents an OSPF area.
24	VTP Domain	Collection	vtpDomain	Represents a VLAN trunking protocol domain.
25	Other	Element	physicalOther	Stores attributes of a component whose entity type the discovery was unable to determine. This occurs if the physical entity class is known, but does not match any of the supported values.
26	BGP Service	Service	bgpService	Represents a BGP service.
27	BGP AS	Collection	bgpAutonomousSystem	Represents a BGP autonomous system.
28	BGP Route	Attribute	bgpRouteAttribute	Represents a BGP route.
29	BGP Cluster	Collection	bgpCluster	Represents a BGP cluster.
30	BGP Network	Service	bgpNetwork	Represents a BGP network.
31	ISIS Service	Collection		Represents an ISIS service.
32	ISIS Level	Element		Represents the ISIS level.
33	OSPF Pseudo-Node	Element		Represents an OSPF pseudo-node.
34	ITNM Service	Collection	itnmService	The base type for other services such as ISIS Service.
35	MPLS TE Service	Service	mplsTEService	Represents a Multi Protocol Label Switching Traffic Engineered (MPLS TE) service

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
36	MPLS TE Tunnel	Element	mplsTETunnel	Represents an MPLS TE tunnel
37	MPLS TE Resource	Element	mplsTETunnel Resource	Represents an MPLS TE resource
38	MPLS LSP	Element	mplsLSP	Represents an MPLS Label Switch Path (LSP)
40	IP Connection	Element	ipConnection	Represents a connection using TCP/IP.
41	PIM Service	Service	pimService	Represents a Protocol Independent Multicast (PIM) service.
42	PIM Network	Collection	pimNetwork	Represents a PIM network.
43	IPMRoute Service	Service	ipMRouteService	Represents an IP Multicast Routing service.
44	IPMRoute Upstream	Element	ipMRouteUpstream	Stores the upstream (RPF) route statistics for each device or Multicast Distribution Tree (MDT).
45	IPMRoute Downstream	Element		Stores the downstream route statistics per device or MDT.
46	IPMRouteMdt	Collection	ipMRouteMdt	Stores the Collection entities representing the MDTs for each Multicast Source or Group.
47	IPMRouteSource	Element	ipMRouteSource	Represents Multicast Sources, as contained by the MDT.
48	IPMRouteGroup	Element	ipMRouteGroup	Represents Multicast Groups, as contained by the MDT.
49	IP Path	Collection	ipPath	Represents a network path between IP devices.
50	IP End point	Protocol Endpoint	ipEndPoint	Represents a logical IP end point that is implemented by a physical interface.
51	VLAN Trunk End point	Protocol Endpoint	vlanTrunkEndPoint	Represents a logical VLAN trunk end point that is implemented by a physical interface.
52	Frame Relay End point	Protocol Endpoint	frameRelay EndPoint	Represents a logical Frame Relay end point that is implemented by a physical interface.
53	OSPF End point	Protocol Endpoint	ospfEndPoint	Represents a logical OSPF end point that is implemented by a physical interface.
54	ATM End point	Protocol Endpoint	atmEndPoint	Represents a logical ATM end point that is implemented by a physical interface.
55	VPWS End point	Protocol Endpoint	vpwsEndPoint	Represents a logical VPWS end point that is implemented by a physical interface.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
56	BGP End Point	Protocol Endpoint	bgpEndPoint	Represents a logical BGP end point that is implemented by a physical interface.
57	ISIS End Point	Protocol Endpoint		Represents a logical ISIS end point that is implemented by a physical interface.
58	MPLS Tunnel End Point	Protocol Endpoint	mplsTETunnelEndPoint	Represents a logical MPLS tunnel end point that is implemented by a physical interface.
59	TCP/UDP End Point	Protocol Endpoint		Represents a logical TCP/UDP end point that is implemented by a physical interface.
60	PIM End Point	Protocol Endpoint	pimEndpoint	Represents the Protocol Independent Multicast (PIM) end points discovered in the network and their associated attributes.
61	IPMRoute End Point	Protocol Endpoint	ipMRouteEndPoint	Stores information on the IP Multicast Routing Protocol End Points.
62	IGMP End Point	Protocol Endpoint	igmpEndPoint	Stores information on the Internet Group Membership Protocol (IGMP) End Points.
63	Network Service Entity End Point	Protocol Endpoint	networkServiceEntityEndPoint	Helps model relationships related to the management of frame relay links.
67	LAG End Point	Protocol Endpoint	lagEndPoint	Represents a logical Link Aggregation Group (LAG) end point that is implemented by a physical interface.
68	Probe End point	Protocol Endpoint	probeEndPoint	Fix Pack 3 Represents the source or target end point of a probe operation, implemented by a physical interface.
70	Topology	Topology		Grouping of connections which belong to a topology.
71	Layer 1 Topology	Topology		Grouping of connections which belong to a Layer 1 topology.
72	Layer 2 Topology	Topology		Grouping of connections which belong to a Layer 2 topology.
73	Layer 3 Meshed Topology	Topology		Grouping of connections which belong to a Layer 3 meshed topology.
74	Converged Topology (Layer 1 - Layer 3)	Topology		Based on data available in NCIM, groups together connections at the lowest layer for which data is available.
75	MPLS TE Topology	Topology		Grouping of connections which belong to an MPLS TE topology.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
77	Pseudo Wire Topology	Topology		Grouping of connections which belong to a Pseudo Wire topology.
78	OSPF Topology	Topology		Represents an OSPF topology.
79	BGP Topology	Topology		Represents a BGP topology.
80	IP Path Topology	Topology	ipPath	Represents an IP path.
81	PIM Topology	Topology		Represents PIM topologies.
82	Local VLAN Topology	Topology		Represents local VLAN topologies.
83	IPMRoute Topology	Topology		Represents an IP Multicast Routing topology.
84	VPLS Pseudo Wire Topology	Topology		Respresents a VPLS Pseudo Wire Topology.
85	Virtualization Topology	Topology		Represents a virtualization topology.
86	Microwave Topology	Topology		Represents a microwave topology.
87	RAN Topology	Topology		Represents a radio access network topology.
90	LTE Control Plane	Topology		Represents the devices and connectivity that make up the LTE control plane.
91	LTE User Plane	Topology		Represents the devices and connectivity that make up the LTE user plane.
92	Probe Topology	Topology		Represents the probe source/target connectivity.
110	Generic Collection	Collection	genericCollection	A collection that is not of any other type.
111	Geographic Location	Element	geographicLocation	Represents a geographic location.
112	Geographic Region	Collection	geographicRegion	Represents a geographic region.
113	VLAN Ports	Collection	vlanCollection	Represents a collection of the ports on a given named VLAN or, if no name is provided, on a given VLAN identifier.
120	IGMP Service	Service	igmpService	Represents an Internet Group Management Protocol (IGMP) service.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
121	IGMP Groups	Collection	igmpGroup	Stores multicast group collections for which there are associated Internet Group Membership Protocol (IGMP) end points in the igmpEndPoint table.
122	VSI (Virtual Switch Instance)	Element	virtualSwitch Instance	Represents a virtual switch instance (VSI) configured on a Provider Edge (PE) device that is associated with a Virtual Private LAN Service (VPLS) Virtual Private Network (VPN) instance.
123	Data Center	Element		Represents a data center.
124	Virtual Cluster	Collection	virtualCluster	Represents a cluster of virtual machines.
125	Virtual Management Service	Service	virtualMgmtService	Represents a virtual management service.
126	Hypervisor	Element	hypervisor	Represents a hypervisor.
127	Port Group	Collection	portGroup	Represents a port group.
128	EMS System	Element	emsSystem	Represents an EMS system accessed by a collector.
130	RAN GSM Cell	Element	ranGSMCell	Represents a GSM cell.
131	RAN UTRAN Cell	Element	ranUtranCell	Represents a UTRAN cell.
132	RAN Sector	Element	ranSector	Represents a RAN sector.
133	RAN NodeB Local Cell	Element	ranNodeBLocalCell	Represents a NodeB Local Cell.
134	RAN Location Area	Collection	ranLocationArea	Represents a RAN Location Area.
135	RAN Routing Area	Collection	ranRoutingArea	Represents a RAN Routing Area.
136	RAN Packet Core	Collection		Represents RAN packet switch core entity.
137	RAN Circuit Core	Collection		Represents a RAN circuit switched core entity.
138	RAN Radio Core	Collection	ranRadioCore	Represents a RAN radio core entity.
139	RAN Transceiver	Collection	ranTransceiver	Represents a RAN transceiver.
150	LTE Sector	Element	eUtranSector	Represents a geographic area of radio coverage and is implemented and supported by physical radio equipment. An LTE sector implements one or more LTE cells.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
151	LTE Cell	Element	eUtranCell	Represents a geographical area of radio coverage and is implemented and supported by physical radio equipment, such as towers, amplifiers, and antennas.
152	MME Function	Element	mmeFunction	The Mobility Management Entity (MME) is the main signalling control element in the core network and is the key control node for enabling user equipment access to the core network. The role of the MME is implemented within a network hardware node and is modelled by NCIM using the mmeFunction entity type. Multiple mmeFunction instances can be implemented within a single network hardware node.
153	Tracking Area	Collection	trackingArea	Represents an LTE tracking area.
154	SGW Function	Element	sgwFunction	The Serving Gateway (SGW) resides in the user plane where it forwards and routes packets to and from the eNodeB and packet data network gateway (PGW). The role of the SGW is implemented within a network hardware node and is modelled by NCIM using the sgwFunction entity type. Multiple sgwFunction instances can be implemented within a single network hardware node.
155	PGW Function	Element	pgwFunction	The Packet Data Network Gateway (PGW) provides user plane connectivity to packet data networks. The role of the PGW is implemented within a network hardware node and is modelled by NCIM using the pgwFunction entity type. Multiple pgwFunction instances can be implemented within a single network hardware node.
156	ENB Function	Element	enbFunction	The eNodeB device manages the radio air interface communication with users of the LTE network. Each eNodeB device controls one or more cells, which are geographic areas of radio coverage. The role of the eNodeB is implemented within a network hardware node and is modelled by NCIM using the enbFunction entity type. Multiple enbFunction instances may be implemented within a single network hardware node.
157	LTE Pool	Collection	ltePool	Generic modelling mechanism for groups of pooled LTE entities, and currently used to model MME pools, PGW pools, and SGW pools. As an example, in order to model an MME pool, the relationship between the ltePool entity and associated mmeFunction entities is modelled using the collects table.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
158	PLMN	Element	plmn	Models a Public Land Mobile Network (PLMN). A PLMN is a network that provides land mobile telecommunications services to the public. Each operator providing mobile services has its own PLMN.
159	HSS Function	Element	hssFunction	Models the LTE Home Subscriber Service (HSS). The HSS manages subscriber identities, service profiles, authentication, authorization, and quality of service (QoS), and acts as the master repository for subscriber profiles, device profiles and state information.
160	PCRF Function	Element	pcrfFunction	Models the LTE Policy and Charging Rules Function (PCRF). The PCRF manages the policy and charging for uplink and downlink service flows and the permitted EPS bearer QoS.
161	EIR Function	Element	eirFunction	Models the LTE Equipment Identity Register (EIR). The EIR keeps track of mobile devices which should either be banned from using the network or monitored. When a mobile phone is stolen its identity it is added to the EIR blacklist and the result is that this phone will never be able to attach to the network for service. Usually each network has its own EIR which is often combined with the HSS node. It is possible for multiple operators to share a common EIR which enables the blacklisted information to be more easily and widely available.
163	LTE Control Plane	Collection	controlPlane ViewCollection	Supports the dynamic collection views under **LTE Network Topology** > **Control Plane by Tracking Area** in the Network Views. Each instance of this entity type collects the eNodeBs in the corresponding tracking area, together with the devices that these eNodeBs are connected to on the control plane.
164	LTE User Plane	Collection	userPlane ViewCollection	Supports the dynamic collection views under **LTE Network Topology** > **User Plane by Tracking Area** in the Network Views. Each instance of this entity type collects the eNodeBs in the corresponding tracking area, together with the devices that these eNodeBs are connected to on the user plane.
170	Aggregated Link	Collection	aggregatedLink	Represents a network link between Link Aggregation Groups (LAGs)
171	Link Aggregation Group	Element	aggregationGroup	Represents a Link Aggregation Group (LAG).
190	Probe Service	Service	probeService	Fix Pack 3 Represents the service that provides probes on a device.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
191	Probe	Collection	probe	Fix Pack 3 Represents configured network probes and their attributes.
192	Probe Collection	Collection	probeCollection	Fix Pack 3 Provides a collection facility for probes or probe collections.
200	LTE S1-U	Topology	entityData	Topology type for LTE S1-U connectivity.
201	LTE S5	Topology	entityData	Topology type for LTE S5 connectivity.
202	LTE S8	Topology	entityData	Topology type for LTE S8 connectivity.
203	LTE S1-MME	Topology	entityData	Topology type for LTE S1-MME connectivity.
204	LTE S10	Topology	entityData	Topology type for LTE S10 connectivity.
205	LTE S11	Topology	entityData	Topology type for LTE S11 connectivity.
206	LTE SGi	Topology	entityData	Topology type for LTE SGi connectivity.
207	LTE Gx	Topology	entityData	Topology type for LTE Gx connectivity.
208	LTE S3	Topology	entityData	Topology type for LTE S3 connectivity.
209	LTE S4	Topology	entityData	Topology type for LTE S4 connectivity.
210	LTE S6a	Topology	entityData	Topology type for LTE S6a connectivity.
211	LTE S13	Topology	entityData	Topology type for LTE S13 connectivity.
212	LTE X2	Topology	entityData	Topology type for LTE X2 connectivity.
250	NR Sector	Element	eUtranSector	5G New Radio Sector Entity.
251	NR Cell DU	Element	NRCellDU	Represents a geographical area of radio coverage and is implemented and supported by physical radio equipment for 5G LTE, such as towers, amplifiers, and antennas.
252	NR Cell CU	Element	NRCellCU	Represents a geographical area of radio coverage and is implemented and supported by physical radio equipment for 5G LTE, such as towers, amplifiers, and antennas.

Table 24. Network Manager entities (continued)

Entity type	Entity type name	Category	NCIM table	Description
253	GNB DU Function	Element	gnbFunction	The gNodeB device manages the radio air interface communication with users of the 5G network. Each gNodeB device controls one or more cells, which are geographic areas of radio coverage. The role of the gNodeB is implemented within a network hardware node and is modelled by NCIM using the gnbFunction entity type. Multiple gnbFunction instances may be implemented within a single network hardware node.
254	GNB CUCP Function	Element	gnbFunction	The gNodeB device manages the radio air interface communication with users of the 5G network. Each gNodeB device controls one or more cells, which are geographic areas of radio coverage. The role of the gNodeB is implemented within a network hardware node and is modelled by NCIM using the gnbFunction entity type. Multiple gnbFunction instances may be implemented within a single network hardware node.
255	GNB CUUP Function	Element	gnbFunction	The gNodeB device manages the radio air interface communication with users of the 5G network. Each gNodeB device controls one or more cells, which are geographic areas of radio coverage. The role of the gNodeB is implemented within a network hardware node and is modelled by NCIM using the gnbFunction entity type. Multiple gnbFunction instances may be implemented within a single network hardware node.

Chapter 8. Administering network view bookmarks

Network view bookmarks group together just those network views that you or your team need to monitor. Create new bookmarks or change existing bookmarks to help network operators visualize just those devices that they need to monitor.

About network view bookmarks

Network view bookmarks group together selected network views.

Each network view bookmark contains selected network views in a tree structure that is inherited from the network view libraries. If you add a parent network view to a bookmark, you automatically also get all the children networks views in the bookmark. If you want only certain child network views you can do this by adding just those child network views to the bookmark.

For example, a NOC administrator is creating a network view bookmark to assign to his NOC. The parent network view **Subnet** contains six subnet network views, A through F. The administrator adds subnets A, B, and C to the bookmark, but does not add subnets D, E, and F, because his NOC is not responsible for monitoring subnets D through F.

Note: In this example, the system automatically adds the parent network view **Subnets** to the bookmark. The Bookmarks treetable displays system-added views, such as the **Subnets** view in this example, with an asterisk to the left of the network view name. Manually added views, such as views A, B, and C in this example, are displayed without an asterisk to the left of the view name.

Read-write and read-only permissions for bookmarks can be set on individual user and on a group basis. By default this can be done by an administrator. Permissions for a bookmark can also be set globally; global permission apply to everyone else, that is, all users who have neither individual user permissions for the bookmark, nor are members of any of the groups that have group permissions for the bookmark. In addition, individual operators can create their own bookmarks.

The maximum alert status of all entities in a network view is reported in the network view bookmark tree for all bookmarks.

Creating network view bookmarks

Create a network view bookmark to group together just those network views that you or your team need to monitor.

About this task

To create a network view bookmark:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. Within **Network Views**, in the **Bookmarks** tab, click **Create Bookmark**  .
3. Complete the **Bookmark Properties** window as follows:

   Name
   To create a new bookmark, type the name of the bookmark. To change the name of an existing bookmark, type the new name of the bookmark over the current name.

   Note: Bookmark names cannot be blank and must be unique per user account.

   Set as Default
   Click here to set this bookmark as the default bookmark which displays on each visit to the **Network Views** > **Bookmarks** tab.

Bookmark permissions sections

If you have the ncp_bookmark_admin role, then you can modify permissions for the current bookmark using the panel sections below. If you do not have this role then you can only view the permissions for the current bookmark. By default the itnmadmin user has this role. Also, any user that is a member of the administrator group Network_Manager_IP_Admin has this role.

User Permissions

In this part of the panel you can set individual user permissions for the current bookmark.

New permission 

Click here to set a new permission for a specific user. Options are read-only or read-write. Clicking this button adds a row to the **User Permissions** table. In the **User** column, click and select from the drop-down list to select a user. In the **Permissions** column, click and select from the drop-down list to set a permission for this user.

Delete permission 

Select one or more rows in the **User Permissions** table and then click this button to remove permissions for the selected user or users.

Group Permissions

In this part of the panel you can set user group permissions for the current bookmark.

New permission 

Click here to set a new permission for a user group. Options are read-only or read-write. Clicking this button adds a row to the **Group Permissions** table. In the **Group** column, click and select from the drop-down list to select a user group. In the **Permissions** column, click and select from the drop-down list to set a permission for this user group.

Delete permission 

Select one or more rows in the **Group Permissions** table and then click this button to remove a permissions for the selected user group or groups.

Global Permissions

Click here and select from the drop-down list to set global permissions for the current bookmark. Options are none, read-only or read-write. The global permission setting on a given bookmark applies to all other users; that is all users who meet both of the following criteria:

- They are not mentioned in the **User Permissions** section.
- They are not members of any of the groups in the **Group Permissions** section.

4. Click **OK**. The new network view bookmark is added to the bookmarks drop-down list. Open the bookmarks drop-down list to see the new bookmark.

   Note: If you set this bookmark as the default bookmark, then it appears at the top of the list. Otherwise it appears in the list in alphabetical order.

Editing network view bookmarks

You can edit bookmarks properties and also change the network views contained in a bookmark.

Editing bookmark properties

You can edit the bookmark name, change the default bookmark settings, or, view or edit the bookmark permissions.

About this task

To edit bookmark properties:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Bookmarks**.
2. Click **Edit Bookmark**  .
3. Complete the **Bookmark Properties** window as follows:

   Name
   To create a new bookmark, type the name of the bookmark. To change the name of an existing bookmark, type the new name of the bookmark over the current name.

   Note: Bookmark names cannot be blank and must be unique per user account.

   Set as Default
   Click here to set this bookmark as the default bookmark which displays on each visit to the **Network Views** > **Bookmarks** tab.

   Bookmark permissions sections
   If you have the ncp_bookmark_admin role, then you can modify permissions for the current bookmark using the panel sections below. If you do not have this role then you can only view the permissions for the current bookmark. By default the itnmadmin user has this role. Also, any user that is a member of the administrator group Network_Manager_IP_Admin has this role.

   User Permissions
   In this part of the panel you can set individual user permissions for the current bookmark.

   New permission 
   Click here to set a new permission for a specific user. Options are read-only or read-write. Clicking this button adds a row to the **User Permissions** table. In the **User** column, click and select from the drop-down list to select a user. In the **Permissions** column, click and select from the drop-down list to set a permission for this user.

   Delete permission 
   Select one or more rows in the **User Permissions** table and then click this button to remove permissions for the selected user or users.

   Group Permissions
   In this part of the panel you can set user group permissions for the current bookmark.

   New permission 
   Click here to set a new permission for a user group. Options are read-only or read-write. Clicking this button adds a row to the **Group Permissions** table. In the **Group** column, click and select from the drop-down list to select a user group. In the **Permissions** column, click and select from the drop-down list to set a permission for this user group.

   Delete permission 
   Select one or more rows in the **Group Permissions** table and then click this button to remove a permissions for the selected user group or groups.

   Global Permissions
   Click here and select from the drop-down list to set global permissions for the current bookmark. Options are none, read-only or read-write. The global permission setting on a given bookmark applies to all other users; that is all users who meet both of the following criteria:

   - They are not mentioned in the **User Permissions** section.
   - They are not members of any of the groups in the **Group Permissions** section.
4. Click **OK**.

Adding a network view to a bookmark

Add a network view to a bookmark by right-clicking the desired network view in the network view libraries tree.

About this task

To add network views to a bookmark:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. Select a single network view as follows:
   a) From the network view library drop-down list above the network view tree, select the network view library that contains the network view to add to the bookmark.
   b) In the network view tree navigate to the desired network view.
3. Right-click the desired network view and click **Add to Bookmark**, then in the submenu, click the name of the bookmark to add the network view to. Only the bookmarks that you have permission to read and write to appear in the list.
   For example, if you want to add the selected network views to an existing bookmark named Bookmark1, then click **Add to Bookmark** > **Bookmark1**.

   Network views are added to the bookmark in the following way:

   - If you selected a parent network view, then the parent network view and all of its child network views are added to the bookmark. If the parent network view is a dynamic network view, then as child network views are added to or removed from the parent following network discovery, the views are added to or removed from the bookmark automatically.
   - If you selected one or more child network views whether of a standard or dynamic parent network view then only the network views you selected are added to the bookmark. In addition, individually selected child network views of dynamic parent network views will be automatically removed from the bookmark if the child network view is removed following network discovery.
   - Whichever view you add to a bookmark, the system automatically adds its parent, the parent's parent, and so on until it gets to the top of the tree.

   Note: Manually added network views appear without an asterisk to the left of the view name. System-added network views appear with an asterisk to the left of the view name. For example, if you added a parent network view to the bookmark, then the parent network view and all of its child network views are added to the bookmark. Asterisks are shown as follows:

   - The parent network view was manually added, and therefore appears without an asterisk.
   - The child network views were added by the system, and therefore appear with an asterisk.

Removing a network view from a bookmark

Remove a network view from a bookmark by right-clicking a network view in the network view bookmarks tree.

About this task

To remove network views from a bookmark:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Bookmarks**.
2. Select a single network view as follows:
   a) From the network view bookmarks drop-down list above the network view tree, select the network view bookmark that contains the network view to remove from the bookmark.

b) In the network view bookmarks tree, navigate to the desired network view.

Restriction: You can only remove network views from the bookmark that were manually added to the bookmark earlier, as follows:

- The network views that you can remove appear without an asterisk to the left of the view name. These are manually added views.
- The network views that you cannot remove appear with an asterisk to the left of the view name. These are views added by the system. System-added views are parents or children of manually added views.

3. Right-click the desired network view and click **Remove view from bookmark**.

   Restriction: You can only remove a view from a bookmark if you have read-write permission on that bookmark, or you have the `ncp_bookmark_admin` role.

   The selected view is removed from the bookmark.

   Note: If a view is removed that is part of a hierarchy of other views that were previously added then that view will not be physically removed from the tree but will be marked with an asterisk (*).

Deleting a network view bookmark

Deleting a network view bookmark completely removes that bookmark from the system.

About this task

To delete a network view bookmark:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Bookmarks**.
2. From the network view bookmarks drop-down list, select the bookmark that you want to delete.
3. Click **Delete Bookmark**  .

   Restriction: You can only delete a bookmark if you have read-write permission on that bookmark, or you have the `ncp_bookmark_admin` role.

   The bookmark is removed from your system.

Chapter 9. Configuring tools and menus

You can create and edit context menus, configure user access to menu items, define the context in which menus are available, and create tools that can be run from the context menus.

About context menus

Context menus are opened by right-clicking on devices, events, subnets, links, or components within the device structure browser, for example network ports. You can run tools from context menus. You apply filters to menus and tools.

As an administrator, you can create context menus that enable operators to run tools on devices, events, subnets, links, or components within the device structure browser. You can configure which users can access the tools, and where the tools, menus and menu hierarchies can be used from.

About filters

Filters are pieces of XML code that form part of an XML menu definition or an XML tool definition. There are two types of filter: *context filters* and *security filters*.

Filter characteristics are inherited by submenu and tools. For example if the `My Tools...` menu has context or security restrictions, then these restrictions are applied to all menus and tools within the `My Tools...` menu.

If no filter is present then the menu or tool will always appear in the context menu.

Related tasks

Defining context filters for tools and menus
You can specify the types of views in which a menu or tool is available, and which devices it can be run on, using context filters.

Defining user access for tools and menus
You can specify the users, roles, and groups authorized to display a tool or menu using security filters.

About tools

Tools are defined in XML files in the `$NMGUI_HOME/profile/etc/tnm/tools/` directory. You can associate URL tools with a menu option.

Related tasks

Creating tools for context menus
You can create tools for operators to use and add them to context menus on a network map.

Configuring context menus

You can add a menu item to, or edit the menu items in, the context menus that are displayed when you right-click a device or subnet from a topology map.

About this task

You can associate tools with menu items to enable network operators to right-click a device, link or subnet and run a script or a third-party Web application. Tools can also be invoked from components in the device structure browser, such as network ports, via the **Tools** menu. Any new menu items you define appear after the default menu items.

To add or edit an item in a context menu for a device, event, subnet, link or component within the device structure browser, complete the following steps.

Procedure

1. Edit an XML file in the $NMGUI_HOME/profile/etc/tnm/menus/ directory.
2. Configure the elements and attributes of the menu definition to define the name, filters, label, and other properties of the menu item. Use the reference information about the XML elements and attributes available for menu items and the example provided to help you define the menu item.
3. Add the menu item that you have defined to the appropriate menu type in the $NMGUI_HOME/profile/etc/tnm/topoviz.properties file:

   Menus launched from devices or subnets
   `topoviz.menu.device = menu-id`

   Menus launched from subviews
   `topoviz.menu.subview = menu-id`

   Menus launched from the background with no objects selected
   `topoviz.menu.background = menu-id`

   Menus launched from a link between devices, subnets, or subviews
   `topoviz.menu.link = menu-id`

   Where *menu-id* is an identifier that points to the top level of a menu hierarchy defined in an XML file in the $NMGUI_HOME/profile/etc/tnm/menus/ directory. Subnets require a separate menu because the tools executed on subnets are executed for all nodes contained within the subnet.

   The following example defines a menu item for devices with the identifier "mytools":

```
topoviz.menu.device = mytools
```

XML elements and attributes for defining context menus

Understand the different XML elements and attributes that define context menu items.

Sample menu item definition

The following example shows the format of an XML file that defines a menu item. Elements are highlighted in bold for clarity.

```
<ncp_menu id="mytools" label="My Tools" key="key">
<context>
<!-- This section of the xml file is a context filter. -->
<!-- Context filters specify the device and view conditions -->
<!-- under which this menu is displayed. -->
</context>
<security>
<!-- This section of the xml file is a security filter. -->
<!-- Security filters specify the users, roles and groups -->
<!-- authorized to display this menu. -->
</security>
<definition>
<tool id="ncp_dns"/>
<separator/>
<menu id="ncp_cisco"/>
<menu id="ncp_juniper"/>
</definition>
</ncp_menu>
```

XML elements and attributes

The following table describes the elements and attributes used to define context menus, with reference to the above example.

Table 25. Elements and Attributes in the menu XML definition file		
Element or attribute	**Type**	**Description**
`ncp_menu`	Element	Introduces the definition of a menu.
`context`	Element	Defines the views and devices that the menu items is available from. Use the reference information about defining context filters to define this attribute.
`security`	Element	Defines the users, groups and roles that are allowed to view the menu item. Use the reference information about defining user access filters to define this attribute.
`id`	Attribute	Contains an alphanumeric identifier for this menu.
`label`	Attribute	Contains the actual text of the menu option that appears in the context menu.
`key`	Attribute	Used as a lookup into the `$NMGUI_HOME/profile/etc/tnm/locale/ncp_menus(_xx_XX).properties` file. This allows you to specify translations of the menu label for users with different locale settings.
`tool`	Element	Inserts a tool with the specified `id` into the menu. In this example, a tool with the id ncp_dns is inserted into the menu. The associated menu text for this tool is **DNS Lookup**. The ncp_dns tool is defined in a separate XML file stored in `$NMGUI_HOME/profile/etc/tnm/tools/`.
`separator`	Element	Inserts a separator into the menu.
`menu`	Element	Inserts a submenu with the specified `id` into the menu. In this example, two submenus are defined: • The `ncp_cisco` submenu. The associated menu text for this submenu is `Cisco Tools...`. • The `ncp_juniper` submenu. The associated menu text for this submenu is `Juniper Tools...`. Each of these submenus is defined in a separate `.xml` file stored in `$NMGUI_HOME/profile/etc/tnm/menus/`. These `.xml` files are formatted according to the rules defined in this section.

Configuring WebTools

The `itnmadmin` user can configure WebTools by modifying values in the related configuration files.

WebTools is one of the ready-to-use right-click tools that are provided by Network Manager. Use WebTools to perform diagnostic and information retrieval actions on network devices that are shown in network views. The `itnmadmin` user can modify how users use WebTools.

About WebTools

The `itnmadmin` user can configure WebTools to extract values from one WebTools command output, and then use the values as parameter-values for the next command.

About this task

To reuse values from a WebTools command, you must update the definition files for the WebTools tool. There is one set of definition files per tool. The definition files consist of a template file that acts as a wrapper, and a processor file.

Procedure

Update the WebTools tool definition files.

- Within `$NCHOME/core/precision/scripts/webtools/etc/templates/` update the template file. The standard template file that is included in the product is called `ncp_wt_border.tmpl`.
- Within `$NCHOME/core/precision/scripts/webtools/etc/processors/` update the processor file. The standard processor files that are included in the product are called `advtraceroute_exec.proc`, `default_exec.proc`, `default_telnet.proc`, and `notitle_exec.proc`.

Example

Enter the following command, this command tells the `ncp_webtool.cgi` script to load the `DNSLookup.xml` file and use `8.8.8.8` as the query parameter and do whatever is defined within the `DNSLookup.xml` file.

```
Run the  command   -  ncp_perl ../bin/ncp_webtool.cgi toolid=DNSLookup query=8.8.8.8
```

The `DNSLookup.xml` file and other `.xml` files give the following types of definitions.

Lists the named parameter to accept and their types.
The template file to use.
The data processor file to use.
The order in which things within the tool must be run.

The tools within WebTools can be one of two types.

- A helper tool. This tool uses the Network Manager SSH Telnet stack to access a device and run a series of commands against the device as defined by the tool definition. Use the `CiscoShowRoute.xml` file as an example of a helper tool. The `CiscoShowRoute.xml` file sets term length zero to avoid pagination and not does not include the output of the query in the results `visible=0`. Then, the file runs `show ip route` and supplies the parameters that are called `vrf, vrfname, target`, in that order and if the parameters are specified. You can also run the helper tools from the command line.

```
<commands>
        <command visible="0" allow_early_match="1" response_time="5000">term length 0</command>
        <command visible="1" allow_early_match="1" response_time="5000">show ip route ##vrf## ##vrfname##
##target##</command>
</commands>
```

- An executable tool. This tool runs a command on the Network Manager backend server and passes named parameters to it. For this example, the `DNSLookup.xml` file runs the executable file and passes in the type and query parameters, which are also defined in the file, into the script in that order.

```
<command>
       <executable>${NCWTHOME}/bin/ncp_wt_nslookup.pl</executable>
       <argument>type</argument>
       <argument>query</argument>
   </command>
```

Limiting menus from WebTools

The `itnmadmin` user can modify the list of **WebTools** menu items visible to a specific role.

About this task

Procedure

1. Within `$ITNMHOME/gui/precision_gui/profile/etc/tnm/menus`, open the configuration file for the **WebTools** menu item that you want to modify.
   For example, for the **Topology Management** menu item, open the `ncp_topo_mgmt_menu.xml` configuration file.
2. Within the configuration file, for the `role name` parameter, enter the role name.

Example

- Display the **Topology Management** menu item if users are assigned the `ncp_topo_mgmt` role and you are in the hop view.

```
[root@CO9128108199 menus]# more ncp_topo_mgmt_menu.xml
<?xml version="1.0" ?>
<ncp_menu id="ncp_topo_mgmt_menu" key="ncp_topo_mgmt_menu" label="Topology Management">
        <definition>
                <tool id="addDevice"/>
                <tool id="deleteDevice"/>
                <tool id="addConnection"/>
                <tool id="removeConnection"/>
        </definition>
        <context>
                <attribute id="clientType">
                        <equals value="ncp_hopview" />
                </attribute>
        </context>
         <security>
                <role name="ncp_topo_mgmt"/>
        </security>
</ncp_menu>
```

- Display the **Apply Policy** menu item if users are assigned the `ncmPolicyCheck` role and they select one device for which there is a record in the `networkConfigMgr` table and the device `ncmKey` is not empty. The `entityId lookup` is implicit in this example.

```
[root@CO9128108199 tools]# more itncm_apply_policy.xml
<?xml version="1.0"?>
<ncp_tool id="itncm_apply_policy" key="itncm_apply_policy"
        label="Apply Policy" type="url" runOnList="true" runForEach="false">
        <url
                value="ITNCMWizard/jsp/servlet/ITNCMWizardApplyPolicy.jsp"
                target="_blank" method="GET">
                <parameter name="ui.action" valueType="text" text="run" />
                <parameter name="ui.name" valueType="text" text="Apply Policy" />
                <parameter name="wizardType" valueType="text" text="apply_policy" />
                <parameter name="applicationType" valueType="text" text="device" />
                <parameter name="applicationKeys" valueType="ncim" table="entity"
                        column="entityid" />
                <parameter name="applicationNames" valueType="ncim" table="entity"
                        column="entityName" />
        </url>
        <context>
                <attribute id="deviceCount">
                        <equals value="1" />
                </attribute>
                <attribute id="ncmKey" valueType="ncim" table="networkConfigMgr"
                        column="ncmKey">
                        <notequals value="" />
                </attribute>
        </context>
        <security>
                <role name="ncmPolicyCheck" />
```

```
        </security>
</ncp_tool>
```

Creating an executable WebTools tool

The itnmadmin user can create a standard WebTools tool.

About this task

An executable WebTools tool uses a task on the Network Manager backend server and the Network Manager administrator user itnmadmin must login to the server to define the new tool. After the itnmadmin user creates a standard WebTools tool, the tool becomes available for use in the WebTools menu to users with relevant roles. The itnmadmin user must complete the following steps to create a standard WebTools tool.

Procedure

1. Within $NCHOME/core/precision/scripts/webtools/etc/, create a WebTools configuration xml file for your new executable WebTools tool. To see existing WebTools configuration xml files, enter the $ ls command within $NCHOME/core/precision/scripts/webtools/etc/.
   For example,

```
$ cd $NCHOME/precision/scripts/webtools/etc/
$ ls
AdvancedPing.xml        CiscoLSPPing.xml             CiscoMRouteInfo.xml
AdvancedSubnetPing.xml  CiscoLSPTraceroute.xml       CiscoOSPFInfo.xml
AdvancedTraceroute.xml  CiscoMBGPInfo.xml            CiscoPIMInfo.xml
CiscoBGPInfo.xml        CiscoMPLSInfo.xml            CiscoPing.xml
CiscoIGMPInfo.xml       CiscoMPLSTEInfo.xml          CiscoRoutingInfo.xml
CiscoISISInfo.xml       CiscoMPLSTELinkMgmtInfo.xml  CiscoShowCDPNeighbors.xml
CiscoInterfaceList.xml  CiscoMPLSTESpecificInfo.xml  CiscoShowEtherChannelSummary.xml
```

2. Create a set of definition files for the new WebTools tool. There is one set of definition files per tool, which consists of a template file that acts as a wrapper, and a processor file. The template file and processor file govern output, format, and content.
   - Either create a template file within $NCHOME/core/precision/scripts/webtools/etc/templates/, or use the standard template file that is included in the product, which is called ncp_wt_border.tmpl.
   - Either create a processor file within $NCHOME/core/precision/scripts/webtools/etc/processors/ or use one of the standard processor files that are included in the product, which are called advtraceroute_exec.proc, default_exec.proc, default_telnet.proc, and notitle_exec.proc.
3. Update your WebTools configuration xml file with details for the template file and processor file to be used.
4. Determine where your new tool menu item appears in the existing menu hierarchy on the Network Manager GUI server.
   a. Within /space/IBM/netcool/gui/precision_gui/profile/etc/tnm/tools create the WebTools tool definition file, for example MyNewScriptTool.xml. Within the new tool definition file, supply the parameters to run the tool, as defined by the WebTools configuration file in the Network Manager backend server, for example the ncp_webtool.cgi configuration file.
   b. Within /space/IBM/netcool/gui/precision_gui/profile/etc/tnm/menus modify the GUI menu definition file, for example MyNewTool.xml.

Results

The WebTools engine takes the new list of commands and uses the default IBM code and scripts to get the information.

Changing the output of a WebTools tool

The `itnmadmin` user can change the output options for a WebTool tool.

About this task

After the `itnmadmin` user configures a new WebTool tool, or determines a change is needed to the output for an existing WebTools tool, the `itnmadmin` can configure the output options of the tool. The `itnmadmin` user must complete the following steps to configure the output options of a WebTool tool.

Procedure

1. Create a set of definition files for the WebTools tool. There is one set of definition files per tool, which consists of a template file that acts as a wrapper, and a processor file. The template file and processor file govern output, format, and content.
   - Create a template file within `$NCHOME/core/precision/scripts/webtools/etc/templates/`.
   - Create a processor file within `$NCHOME/core/precision/scripts/webtools/etc/processors/`.
2. Within the `.xml` configuration files for the WebTools tool, remove references to older definition files and add references to the new definition files.

Creating tools for context menus

You can create tools for operators to use and add them to context menus on a network map.

Related concepts

About tools

Tools are defined in XML files in the `$NMGUI_HOME/profile/etc/tnm/tools/` directory. You can associate URL tools with a menu option.

Adding reports to context menus

You can add existing reports to context menus. Operators can run the reports from devices in any network map.

About this task

There are several reports available by in the context menu by default. You can add additional reports to the context menu.

To add a report to a context menu, complete the following steps.

Procedure

1. On the server where the Dashboard Application Services Hub is installed, create or edit a tool definition XML file in the following directory:

   `$NMGUI_HOME/profile/etc/tnm/tools/`. Create a separate file for each menu item and give each file a meaningful name.
2. In the tool definition file, define the parameters for the report. Some parameters, such as the domain and entity name, are retrieved from the environment and embedded in the report URL. Default values are used for report parameters that are not defined. If no default values exist, you are prompted for a value.

   The following example tool definition defines a tool called ifInDiscards, which launches a generic trend analysis report using the poll policy ifInDiscards.

```
<?xml version="1.0"?>
<ncp_tool id="ncp_ifindiscards_report" key="ncp_ifindiscards_report" label="IfInDiscards
```

```
Report" type="url">
        <url value="../../../tarf/servlet/component" target="_blank"
windowFeatures="ScrollBars=yes,
Resizable=yes,Width=1280,Height=1024" method="GET">
        <parameter name="b_action" valueType="text" text="cognosViewer"/>
        <parameter name="ui.action" valueType="text" text="run"/>
        <parameter name="ui.object" valueType="text" text="/content/package[@name='Network
Manager']
/folder[@name='Performance Reports']/report[@name='Generic Trend Analysis']"/>
        <parameter name="ui.name" valueType="text" text="ifInDiscards Usage"/>
        <parameter name="run.outputFormat" valueType="text" text="HTML"/>
        <parameter name="run.prompt" valueType="text" text="false"/>

        <parameter name="p_Domain" valueType="domainName" />
        <parameter name="p_PollDefinition" valueType="text" text="ifInDiscards"/>
        <parameter name="p_Hostname" valueType="ncim" table="entityData" column="entityName"
runOnMainNode="true"/>

  </url>
</ncp_tool>
```

3. Edit the file $NMGUI_HOME/profile/etc/tnm/menus/ncp_reports.xml and add a menu entry that references the tool definition file.
   The following example defines context menu options for several reports, including the ncp_ifindiscards_report defined in the previous example, under a menu titled **Reports**.

```
<ncp_menu id="ncp_reports_menu" key="ncp_reports_menu" label="Reports">
    <definition>
        <tool id="ncp_bandwidth_in_report"/>
        <tool id="ncp_bandwidth_out_report"/>
        <tool id="ncp_availability_report"/>
        <tool id="ncp_ifindiscards_report"/>
        <tool id="ncp_memory_usage_report"/>
        <tool id="ncp_cpu_usage_report"/>
        <tool id="ncp_cisco_device_dashboard"/>
        <tool id="ncp_monitored_policies_report"/>
    </definition>
</ncp_menu>
```

What to do next

You can define which reports are available to run on which kinds of devices by using context filters.

URL tools

A URL tool opens a new browser window and applies a specified URL.

Examples of URL tools that you can configure to extend the right-click tools include the following:

- Third-party applications.
- Custom CGI scripts.
- Web sites: Use an absolute URL, for example http://www.any_company.com.

URL tools are defined in an XML file that is located in the $NMGUI_HOME/profile/etc/tnm/tools/ directory.

You can specify the features of the window in which the tool opens. You can specify window features either by specifying the most common features using a parameter per feature, or by specifying any feature using a common parameter.

Example

The following example shows a URL tool that traces a route from the server to a selected device or component, and shows the format of the XML file used to define the URL tool. Elements and attributes are highlighted in bold for explanatory purposes only.

```
<ncp_tool id="server_traceroute" label="Trace route from server" type="url" runforeach="false"
runonlist="true"
```

```
key="key">
<url value="/webtop/cgi-bin/traceroute.cgi" target="_blank">
<parameter name="host" valueType="ncim" table="chassis" column="accessIPaddress" runOnMainNode="true"/>
</url>
<context>
<!-- This section of the xml file is a context filter. -->
<!-- Context filters specify the device and view conditions -->
<!-- under which this tool is displayed.-->
</context>
<security>
<!-- This section of the xml file is a security filter. -->
<!-- Security filters specify the users, roles and groups -->
<!-- authorized to display this tool. -->
</security>
</ncp_tool>
```

Sample URL tool

Use this example information to understand the XML attributes and elements that are used to define a URL tool.

The following XML code shows the use of the `parameter` attribute.

```
<ncp_tool id="url_tool_id" label="My URL Tool" type="url"
<url value="/mytool/doSomething.do" target="_blank">
<parameter name="domain" valueType="domainName"/>
<parameter name="webtopds" valueType="webtopDataSource"/>
<parameter name="host" valueType="ncim" table="chassis"
column="accessIPaddress" runOnMainNode="true"/>
<parameter name="retries" valueType="text" text="3"/>
<parameter name="userId" valueType="cookie" cookieName="userId"/>
</url>
<context>
……
</context>
<security>
……
</security>
</ncp_tool>
```

This example, when executed against a device, produces a URL that has the following form:

`https://server:`*`port`*`/ibm/console/mytool/doSomething.do?`
`domain=NCOMS&webtopDataSource=NCOMS&host=1.2.3.4&retries=3&userId=fred`

Sample Window features for URL tools

Use these examples to help you specify the features of the window in which a URL tool opens.

In the following examples, attributes are highlighted in **bold** for explanatory purposes only.

Example 1

The following example shows how to specify the most common features using a parameter per feature.

```
<ncp_tool id="url_tool_id" label="My URL Tool" type="url"
<url value="/mytool/doSomething.do" target="_blank" width="500" height="500"
status="no" resizable="no">
</url>
……
</ncp_tool>
```

Example 2

The following example shows how to specify any window feature using a common `windowFeatures` parameter.

```
<ncp_tool id="url_tool_id" label="My URL Tool" type="url"
<url value="/mytool/doSomething.do" target="_blank" windowFeatures="width=500,
height=500, menubar=no, toolbar=no,
location=no, status=no, resizable=no">
</url>
```

```
.....
</ncp_tool>
```

Adding CGI scripts to context menus

To make additional tools available when network operators right-click a device, extend the context menu to include a custom CGI script. User-defined tools are accessed by right-clicking a device.

About this task

Restriction: You cannot launch a user-defined tool on a device of type `Subnet`.

You must store all CGI scripts in `NCHOME/omnibus_webgui/etc/cgi-bin`

You must register CGI tools in the Tivoli Netcool/OMNIbus Web GUI.

CGI script parameters

When you write a CGI script for use in an extended context menu, you must use the script parameters to reference the device from which the script is called.

To reference the device, use the following fixed parameters, which are automatically passed to user-defined scripts by TopoViz.

Attention: The parameters are provided only when no parameters are specified in the URL tool definition. Otherwise, the parameters passed to the CGI script are as specified in the tool.

$selected_rows.ServerName
This value defines the name of the ObjectServer that corresponds to the current Network Manager domain. This value is defined in the `ncp.domains` table when the topology database is created.

$selected_rows.NmosObjInst
This value is a unique identifier for the device. It is equivalent to the ObjectId field in the mainNodeDetails table of the topology database.

$selected_rows.Node
This value is from the ObjectServer. The value is usually equivalent to the IpAddress field in the mainNodeDetails table of the topology database.

These values refer to the device that was selected when the context menu was used. Topoviz uses an HTTP `Get` request to call the script and passes the above parameters in the URL. The URL is encoded into x-www-form-urlencoded format. Non-alphanumeric characters are converted into the 3-character string *%xy*, where *xy* is the two digit hexadecimal representation of the lower 8-bits of the character.

Example

If a script named `traceroute.cgi` is run on the host `192.168.21.35`, and the script is passed the following variables:

- *ServerName=Primary_01*
- *NmosObjInst=1477*
- *Node=192.168.0.7*

A new browser window is opened with the following URL:

```
https://192.168.21.35:16316/ibm/console/webtop/cgi-bin/traceroute.cgi?
%24selected_rows.ServerName%3DPrimary_01%26%24selected_rows.NmosObjInst
%3D1477%26%24selected_rows.Node%3D192.168.0.7
```

Registering tools in the Tivoli Netcool/OMNIbus Web GUI

After you have created the CGI script, and defined the appropriate tool, you must register the tool in the Web GUI so that you can use the tool in Topoviz.

About this task

The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below. Registering your tool makes it available in Topoviz only.

From the **CGI Registration** window you can configure settings and properties for the tool. See the *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide* for more details.

To register a tool in the Web GUI:

Procedure

1. Click **Content**. From the **Menus & Tools** list, select **CGI Registration** > **Register**.
   The **CGI Registration** page is displayed.
2. Type the name of the tool and the file name of the script.

What to do next

To make the tool available in the Web GUI, you must add the tool to the main Web GUI client.

Making tools available in the Tivoli Netcool/OMNIbus Web GUI

In addition to registering the tool in the Web GUI, you must also make the tool available in the main Web GUI client.

About this task

The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below.

From the **Tools Editor** window you can configure settings and properties for the tool. See the *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide* for more details.

To create a tool in the Web GUI:

Procedure

1. Click the **Content** tab. From the **Menus & Tools** list, select **Tools**.
   The **Tools Editor** page is displayed.
2. Click **Create**.
   The **Create New Tool** page is displayed.
3. Type the name and type of the tool.

Configuring the Show Connectivity Information tool

You can specify which interface types to display when the **Show Connectivity Information** tool is run on a device in **Network Hop View** or **Network Views**. You can also change what information is displayed for interfaces.

Before you begin

If you want to change the interface types that are displayed, you must know the IDs for the interface types. You can determine the interface type IDs by running the following SQL query on the NCIM topology database.

```
SELECT * FROM ncim.enumerations where enumGroup = 'ifType';
```

About this task

The **Show Connectivity Information** tool displays a table of devices and interfaces that are connected to a selected device.

Procedure

1. Configure which interface types are displayed.

   By default, all interface types on the selected device are included.

   a) Open the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` configuration file.

   b) Include interface types by typing a line similar to the following example anywhere in the `topoviz.properties` file.

   ```
   topoviz.connectivity.includes=2,36
   ```

   In this example, the **Show Connectivity Information** tool displays interface types 2 and 36 only.

   c) Exclude interface types by typing a line similar to the following example anywhere in the `topoviz.properties` file.

   ```
   topoviz.connectivity.excludes=1
   ```

   In this example, the **Show Connectivity Information** tool displays all interface types except for interface type 1.

   d) Specify interface types to display in the **Show Connectivity Information** tool by either including interface types or excluding interface types.

   Note: You must not use both includes and excludes parameters in the `topoviz.properties` file. Doing so might produce unexpected results in the **Show Connectivity Information** tool.

   e) Save and close the `topoviz.properties` file.

2. Configure which columns are displayed.

   By default, these columns are displayed: `ifDescr`, `ifType`, and `ifTypeString`.

   a) Back up and edit the `$NMGUI_HOME/profile/etc/tnm/ncimMetaData.xml` file.

   b) Locate the following section.

   ```
   <columnView tableMode="showconnecttable">
               <columnName tableAlias="n" column="ifDescr"/>
               <columnName tableAlias="n" column="ifType"/>
               <columnName tableAlias="n" column="ifTypeString"/>
           </columnView>
   ```

   c) Add or remove the columns that you want to display.

   You can use any columns from the `networkInterface` entity attribute table.

   d) Save and close the `$NMGUI_HOME/profile/etc/tnm/` file.

Creating tools that open the MIB browser

To provide additional diagnostic information for network operators, create custom tools that open the MIB browser from an **Event Viewer** or from a topology map, and display information in the MIB browser.

About this task

For example, you can create a tool that opens the MIB browser in an **Event Viewer**, performs an SNMP Walk query on all the interfaces of the affected device, and automatically displays this interface MIB data in the MIB browser.

MIB browser modes

Custom tools can open the MIB browser in one of two modes, *full mode* or *results-only mode*.

Full mode
The complete MIB browser page is displayed, with the MIB tree, **MIB Variable Information panel**, and the **SNMP Query Results** panels

Results-only mode
The results of the MIB browser query are displayed in the **SNMP Query Results** panel, as a single page.

Creating a custom tool

To provide additional information for network operators from an **Event Viewer** or topology map, create a custom tool that displays information in the MIB browser.

Procedure

1. Decide which data you want the MIB browser to display, and how you want the MIB browser to display the data.
2. Determine the URL that opens the MIB browser with the required content and format.

   The URL must have the following format:

   ```
   https://host:port/ibm/console/ncp_mibbrowser/Launch.do
   ```

   Where:

   - *host* is the IP address of the host on which the Dashboard Application Services Hubserver is running.
   - *port* is the port to access on the host. The default value is 16316.

   A URL in this format starts the MIB browser with the `Domain` option set to the first value in the list, and with no **Host** or **Value** options set in the **SNMP Query** toolbar.
3. Write a CGI script that constructs the URL in response to a right-click in an **Event Viewer** or in a topology map.
4. To define and store the tool for use in Topoviz, register the tool in the Tivoli Netcool/OMNIbus Web GUI. The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below.
5. To define and store the tool for use in the Web GUI, create the tool in the Web GUI.
6. To make the tool available as a right-click option in a context menu, create a menu entry in the Web GUI.

Optional parameters for MIB browser URLs

When you define a URL that starts the MIB browser, you can supply a number of additional optional parameters.

domain
The name of the IBM Tivoli Network Manager IP Edition domain to use to obtain the MIB and SNMP data. The value of this parameter is used to set the **Domain** option menu in the **Configuration Toolbar**.

Tip: To write a tool that opens the MIB browser from an **Event Viewer**, you can specify the name of the ObjectServer instead of the IBM Tivoli Network Manager IP Edition. To do this, specify the parameter $selected_rows.*ServerName* where *ServerName* is the field in the **Event Viewer** event that specifies the name of the ObjectServer.

host
The IP address of the target device to be queried for SNMP data. This value is used to populate the **Host** field in the **SNMP Query Toolbar**.

variable
The MIB object to query. This value can be the OID of the MIB object, for example 1.3.6.1.2.1.1.3 or it can be the name of the MIB object, for example sysUpTime. This value is used to populate the **OID** field in the **SNMP Query Toolbar**.

resultsOnly
Specifies whether the MIB browser is started in full mode or results-only mode. Specify one of the following options:

- `true`: The MIB browser opens in results-only mode.
- `false`: The MIB browser is opened in full mode.

If you supply the `domain`, `host`, and `variable` parameters, the MIB browser is started, automatically performs the SNMP query specified by these parameters and displays the results in the **SNMP Query Results** area. The type of SNMP query varies depending on the value of the variable parameter

XML elements and attributes for defining tools

Use these XML elements and attributes to define URL tools and tools that open reports.

The following table describes the XML elements and attributes used to define URL tools and tools that open reports.

Table 26. Elements and Attributes used to define URL tools and tools that open reports

Element or attribute	Type	Description
`context`	Attribute	Specifies the context filters for the tool.
excludeBaseContext	Attribute	Determines if the default base context should be excluded, but retains the protocol server port portion of the base URI. For example, to exclude the `/ibm/console` from the base URI, set the value to `true`. The default value is `false`.
excludeBaseURI	Attribute	Determines if the default base URI should be excluded, which includes everything up to and including `https://server:port/ibm/console`. The default value is `false`.
`id`	Attribute	Contains an alphanumeric identifier for this tool.
key	Attribute	Used as a lookup into the `$NMGUI_HOME/profile/etc/tnm/locale/ncp_tools(_xx_XX).properties` file. This attribute allows you to specify translations of the tool label for users with different locale settings.

Table 26. Elements and Attributes used to define URL tools and tools that open reports (continued)

Element or attribute	Type	Description
`label`	Attribute	Contains the actual text of the menu option for this tool that appears in the menu.
`name`	Attribute	Specify a name to be used for the parameter.
`ncp_tool`	Element	Introduces the definition of a tool.
`omitDefault Parameters`	Attribute	As an attribute of the `<url>` element, prevents any default parameters from being added to the URL if it is set to `true`. Set this attribute to true if your tool has no `<parameter>` tags and you do not want any default parameters added. If your tools has some `<parameter>` tags, this attribute has no effect.
Fix Pack 9 `omitDuplicateP arameterValues`	Attribute	If set to `true` as an attribute of the `url` element, omits duplicate parameters from the URL. When a right-click tool is launched from a selection of multiple devices, each device can contribute the same parameters to the URL. If these parameters have the same value, they can be removed by enabling this feature. Removing duplicate parameters can make very long URLs shorter. If you change this attribute, log out of the GUI and log back in again to see the change. If you do not see the change, restart the Dashboard Application Services Hub. If the `omitDuplicateParameterValues` element is not specified, it defaults to `false`. To change the default to `true`, set `tnm.tools.menu.omit.duplicate.parameter.values.default` to `true` in the `tnm.properties` file.
`parameter`	Element	Specifies parameters to pass to the URL. You can configure multiple parameters using the following parameter types. Each of these parameter types is formulated using a different `valueType` attribute: • Value of an NCIM topology database field. The data retrieved must be associated with an entity. • Name of the Network Manager domain containing the device or devices against which the tool is executing. • Name of the Tivoli Netcool/OMNIbus Web GUI data source mapped to the Network Manager domain containing the device or devices against which the tool is executing. • Value of a Web browser cookie. • Plain text. Use this parameter type to specify tool-specific parameters, such as the number of hops to pass to the tool that launches the Hop View, or the number of retries.
`runforeach`	Attribute	If set to the value `true`, then this tool is run once for each selected node.
`runonlist`	Attribute	If set to the value `true`, then this tool is run once only. The selected nodes are passed to the tool as a comma-separated list.
`security`	Attribute	Specified the security filters for the tool.

Table 26. Elements and Attributes used to define URL tools and tools that open reports (continued)		
Element or attribute	**Type**	**Description**
`type`	Attribute	The following types of tool are supported: • `url`: use this option to define a URL tool.
`target`	Attribute	This attribute is standard HTML syntax and specifies the name of the window to open the tool into. Possible values include: • `_blank`: Opens the tool in a new window • `_self`: Opens the tool in the current window You can also specify a window name.
`url`	Element	Specifies the URL to open when a user selects this tool.
`value`	Attribute	Specifies the value of the URL for the <url> element. You can use variables here that you have defined in the `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file. For example, you could reference two variables called tnm.myserveraddress and tnm.myserverport using a URL similar to the following: `url="https://{%prop:tnm.myserveraddress}:{%prop:tnm.myserverport}/rest_of_url"`
`valueType`	Attribute	Indicates how the Network Manager Web application from which the tool is called obtains the value of the parameter. This attribute can take the following values: • `domainName`: obtains the name of the Network Manager domain containing the device or devices against which the tool is executing. • `webtopDataSource`: obtains the name of the Tivoli Netcool/OMNIbus Web GUI data source mapped to the Network Manager domain containing the device or devices against which the tool is executing. • `ncim`: retrieves the value of a field in the NCIM topology database. Use the `table` and `column` parameters to specify the topology database field. Set the `runOnMainNode` attribute to `true` in order to use the `entityId` field associated with the main node containing a selected interface. • `cookie`: obtains the value of the cookie specified using the `cookieName` attribute. • `text`: specified text attribute is added as a parameter value.

Defining context filters for tools and menus

You can specify the types of views in which a menu or tool is available, and which devices it can be run on, using context filters.

About this task

To define a context filter for a menu or tool, complete the following steps.

Procedure

1. Edit the XML file in the $NMGUI_HOME/profile/etc/tnm/menus/ directory that defines the menu or tool to which you want to apply the filter.
2. Optional: Edit the <context> element to define the filter. Use the reference information about the XML elements and attributes available for context filters and the example provided to help you define the context filter. If the <context> element is not used, the tool or menu is available for all devices, subject to any restrictions imposed by the optional security element.

Related concepts

About filters

Filters are pieces of XML code that form part of an XML menu definition or an XML tool definition. There are two types of filter: *context filters* and *security filters*.

XML attributes for defining context filters

Understand the different XML elements and attributes that define context filters.

Sample context filter

The following example shows the format of a context filter:

```
<context>
        <attribute id="class">
                <matches regexp=".*Cisco*"/>
        </attribute>
        <attribute id="clientType">
                <equals value="ncp_networkview"/>
        </attribute>
        <attribute id="managed">
        </attribute>
        <attribute id="entityType">
                <equals value="1"/>
        </attribute>
        <attribute id="viewType">
                <equals value="1"/>
        </attribute>
        <attribute id="{%prop:status.view.enabled}">
                <equals value="true" />
        </attribute>
</context>
```

If the menu is to be displayed, the context must match each of the id attributes. In this example, the tool or menu is displayed only in filtered (viewType = "1") Network Views, only when device status is configured to be displayed, and can be run only against managed, main node devices.

XML attributes of a context filter

The following table describes the XML elements, attributes, and operators available for the definition of a context filter.

Table 27. Elements, attributes, and operators in the context filter XML definition section

Element or Attribute	Description

{%prop:*property*}	This element displays the menu item based on the given property in a properties file.
	For example, the following definition displays the menu item if the value of the status.view.enabled property is true. If the value is false, the menu item is hidden.
	`<attribute id="{%prop:status.view.enabled}">`
	`<equals value="true" />`
	`</attribute>`

Table 27. Elements, attributes, and operators in the context filter XML definition section (continued)	
Element or Attribute	**Description**
`childViewType`	The childViewType attribute filters for a view type, where the selected view is contained within another view. Possible values are: • 0 - Container • 1 - Filtered • 2 - Collection • 3 - MPLS VPN • 4 - IP Filter • 5 - Unassigned • 6 - Custom • 7 - VPLS VPN • 8 - Dependency • 100 - Dynamic Collection • 101 - Dynamic Subnet • 102 - Dynamic MPLS VPN • 103 - Dynamic Distinct • 104 - Dynamic Template • 107 - Dynamic MPLS VPN
`class`	Corresponds to the `ClassName` of the device on which the right-click is performed
`clientType`	Web application from which the tool may be run. Possible values are: • `ncp_hopview` • `ncp_networkview` • `ncp_structurebrowser`
`entityType`	The type of device (`entityType`) that the tool can be run against.
`equals`	Performs a simple = comparison between attributes
`managed`	Indicates whether the tool can only be run against devices that are in the managed state. Possible values are: • `true` • `false`
`matches`	Performs a regular expression comparison between attributes
`notequals`	Performs a simple `not=` comparison between attributes

Table 27. Elements, attributes, and operators in the context filter XML definition section (continued)	
Element or Attribute	**Description**
`viewType`	Defines the type of view in which the tool can appear and be used. Refers to the view that contains the selected device. Possible values are: • 0 - Container • 1 - Filtered • 2 - Collection • 3 - MPLS VPN • 4 - IP Filter • 5 - Unassigned • 6 - Custom • 7 - VPLS VPN • 8 - Dependency • 100 - Dynamic Collection • 101 - Dynamic Subnet • 102 - Dynamic MPLS VPN • 103 - Dynamic Distinct • 104 - Dynamic Template • 107 - Dynamic MPLS VPN

Defining user access for tools and menus

You can specify the users, roles, and groups authorized to display a tool or menu using security filters.

About this task

To define a security filter for a tool or menu, complete the following steps.

Procedure

1. Edit the XML file in the `$NMGUI_HOME/profile/etc/tnm/menus/` directory that defines the menu or tool to which you want to apply the filter.
2. Edit the `<security>` element to define the filter. Use the reference information about the XML elements and attributes available for security filters and the example provided to help you define the security filter.

Related concepts

About filters

Filters are pieces of XML code that form part of an XML menu definition or an XML tool definition. There are two types of filter: *context filters* and *security filters*.

XML attributes for defining security filters

Understand the different XML attributes of the `<security>` element that define security filters.

Example

The following example shows a security filter:

```
<security>
        <user name="bob"/>
        <user name="mary"/>
        <group name="Network Manager IP Desktop"/>
        <role name="ncp_networkview"/>
</security>
```

If the menu or tool is to be displayed, the context must match at least one of the following attribute assignments:

- User bob
- User `mary`
- Any user with the role `ncp_networkview`
- Any user in the group `Network Manager IP Desktop`

Elements and attributes of a security filter

The following table describes the XML elements, attributes, and operators available for the definition of a security filter.

Table 28. Elements, attributes, and operators in the security filter XML definition section

Element or attribute	Type	Description
`user`	Attribute	Assigns the tool or menu to a specific user
`group`	Attribute	Assigns the tool or menu to a specific group
`role`	Attribute	Assigns the tool or menu to a specific role

Defining variables for tools

You can define variables for use in tools in the `tnm.properties` file.

About this task

If you want to use variables in tools and do not want to hardcode them in each tool, you can define them in the `tnm.properties` file. You can reference the variables in any tool definition.

For example, right-click tools that launch into other applications must be configured with the server and port details of the application.

To define variables for use in tools, complete the following steps:

Procedure

1. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file.
2. Add or edit an entry similar to the following example:

```
tnm.bhm.server=myserver.mydomain.com
tnm.bhm.port=40443
```

Note: Variables must begin with the string `tnm.` in the `tnm.properties` file.

3. In the tool definition XML file, reference these variables as in the following example:

```
url="https://{%prop:tnm.bhm.server}:{%prop:tnm.bhm.port}/rest_of_url"
```

Chapter 10. Editing network topology

Edit the discovered network topology to manually add and remove devices and connections.

About topology editing

You can edit the discovered network topology by performing the following actions: adding network devices, adding connections between network devices, removing and deleting devices from the domain, and removing connections between network devices. The topology can only be edited in the **Network Hop View**.

For information on how to configure the **Network Hop View** to differentiate between manually added network devices and discovered network devices, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Topology editing and the discovery process

Following a discovery, the Topology manager, ncp_model, inspects relevant tables in the NCIM topology database to determine which manual topology changes were made, and then makes sure not to overwrite those manual changes.

All manual changes to the topology are recorded in the NCIM topology database entityActions and connectActions tables.

For information on how to examine the audit log for manually added devices and connections, see the description of the `entityActions` and `connectActions` tables in the *IBM Tivoli Network Manager Reference*.

Audit trail of manual changes to the topology

All manual changes to the topology will be recorded in the NCIM topology database entityActions and connectActions tables. These tables facilitate an audit trail for manual topology changes as well as allow for the undo or reversal of a manual action.

For information on how to examine the audit log for manually added devices and connections, see the description of the `entityActions` and `connectActions` tables in the *IBM Tivoli Network Manager Reference*.

Adding devices to the topology

You can manually add main node device entities to the discovered network topology. You might want to do this because there is no access to a specific network device, or because device support (discovery agents) is not available for certain device types.

About this task

You use the Add Device Wizard to manually add a device to the topology. This wizard updates the NCIM topology database entityData, chassis, and ipEndPoint tables. For more information on these NCIM topology database tables, see the *IBM Tivoli Network Manager Reference*.

Note: Devices that are added manually can be displayed in the Network Views. Go to **Network Availability** > **Network Views** and select **Manually Added Devices** from the Network View tree.

To launch the wizard, complete these steps.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.

2. Ensure that the topology map displayed contains at least one of the devices to which you want to add a connection. For information about how to display a topology map in the **Network Hop View**, see the *IBM Tivoli Network Manager User Guide*.
3. In the **Network Hop View**, right-click a device or the background area of the topology map, and click **Topology Management** > **Add Device**.

   The Add Device Wizard **Entity Details** window opens.
4. Complete the **Entity Details** window as follows. The fields in this window populate the NCIM entityData table for the device that you are adding.

   domain
   The domain to which the device is being added. This value is retrieved from the domain of the Hop View from which the Add Device Wizard was launched.

   entityName
   IP address or DNS name for this device. For example, an IP address such as 172.20.1.7, or a DNS name, such as company-abc.net.

   Restriction: Fix Pack 2 Device names can include square brackets `[]` in the device name, but not at the end of the device name.

   Restriction: This name must be unique for all entities within the current domain. If a device with the same entity name already exists in this domain then the wizard requires you to specify a different entity name. This applies whether the device is manually added or discovered. In this case, do one of the following:

   - Enter a different entity name.
   - Cancel the wizard, and select a different domain. Try to add the device to this new domain, by going back to step 2 of this procedure.

   entityType
   Type of entity. This value is set to chassis. This means that you can only add a chassis, or main node device.

   displayLabel
   Label to display for this device in a network view or network hop view.

   description
   Textual description of this device

   reason
   Reason for adding this device to the topology.
5. Click **Next**. Complete the **Chassis Details** window as follows. The fields in this window populate the NCIM chassis table for the device that you are adding.

   className

   The name of a class of devices. The master className field is in the entityClass table.

   If you specified **className** then this field lists the classes available in the NCIM database entityClass table. Select a class from this list to classify the device.

   sysObjectId

   The vendor's authoritative identification of the network management subsystem contained in the entity.

   If you specified **sysObjectId** then type a valid sysObjectId value for this device.

   sysName

   An administratively-assigned name for this managed node. By convention, this is the fully-qualified domain name of the node. If the name is unknown, the value is the zero-length string.

   sysDescr

   A textual description of the entity. This value must include the full name and version identification of the system hardware type, software operating-system, and networking software.

sysLocation

The physical location of this node, for example "telephone closet, 3rd floor." If the location is unknown, the value is the zero-length string.

sysContact

The textual identification of the contact person for this managed node, and information on how to contact this person. If no contact information is known, the value is the zero-length string.

ipForwarding

Indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by this entity but not addressed to this entity. IP gateways forward datagrams, whereas IP hosts do not, unless the source is routed through the host. Takes one of the following values:

- forwarding
- not-forwarding

serialNumber

The serial number of the entity.

modelName

The model name of the entity.

accessIPAddress

The IP address through which this entity was discovered and will be monitored.

Note: For non-IP entities, such as layer 1 optical devices, this field is null.

If you specify a value for **accessIPAddress** then you must also specify a value for **accessProtocol**. The value specified for **accessIPAddress** must be valid within the Internet protocol specified for **accessProtocol**. For example, if you set **accessProtocol** to IPv4, then you must specify an IPv4 address.

accessProtocol
The Internet protocol used by the chassis. If you specify a value for **accessProtocol** then you must also specify a value for **accessIPAddress**.

DNSName
DNS name for the IP address associated with this IP end point. The value specified in this field is used to populate the NCIM ipEndPoint table for the device that you are adding.

Note: The DNSName field in the NCIM ipEndPoint table is only updated if you have specified a value for both the **accessProtocol** and **accessIPAddress** fields in this window.

6. Click **Next**.

   The Add Device Wizard checks the chassis details entered.

   - If no errors are returned, then the **Confirm Details** window opens.
   - If there are any errors, then you are prompted to correct them before proceeding.

7. In the **Confirm Details** window, review the information that you specified and click **Finish**.

   The Add Device Wizard checks the entity details entered.

   If the operation was successful then a window opens indicating that the device was successfully added to the domain. Click **Add Like** option to add more devices with identical data except for the **entityName** and **displayName** fields. The topology map in the **Network Hop View** is updated to display the newly added device.

   Note: If the **Network Hop View** is refreshed before a connection is added to the manually added device, then the manually added device will disappear from the network hop view as it has no connections.

Adding connections between devices

You can manually add connections between devices in the discovered network topology. You can add these connections between manually added devices or between discovered devices or between a mix of the two. This enables you to add connections that the Discovery engine was unable to discover.

About this task

You use the Add Connection Wizard to manually add a connections between devices. All connections added are stored in the NCIM topology database as bidirectional.

To launch the wizard, complete these steps.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. Ensure that the displayed topology map contains at least one of the devices to which you want to add a connection. For information on how to display a topology map in the **Network Hop View**, see the *IBM Tivoli Network Manager User Guide*.
3. In the **Network Hop View**, select one device or two devices. Then right-click to display the context menu and click **Topology Management** > **Add Connection.** from the context menu.

   Based on your device selections, you can perform one of the following actions:

   You selected one device
   You can connect this device to a device that is not displayed in the current hop view.

   You selected two devices
   You can connect these two devices to each other.

   Note: If you select more than two devices then the **Topology Management** > **Add Connection.** option is not available in the context menu.

   The Add Connection Wizard **Device Selection** window opens.
4. Complete the **Device Selection** window as follows.

   The fields in this window populate the NCIM connects table for the connection that you are adding.

   From Device
   IP address of the device that is the notional start of the connection.

   To Device
   IP address of the device that is the notional end of the connection. If you selected one device only then this field contains the text **<Click Next to select device>**.

   Swap Devices
   Allows you to switch the notional start and notional end of the connection.
5. Click **Next**.

   The next window displayed depends upon whether you initially selected one or two devices in the **Network Hop View**.

   - If you selected one device, then the **Entity Search** window opens. Use the **Entity Search** window to locate the **To Device**, the device at the notional end of the connection.
   - If you selected two devices then the **Connection Details** window opens. Go to Step "7" on page 251
6. Complete the **Entity Search** window as follows.
   - Use the **Basic** tab to search by IP address or device name.

     Domain
     Select the domain in which you want to search.

     Note: If you opened the Entity Search window from the Path Views GUI, then you cannot change domain. This is done to prevent cross-domain path traces.

IP Address
Specify the IP address of the device. You can specify all of the address, or only the first part of the address. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets.

Device Name
Specify the name of the device. You can specify all of the name, or only the first part of the name. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets. Device names are not case-sensitive. If you specify both an IP address and a device name, the IP address takes precedence.

- Use the **Advanced** tab to search by device attributes.

  Domain
  Select the domain in which you want to search.

  Note: If you opened the Entity Search window from the Path Views GUI, then you cannot change domain. This is done to prevent cross-domain path traces.

  Table
  Select the database table that you want to search. The mainNodeDetails table lists network devices.

  Field
  Select the field whose value you want to search. The selection available for this field is automatically populated based on the chosen database.

  Comparator
  Select a comparator.

  Value
  Required. Type the value that you want to search for. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets.

7. Complete the **Connection Details** window as follows.

From Device
IP address of the device that is the notional start of the connection.

From Interface
If interfaces exist on this device, then these are presented in the **From Interface** list. If an interface list exists, then you can make the connection at the interface or device level for this device.

To Device
IP address of the device that is the notional end of the connection. If you selected one device only then this field contains the text **<Click Next to select device>**.

To Interface
If interfaces exist on this device, then these are presented in the **To Interface** list. If an interface list exists, then you can make the connection at the interface or device level for this device.

Connectivity
Defaults to the connectivity setting in the **Network Hop View**.

Note: If the topology map in the **Network Hop View** is set to IP Subnets then the **Connectivity** setting in this window defaults to Layer 2, the first item in the list.

Speed
The speed for this connection. This must be an integer value.

Reason
Reason for adding this connection to the topology.

8. Click **Next**.

   The **Confirm Details** window is displayed.
9. Review the information that you specified and click **Finish**.

   The Add Connection Wizard checks that a connection between the specified interfaces on the two devices does not already exist. If such a connection already exists, then a screen is displayed indicating that the wizard is unable to create this connection.
10. If one of the following conditions holds, then the **Success** window requires you to recenter the topology map before you can display the new connection. Click **Recenter & Close** to do this.
    - Neither of the devices selected for connection were seed devices in the original network hop view and one of the selected devices was not on the current network hop view.
    - The connectivity specified for the connection is not the same as the connectivity on the original network hop view.

Deleting manually added devices

You can delete manually added devices from the topology. This action completely removes all data associated with the deleted devices from the NCIM topology database.

About this task

You use the Delete Device Wizard to delete manually added devices from the topology. All data associated with the manually added device is removed from the NCIM topology database.

Note: If you want to remove a discovered device from the domain, you must use the RemoveNode.pl script. For more information on the RemoveNode.pl script, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Complete the following steps to launch the wizard and delete manually added devices from the topology.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. Within the **Network Hop View**, display a topology map.

   The displayed topology map must contain at least one of the devices which you want to delete. For information on how to display a topology map in the **Network Hop View**, see the *IBM Tivoli Network Manager User Guide*.
3. In the **Network Hop View**, select one or more manually added devices to delete. Then right-click to display the context menu and click **Topology Management** > **Delete Device** from the context menu.

   Note: You can distinguish manually added devices from discovered devices by noting which devices have the associated manually added device icon  .

   The Delete Device Wizard **Device Selection** window opens.
4. Complete the **Device Selection** window as follows.

   Please select the devices you would like to permanently delete
   Lists all manually added device selected in the topology map. If you also selected discovered devices, these are ignored and are not shown in this list. You can change the selection here by deselecting devices as required.
5. Click **Next**.

   The **Confirm Device Deletion** window is displayed.
6. Review the information on the **Confirm Device Deletion** window and click **Finish**.

   The **Success** window is displayed indicating that the specified devices have been deleted from the topology.

Removing connections between devices

You can manually remove connections between devices in the network topology.

About this task

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. Ensure the displayed topology map contains the connection that you want to delete. For information on how to display a topology map in the **Network Hop View**, see the *IBM Tivoli Network Manager User Guide*.
3. In the **Network Hop View**, select the connection to remove. Then right-click to display the context menu and click **Topology Management** > **Remove Connection** from the context menu.

   The header at the top of the context menu displays the connection that is selected for removal.

   Note: You can only remove one connection, or one link in a multilink connection, at a time.

   - If the selected connection is made up of multiple links, then you must first click the link you want to remove, and then from the submenu that is displayed, click **Topology Management** > **Remove Connection**.
   - If you selected two or more different connections, then only the first connection that you selected is presented for removal.

   The **Confirm Connection Removal** window opens.
4. Complete the **Device Selection** window as follows.

   Connection
   Displays the device and interface details at either end of the connection. If the connection endpoint at either end is the device itself, then no interface data is shown.

   Layer
   Displays the connection layer for this connection.

   Reason
   Specify a reason for removing these devices from the domain.
5. Click **Confirm**.

   The **Success** window is displayed confirming that the connection has been removed.

Chapter 11. Administering path views

Path views display devices and links that make up a network path between two selected devices. Create new path views or change existing path views to help network operators visualize network paths.

Note: You can only trace a path across a single domain. All devices specified in the **Trace Network Path** window must be in the same domain.

About path views

During the discovery process, system paths such as MPLS TE paths and Virtual Circuits are discovered and displayed as path views. In addition, you can trace IP paths on an ad hoc basis to view a snapshot of a network path at a specific moment. Once saved, you can monitor these paths regularly.

Types of path

Read about the differences between system paths and user-defined paths.

System paths

System paths are MPLS TE paths and Virtual Circuits. These are automatically added during the discovery process and cannot be edited or deleted.

User-defined paths

You can create IP paths from the **Path Views GUI** or from the **Path View Administration GUI**, using the **Trace IPv4 network path** window to define the path trace.

You can also select a device in the **Network Views** , **Network Hop View** , or **Event Viewer**, and launch the **Trace IPv4 network path** window with that device already defined as the start point of a path. If you select two devices before launching the **Trace IPv4 network path** window from these interfaces, the end point will also be populated.

You can specify a device to be included on the path between a start and end device by using the **Via** field, and you also have the option to trace a return path back to you start device. By using the 'ping-verify each hop' option, you can ping each device encountered on the route between two selected devices. This is especially useful in troubleshooting the network path once a failure has occurred.

While paths are usually traced inside a network domain, you can trace a path between an interface inside your domain and one outside, an option that is referred to as an 'out-of-band' trace.

You can retrace user-defined IP paths on demand by selecting the path and pressing the retrace button. The 'elapsed time' column displays the time that has elapsed since the path was last traced.

Note: Network Manager path views also include the concept of a *full path* and a *partial path*.

In some cases, when creating a user-defined path, it is not possible to trace the full path between start and end devices. This can occur when path trace prerequisites are not met; for example, one of the devices along the path might not provide SNMP access. Another reason why it might not be possible to trace the full path is that one of the devices along the path does not provide routing information. If Network Manager is unable to trace a full path, then it will create a partial path made up of a subset of the nodes along the path. Partial paths are highlighted in the **Path View Administration GUI** by means of a warning icon in the **Trace Status** column.

Path trace prerequisites

You run a path trace to generate path views. A path trace can fail because any of the devices involved in the path do not satisfy path trace prerequisites. Use this information to ensure that all path trace prerequisites are met.

Prerequisites

The devices involved in the path must meet the following requirements:

SNMP access

- All devices specified when running the path trace must provide SNMP access so that the path trace operation can access relevant MIB variables in the device. For one-way paths, the source device (specified in the **From** field in the **Trace IPv4 Network Path** window) and the devices along the route (specified in the **Via** field) must allow SNMP access. For return paths, the source device, the devices along the route, *and* the target device (specified in the **To** field) must allow SNMP access.
- All routers identified by the path trace operation as next hop devices along the path must allow SNMP access.

Routing information

- All devices specified when running the path trace must provide basic routing information. For one-way paths, the source device (specified in the **From** field) and the devices along the route (specified in the **Via** field) must at a minimum store information on the next hop device. For return paths, the source device, the devices along the route, *and* the target device (specified in the **To** field) must store information on the next hop device.
- All routers identified by the path trace operation as next hop devices along the path must support the following MIB variables:

  General MIB variables

  - sysName
  - ifName
  - ifType
  - ifConnectorPresent
  - ipAdEntIfIndex

  Routers identified by the path trace operation as next hop devices along the path must, in addition, support either of the following sets of MIB variables that govern routing:

  Classless Inter-Domain Routing (CIDR) MIB variables
  This set of routing variables is made up of the following MIB variables:

  - ipCidrRouteNumber
  - ipCidrRouteIfIndex
  - ipCidrRouteDest
  - ipCidrRouteMask
  - ipCidrRouteType
  - ipCidrRouteMetric1
  - ipCidrRouteNextHop
  - ipCidrRouteProto

  IP route MIB variables
  This set of routing variables is made up of the following MIB variables:

  - ipRouteIfIndex
  - ipRouteDest

- ipRouteMask
- ipRouteType
- ipRouteMetric1
- ipRouteNextHop
- ipRouteProto

Creating path views

To create a path view, launch the **Trace Network Path** window, enter valid devices as start and end points of your path, and then launch the path trace.

Before you begin

Before you can work with network paths, the administrator must have successfully completed the first network discovery, and network views must be configured for your user ID.

About this task

A full list of network paths that have been defined is displayed in the **Path View Administration** and in the **Path Views GUI** windows in list format. From here, you can create new path views. The paths are displayed per user, and the user required can be selected from the drop-down list.

Restriction: Network path monitoring is not available for IPV6 addresses.

Note: You can only create or edit IP path views. MPLS TE paths are populated during discovery and cannot be edited or retraced. MPLS TE paths are displayed by default under the itnmadmin views. This can be altered by editing the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file and changing the values for the following attributes:

- topoviz.pathview.accesslevel
- topoviz.pathview.accessid

Note: You can only trace a path across a single domain. All devices specified in the **Trace Network Path** window must be in the same domain.

You can also create a path view by running the itnm_pathTool.pl Perl script from the command line. For more information, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

To create a path view, complete the following steps.

Procedure

1. Go to one of the following windows.
   a) Click the **Administration** icon and select **Network** > **Path View Administration**.
   b) Click the **Incident** icon and select **Network Availability** > **Path Views**.

   The **Path View Administration GUI** or the **Path Views** GUI opens. Within the **Path View Administration GUI**, all monitored paths display in table format.
2. Click **Create and trace a path** within **Path View Administration** , or click **New Path** within **Path Views**.

   The **Trace Network Path** window displays.
3. In the **Trace Network Path** window, complete the trace criteria fields:

   Domain
   Select a network domain in which to trace a path.

   Name
   Type a name describing the network path. This name is displayed in the tree view of network paths in the **Path View** window, as well as in the table of network paths that are being monitored in the **Path View Administration** window.

Start
Enter the device that will be the start point of the network path to be monitored. Use the **Browse** button to open the **Entity Search** dialog, which helps you to find a device.

End
Enter the device that will be the end point of the network path to be monitored here. Use the **Browse** button to open the **Entity Search** dialog, which helps you to find a device.

Click **Swap** to switch end and start device. As network paths are dynamic, the trace results could be different.

Via
Enter a specific device to be included in the route of the network path to be monitored . Use the **Browse** button to open the **Entity Search** dialog, which helps you to find a device.

Get return path
Select this option to trace the return path as well. As network paths are dynamic, the return path could be different.

When selected, this options runs a trace from your Start device to your End device and back to you Start device. During the trace, the End device is treated as a Via device, and therefore the Via option is unavailable when this option has been specified.

Perform out-of-band trace
Select this option when tracing IP addresses that are utilised for out-of-band access. Selecting this option forces the trace to set the next-hop IP address for a device to the access IP address value stored for this device in the NCIM topology database. Note that specifying this option reduces the accuracy of the tool because the utility does not resolve the next-hop ingress interface and physical port if an out-of-band access IP address is used.

Note: You can only specify an out-of-band **End** device. The **Start** and **Via** devices cannot be outside the domain.

Ping-verify each hop
Select this option to ping each device encountered on the route between two selected devices. You can use this option to troubleshoot the network path once a failure has occurred.

Save and trace
Click this button to save the path view and trace the path between the devices entered. If the trace fails, an error message is displayed.

What to do next

If the path was not successfully traced, then you get a path trace error, indicating the reason that the path could not be traced. To see more detailed path trace output, click the error at the top of the **Trace Network Path** window. Detailed path trace output opens in a second window. To troubleshoot the path trace, refer to the related information on troubleshooting path views.

Troubleshooting path views

If the path was not successfully traced, then you get a path trace error, indicating the reason that the path could not be traced.

About this task

Path trace troubleshooting table

Use this troubleshooting table to determine the type of error that you are encountering and to determine the possible reason for the error and actions to take that might resolve the error.

The following table provides possible reasons and corrective actions for each type of path trace error.

Table 29. Path trace troubleshooting table

Type of error	Possible reason	Possible corrective actions	Example of an error of this type
Internal Network Manager error	Internal database failure.	Switch on path trace debugging and review the logs.	Failed to create a path due to an internal database error. For more details check the log file `$NMGUI_HOME/profile/logs/tnm/ncp_topoviz.X.log`, where *X* is a number such as 1, or 2, and consult documentation on how to turn on further path tool logging.
Invalid input parameters	Input parameters specified in the **Trace an IPv4 Path** window are invalid. For example, the IP address is incorrectly formatted, or does not exist in the specified domain.	Correct the parameters specified in the **Trace an IPv4 Path** window and retrace the path.	The parameter is not a valid IPv4 address or IP forwarding has been disabled for the address. Cannot continue with the path trace.
Network devices not responding	An IP address in the path did not respond to ping verification. **Note:** This message is only generated if **Ping-verify each hop** is selected in the **Trace IPv4 Network Path** window.	Check whether the device is can be pinged. Configure the network or device as required.	*ip_address_or_device_name* address did not respond to ping verification. Cannot continue with trace.
Path trace error	Internal path trace error.	Switch on path trace debugging and review the logs.	An error occurred during the trace of this path. For more details check the log file `$NMGUI_HOME/profile/logs/tnm/ncp_topoviz.X.log`,, where *X* is a number such as 1, or 2, and consult documentation on how to turn on further path tool logging.

Table 29. Path trace troubleshooting table (continued)

Type of error	Possible reason	Possible corrective actions	Example of an error of this type
Path trace prerequisites not met	For one or more of the devices along the path, SNMP access or routing information has not been configured.	Check that there is SNMP access to devices along the path. If necessary, correct the SNMP community string settings for this device in the **Discovery Configuration GUI**. Check, and if necessary, correct the MIB settings for this device using the **SNMP MIB Browser**.	The path start point *ip_address_or_device_name*, does not satisfy prerequisites. Cannot continue the path trace. The ipCidrRouteNumber MIB variable is not retrievable from the device and therefore the path trace script itnm_pathTool.pl cannot determine an IP route.
Required Network Manager process not running	Some Network Manager processes are not running.	Check that all relevant Network Manager processes are running. In particular, check that the processes Topology manager, ncp_model, and WebTools, ncp_webtool, are running and that the NCIM topology database is accessible.	OQL WebTools request failed. Check that all ncp processes are running. For more details check the log file `$NMGUI_HOME/profile/logs/tnm/ncp_topoviz.X.log`,, where *X* is a number such as 1, or 2, and consult documentation on how to turn on further path tool logging.
Timeout error	Path trace timeouts are too short. For example, one of the devices along the path was unable to provide the necessary SNMP routing data within the specified timeout. For example, the device might be set to non-forwarding mode.	Increase the length of path trace timeouts by adjusting the relevant configuration file property.	A timeout occurred. The path trace is taking longer than the configured OQL timeout and might still be running. Increase the oql.response.poll.timeout in `$NMGUI_HOME/profile/etc/tnm/tnm.properties` to wait longer for the path trace result.

Interpreting detailed path trace output

In the case of a path trace error you can access detailed path trace output by clicking on the error message that is displayed in the **Trace Network Path** window. Scroll down to the end of the path trace output and look for lines that contain the text WARNING and ERROR. These lines contain the most precise information on the nature and cause of the problem.

About this task

Note: You can obtain the most detailed output by switching on path trace debugging and tracing the path again.

Setting path trace timeouts

There are three timeouts associated with the path trace. You can modify the path trace timeouts; for example, you can make the timeouts longer if you want to give the path trace more time to retrieve device information.

About this task

The path trace timeouts are associated with the following Network Manager processes. The path trace interacts with all of these system components when constructing a path:

- OQL Service Provider (ncp_oql) timeout: the default value for this timeout is two minutes.
- Webtools (ncp_webtools) timeout: the default value for this timeout is five minutes.
- GUI timeout: the default value for this timeout is 10 minutes.

Setting the OQL Service Provider timeout

Set the OQL Service Provider timeout by modifying the appropriate configuration file.

About this task

To change the OQL Service Provider timeout:

Procedure

1. Edit the following configuration file: `$NMGUI_HOME/profile/etc/tnm/tnm.properties`.
2. Find the line that contains the property: `tnm.oql.response.poll.timeout`.
   This property is set to a default value of 320,000 milliseconds (five minutes and 20 seconds).
3. Modify this value as appropriate.
4. Save the file `$NMGUI_HOME/profile/etc/tnm/tnm.properties`.

Setting the WebTools timeout

Set the WebTools timeout by modifying the appropriate configuration file.

About this task

To change the WebTools timeout:

Procedure

1. Edit the following configuration file: `$NCHOME/precision/scripts/webtools/etc/PathToolGUI.xml`.
2. Find the line that has the following form: `<tool id="PathToolGUI" type="executable" timeout="300">`. The timeout parameter is set by default to 300 seconds (five minutes).
3. Modify this value as appropriate.
4. Save the file `$NCHOME/precision/scripts/webtools/etc/PathToolGUI.xml`.

Setting the GUI timeout

Set the GUI timeout by modifying the appropriate configuration file. This timeout applies to both the **Path View Administration GUI** and the **Path Views GUI**.

About this task

The GUI timeout applies to paths that are being traced and hence are in an In Progress state. If the timeout expires and the path is still an In Progress state, then the **Trace Status** for that path is set to Unknown. In this state, it is possible to retrace the path.

To change the GUI timeout:

Procedure

1. Edit the following configuration file: `$NMGUI_HOME/profile/etc/tnm/monitorconfig.properties`.
2. Find the line that contains the property: `monitorconfig.pathtrace.timeout`.
   This property is set to a default value of 600 seconds (10 minutes).
3. Modify this value as appropriate.
4. Save the file `$NMGUI_HOME/profile/etc/tnm/monitorconfig.properties`.

Switching on path trace debugging

To get more detailed path trace output in the logs and in the **Path Views GUI** and **Path View Administration GUI**, switch on path trace debugging.

Procedure

1. Open the `$NMGUI_HOME/profile/etc/tnm/tnm.properties` configuration file and identify the line that contains the following paramteter:

   ```
   tnm.pathtool.script.debug
   ```

2. Set this parameter as follows:

   ```
   tnm.pathtool.script.debug=true
   ```

   Based on this setting the path trace provides the most detailed output. Look for this output in one of the following places depending on how you ran the path trace:

Table 30.

If you ran the path trace run from...	**Then display the detailed path trace output by...**
GUI (**Path Views GUI** or **Path View Administration GUI**	Clicking an error message in the **Trace Network Path** window.
Command line using the itnm_pathTool.pl script	Viewing the `$NMGUI_HOME/profile/logs/tnm/ncp_topoviz.`*num*`.log` file, where *num* is a number such as 1, or 2

Fix Pack 2 Chapter 12. Configuring geographical views

Geographical views display devices that are enriched with geographical information. Before you use geographical views, you must enable and configure them.

Fix Pack 2 Enabling geographical views

Before you can configure geographical views, you must ensure that there are devices to display, and give access to the appropriate users.

Before you begin

Before you can enable geographical views, you must configure and run a geographical discovery.

About this task

You must give users who need to use geographical views the `ncp_gis` user role. Without this role, the options to open geographical views are not visible.

You must give users who need to administer geographical views the `ncp_gis_admin` user role. Without this role, the options to edit portlet layout preferences are not visible.

To enable geographical views, complete the following tasks:

Procedure

1. Create a group, or edit an existing group to which you want to add the appropriate roles, and add the `ncp_gis` or `ncp_gis_admin` role to the group.
2. Assign the group to the users who need to use or administer geographical views.

Fix Pack 2 Scoping and filtering geographical views

To improve visibility and performance, you might want to limit the devices that are displayed in geographical views.

About this task

The number of items rendered on a geographical map depends on how many devices, locations, and links are in scope to be displayed, and how many of those in-scope items you choose to filter out. To keep the total items that are included in a view down to a number that allows for clear navigation and good performance, use the scoping methods described in this task. If you want to reduce the number of in-scope items that are displayed for a particular view, use the filtering methods described in this task.

Procedure

1. To scope the **GIS Device Map** to a particular set of devices, select the devices in a topology view, right click and select **Show on Map**.
2. To scope the **GIS Device Map** to a particular Network View, add the **Network Views** widget and the **GIS Device Map** to a page.

   When you select a Network View, the **GIS Device Map** updates to display all devices with location information in that Network View.
3. To open the **GIS Device Map** scoped to a particular network view by using a URL, construct a URL similar to the following:

   ```
   https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?viewId=760
   ```

In the preceding example, 760 is the numeric ID of a network view.

4. To scope the **GIS Device Map** to a particular geographical area, construct a URL similar to the following:

```
https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?
bounds=((northern latitude,western longitude),
(southern latitude,eastern longitude))
```

   Where the latitudes and longitudes define the corners of a geographical area. For example:

```
https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?
bounds=%28%2851.50,-0.15%29,%2851.45,-0.09%29%29
```

5. To filter the items that are shown in the map, click the **Map Configuration** icon in the upper left of the **GIS Device Map**. Select the **Topology Filtering** tab in the **Map Configuration** window.
   a) Select domains in the **Domain** section to include and exclude devices by domain.
   b) Select device classes in the **Device Class** section to include and exclude devices by class.
   c) Select the option in the **Connectivity** section to display or hide links between devices or locations.
   d) Select the option in the **Connectivity** section to enable or disable links within locations.
   e) Select network layers in the **Connectivity** section to include and exclude links on a particular network layer.

Related tasks

Showing events in geographical context
Use the **GIS Device Health View** to view events and devices in their geographical context. The **GIS Device Health View** consists of the **GIS Device Map** displayed above the **Event Viewer**.

Related reference

URL parameters for geographical maps
You can use URL parameters to open geographical maps with specific configurations.

Fix Pack 3 Enabling regional aggregation for geographical views

You can group locations into cities, group cities into states, and group states into countries. This grouping is called regional aggregation.

About this task

Regional aggregation has the following advantages:

- The number of markers that are placed on the geographical maps is reduced.
- You can view large geographical areas, for example, connectivity from data center to data center or from country to country.

The geographical view can be scoped by a network view, a defined set of geographic bounds, a specific set of devices, specific domains, or all devices across all domains. Events for devices and locations are also aggregated. The region displays the highest status level of any of the subregions.

Links between regions represent the aggregate links from region to region, region to location, or region to device.

To enable regional aggregation for geographical views, complete the following steps.

Procedure

1. Ensure that the following fields in the `ACMEGeoLocation` (or equivalent) database table are correctly populated for all devices that you want to include in geographical views:

```
IP,ADDRESS,CITY,STATE,COUNTRY,LATITUDE,LONGITUDE
```

Restriction:

Ensure that each level in a hierarchy is unique. The following examples are incorrect because the city and state values are the same:

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
192.168.0.1,"113620 Redwood Gulch Rd, Cupertino, CA 95014,
 USA",PLAL,PLAL,US,37.15458,-122.05561
192.168.0.2,"113620 Redwood Gulch Rd, Cupertino, CA 95014,
 USA",CA,CA,US,37.15458,-122.05561
```

The following example is incorrect because the city and country values are the same.

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
Redwood Gulch Rd, Cupertino, CA 95014,
USA",US,CA,US,37.15458,-122.05561
```

The following example is incorrect because the PLAL value was used previously as a city and is used here as a state. CA was used as a state and is used here as a country.

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
192.168.0.3,"113620 Redwood Gulch Rd, Cupertino,
CA 95014, USA",Redwood,PLAL,CA,37.15458,-122.05561
```

The following example is correct, because the geographical hierarchy is properly ordered and contained.

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
192.168.0.1,"113620 Redwood Gulch Rd, Cupertino,
CA 95014, USA",PLAL,CA,US,37.15458,-122.05561
```

Incorrect hierarchies are not included in the geographical views. The `PopulateDNCIM_CustomGeography` stitcher removes incorrect hierarchies from the topology and logs each occurrence in the `ncp_disco` logs with an error similar to the following:

```
Cyclic collection detected : Entity with entityId
123 should not be collected with collectingEntityId 8912
```

The default regional aggregation is `address -> city -> state -> country`. This logic is defined in the following stitcher: `$NCHOME/precision/disco/stitchers/DNCIM/PopulateDNCIM_CustomGeography.stch`

The character sequence `->` is reserved for regional aggregation. Device and location names must not contain this sequence.

2. Open the **GIS Device Map** and click the **Topology Rendering** tab. Enable the **Aggregate Locations to Regions** option.

   You can also enable or disable regional aggregation by using the URL parameters for geographical maps.

Results

Devices and locations can be grouped automatically to the highest regional hierarchy available in the geographical view. Double-click a region to drill into that region and show the next logical level of the hierarchy. Users can enable regional aggregation for their session by selecting **Aggregate Locations to Regions** > **Enable** on the **Topology Rendering** tab in the **Map Configuration** window.

Related tasks

Viewing devices in geographical context

Use the **GIS Device Map** to view devices and events in their geographical context. The **GIS Device Map** is like a Network View that is superimposed on a geographical map.

Related reference

URL parameters for geographical maps

You can use URL parameters to open geographical maps with specific configurations.

Fix Pack 2 Configuring event status for geographical views

You can configure the intervals at which geographical views update event status.

About this task

To configure event status, complete the following steps.

Procedure

1. Configure the interval at which device status is queried from Tivoli Netcool/OMNIbus. Set the interval by changing the `mapStatusRefreshInterval` property in the `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json` file.

   The value is in seconds. The default is 20 seconds. When you configure this property, consider the Tivoli Netcool/OMNIbus refresh rate and the Network Manager poll policy cycle.
2. Configure the interval at which the status indicator is refreshed when it is visible on a device, link, or location. Change the `gridStatusRefreshInterval` property in the `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json` file.

   You do not normally need to modify this interval. If you set the `mapStatusRefreshInterval` to a higher value than the default, you might want to modify this interval.

Configuring the appearance of geographical views

You can hide the IP address of devices, configure the severity colors of links, and set the UI theme.

About this task

To configure the appearance of geographical views, complete the following steps.

Procedure

1. To customize the node icon for a device class in a geographical view, add the icon to this directory: `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/common_assets/topology_icons/`. The icon must be a PNG file of size 32 x 32 pixels, 8-bit/color RGBA, non-interlaced. Rename the icon file to match the classtype of the type of device you want it to represent. The file name must be lower case. Log out, clear cookies and cached data, and log in again to see the changes.
2. To hide the IP address of devices on geographical maps, modify the following file on the Dashboard Application Services Hub server: `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json` and set the property `rendering.obsfucateMarkerNames` to `true`.

   The IP address is replaced with asterisks `****`. If you right click the device or location, the IP address is visible.
3. To configure the colors that are used to represent the status of events on links, change the colors and icons in the following file: `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json`.
   For example, to overwrite the unknown state icon with the clear icon, copy the `clear.png` file over the `unknown.png` file in the `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/common_assets/status_icons/` directory.
4. To configure the theme that is applied to geographical views when they are opened by using a direct URL, set the `config.rendering.idxStyle` option in the `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json` file.

   Supported values are: `oneui`, `TIPDark`, and `idl`.

When the geographical views are opened from another GUI in the Dashboard Application Services Hub, the active theme is applied, regardless of the setting in the `config.json` file.

Fix Pack 2 Integrating geographic views with other widgets

You can change the devices that are displayed in the **GIS Device Map** by integrating it with another widget.

About this task

The **GIS Device Map** listens for `NodeClickedOn` events. If it receives a `NodeClickedOn` event that contains the correct parameters, the **GIS Device Map** displays the corresponding devices.

To remove the integration between the **GIS Device Map** and another widget, for example, between the **GIS Device Map** and the **Event Viewer** in the **GIS Device Health View**, edit the widget and disable the publishing of the `NodeClickedOn` event.

To integrate the **GIS Device Map** with another widget, complete the following steps:

Procedure

1. Ensure that the widget that you want to integrate sends a `NodeClickedOn` event with the following parameters:
   - Only one of the following required parameters: `viewId`, `bounds`, `deviceId`, `locationId`.
   - One or more of the following optional parameters: `config.filter.domain`, `config.filter.class`, `config.filter.layer`, `config.enableLinks`, `config.enableLinkStatus`, `config.enableTopologyStatus`, `config.minTopologyStatus`, `config.minLinkStatus`.
2. Add the integrating widget to a dashboard.
3. Add the **GIS Device Map** to the same dashboard.

Fix Pack 2 URL parameters for geographical maps

You can use URL parameters to open geographical maps with specific configurations.

Parameters for scoping geographical maps

The following URL parameters can be used to define the scope of the geographical maps.

Table 31. URL parameters for scoping geographical maps

Parameter	Description	Example
None	Displays all geographically enriched devices, locations, and links in all domains.	`https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp`

Table 31. URL parameters for scoping geographical maps (continued)

Parameter	Description	Example
bounds	Displays geographically enriched devices and links within a defined area. The area is defined as the rectangle between the north-west and south-east points. The values must be in the following format: `((`*`northern latitude`*`,`*`western longitude`*`), (`*`southern latitude`*`,`*`eastern longitude`*`))` The regular expression for the allowed values is: `(\\()(\\()([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(,)([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(\\))(,)(\\()([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(,)([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(\\))(\\))`	`https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp?bounds=((`*`northern latitude`*`,`*`western longitude`*`), (`*`southern latitude`*`,`*`eastern longitude`*`))` `https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp?bounds=%28%2851.50,-0.15%29,%2851.45,-0.09%29%29`
deviceId	Displays specific geographically enriched devices. The `deviceId` parameter must be a comma-separated list of positive numeric value device IDs. The regular expression for the allowed values is: `([1-9][0-9]*,[ ])*[1-9][0-9]*`	`https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp?deviceId=19078,19062,19067`
getAllLocations	Fix Pack 3 Controls regional aggregation. Displays all aggregated locations within the top level. For example, if the top level is Country, displays Regions. Locations that do not contain any in-scope entities, for example, because entities have been excluded by domain or class, are not shown.	`https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp?getAllLocations`

Table 31. URL parameters for scoping geographical maps (continued)

Parameter	Description	Example
`getLocationsWithinBounds`	Fix Pack 3 Controls regional aggregation. Displays all aggregated locations within the top level, within the specified map boundaries. For example, if the top level is Country, displays Regions. Locations that do not contain any in-scope entities, for example, because entities have been excluded by domain or class, are not shown. The area is defined as the rectangle between the north-west and south-east points. The values must be in the following format: `((`*`northern latitude`*`,`*`western longitude`*`),(`*`southern latitude`*`,`*`eastern longitude`*`))` The regular expression for the allowed values is: `(\\()(\\()([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(,)([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(\\))(,)(\\()([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(,)([+-]?\\d*\\.\\d+)(?![-+0-9\\.])(\\))(\\))`	`https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp?getLocationsWithinBounds=%28%2851.50,-0.15%29,%2851.45,-0.09%29%29`
`getLocationsByViewId`	Fix Pack 3 Controls regional aggregation. Displays all aggregated locations within the top level, for the given network view ID and all views that it contains. For example, if the top level is Country, displays Regions. Locations that do not contain any in-scope entities, for example, because entities have been excluded by domain or class, are not shown.	`https://`*`server`*`:`*`port`*`/ibm/console/ncp_gis/NetKitMapWidget.jsp?getLocationsByViewId`

Table 31. URL parameters for scoping geographical maps (continued)		
Parameter	**Description**	**Example**
`getLocationsByDeviceIds`	Fix Pack 3 Controls regional aggregation. Displays all aggregated locations within the top level, for the given device IDs (recursively traversing the view tree). For example, if the top level is Country, displays Regions. Locations that do not contain any in-scope entities, for example, because entities have been excluded by domain or class, are not shown.	`https://server:port /ibm/console/ncp_gis/ NetKitMapWidget.jsp? getLocationsByDeviceIds`
`locationId`	Displays geographically enriched locations. The value must be a positive numeric value representing a valid location collection `entityId`. The regular expression for the allowed values is: `(\\d+)`	`https://server:port /ibm/console/ncp_gis/ NetKitMapWidget.jsp? locationId=47672`
`viewId`	Displays all geographically enriched devices and links within the specified network view. Valid values are: • `NCP_VIEW_$viewId` • `$viewId` Where `viewId` is a positive numeric value only, and a valid Id of a network view.. The regular expression for the allowed values is: `(((NCP_VIEW_)(\\d+))|(\\d+))`	`https://server:port /ibm/console/ncp_gis/ NetKitMapWidget.jsp? viewId=760` `https://server:port /ibm/console/ncp_gis/ NetKitMapWidget.jsp? viewId=NCP_VIEW_760`

URL parameters for filtering geographical maps

The following URL parameters can be used to filter the contents of the geographical map.

Table 32. URL parameters for filtering geographical maps

Parameter	Description	Example
`config.filter.domain`	Scopes the view to the specified domains. The value must be a comma-separated list of positive numeric value domain IDs. The regular expression for the allowed values is: `([1-9][0-9]*,[ ])*[1-9][0-9]*`	The following example displays network entities in the specified domain: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.filter.domain=5`
`config.filter.class`	Scopes the view to devices that match the specified class type. The value must be a comma-separated list of positive numeric value entity class type IDs. The regular expression for the allowed values is: `([1-9][0-9]*,[ ])*[1-9][0-9]*`	The following example displays CiscoCat35xx class devices only: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.filter.class=110`
`config.filter.layer`	Scopes the view to links that match the defined topology layer type. The value must be a comma-separated list of positive numeric value topology layer type IDs. The regular expression for the allowed values is: `([1-9][0-9]*,[ ])*[1-9][0-9]*`	The following example displays devices on only Layer 2: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.filter.layer=72`
`config.enableLinks`	Scopes the view to exclude or include all links from the view. This value can be true or false. The regular expression for the allowed values is: `((true)|(false))`	The following example excludes links: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.enableLinks=false`
`config.enableLinkStatus`	Scopes the view to exclude or include link status from the view. This value can be true or false. The regular expression for the allowed values is: `((true)|(false))`	The following example displays links without severity colors: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.enableLinkStatus=false`

Table 32. URL parameters for filtering geographical maps (continued)

Parameter	Description	Example
`config.enableTopologyStatus`	Scopes the view to exclude or include device and location status from the view. This value can be true or false. The regular expression for the allowed values is: `((true)|(false))`	The following example displays devices and locations without any severity icons. `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.enableTopologyStatus=false`
`config.minTopologyStatus`	Scopes the view to show only status for devices and locations with events of a status greater than the specified value. The value must be one of the following: • 0 : Clear or Higher • 1: Indeterminate or Higher • 2: Warning or Higher • 3: Minor or Higher • 4: Major or Higher • 5: Critical only The regular expression for the allowed values is: `[0-5]`	The following example displays device and location status of Warning or higher: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.minTopologyStatus=2`
`config.minLinkStatus`	Scopes the view to show only status for links with events of a status greater than the specified value. The value must be one of the following: • 0 : Clear or Higher • 1: Indeterminate or Higher • 2: Warning or Higher • 3: Minor or Higher • 4: Major or Higher • 5: Critical only The regular expression for the allowed values is: `[0-5]`	The following example displays link status of Critical: `https://server:port/ibm/console/ncp_gis/NetKitMapWidget.jsp?config.minTopologyStatus=5`

Related tasks

Enabling regional aggregation for geographical views
You can group locations into cities, group cities into states, and group states into countries. This grouping is called regional aggregation.

Scoping and filtering geographical views
To improve visibility and performance, you might want to limit the devices that are displayed in geographical views.

Chapter 13. Configuring GUIs

You can change the appearance and functionality of the Hop Views; update MIB information; and configure the presentation of events from unmanaged devices.

Related tasks

Setting up network visualization

To set up network visualization, you can set up Network Views for your operators, and configure users, roles and groups.

Administering the TopoViz client

You can customize the operations of the TopoViz client. This includes the display settings, for example device icons, the frequency of topology updates, and alert settings.

About this task

Setting up automatic view maintenance

If you have multiple GUI servers, you must configure them so that only one server performs automatic network view and path view maintenance. If you have only one GUI server, you do not need to perform this task.

About this task

Network Manager performs automatic network view and path view maintenance.

Note: Only one server must perform network view maintenance. If no servers, or multiple servers, are configured to perform automatic view maintenance, undesired results can occur, such as views not being created and deleted properly.

To set up automatic view maintenance, complete the following steps.

Procedure

1. Choose one GUI server to perform view maintenance.
2. On the maintenance server, back up and edit the following file: `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`.
3. Fix Pack 8 To set all view maintenance properties at once, locate and uncomment the following line:

   ```
   # topoviz.engine.views.enabled=true
   ```

   Set this property to `true` to enable all automatic view maintenance settings. Setting it to `false` disables all the automatic view maintenance settings.

   Setting this property to `true` is equivalent to setting all of the individual view maintenance properties to `true`, as in the following example:

   ```
   topoviz.engine.viewsummary.enabled=true
   topoviz.engine.dynamicview.enabled=true
   topoviz.engine.pathview.enabled=true
   topoviz.networkview.deletedView.cleanUp.enabled=true
   ```

   Setting the `topoviz.engine.views.enabled` property to `false` is equivalent to setting all of the individual view maintenance settings to `false`.

   Setting this property to either `true` or `false` overrides any individual view maintenance property.
4. To set view maintenance properties individually, make the following changes.

a) Locate and comment out the following line:

```
# topoviz.engine.views.enabled=true
```

b) Uncomment all of the following properties and set them to `true` to enable them on this server:

topoviz.engine.viewsummary.enabled
This setting updates view membership.

topoviz.engine.dynamicview.enabled
This setting creates and deletes dynamic views.

topoviz.engine.pathview.enabled
This setting creates and deletes network path views.

topoviz.networkview.deletedView.cleanUp.enabled
This setting deletes views from the database when they are deleted by a user.

5. On each of the other GUI servers, ensure that the following line in the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file is uncommented and set to `false`:

```
topoviz.engine.views.enabled=false
```

6. Save and close the `topoviz.properties` files.

Features of the TopoViz client

Use this information to understand the features of the TopoViz client that can be customized.

TopoViz icons

In a topology map, icons represent types of device or network elements. You can customize these icons.

The following icons can be customized:

- Device icons
- Tree and map icons

The following figure shows a representation of the tree and map icons:

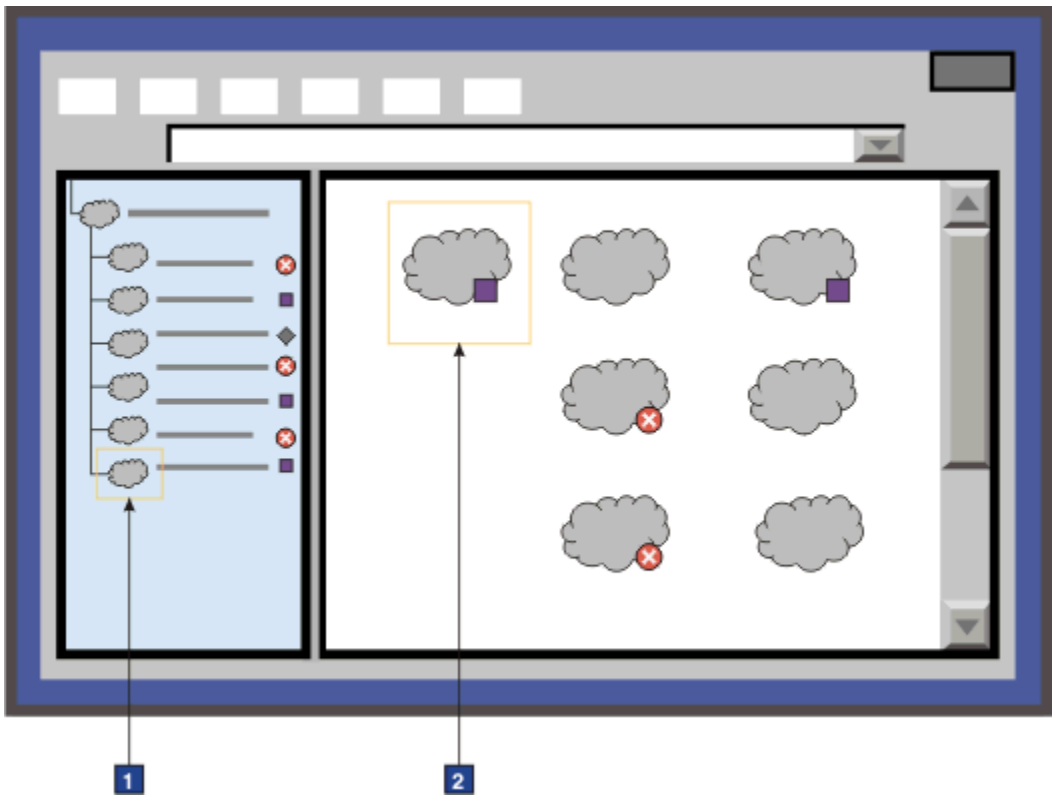

Figure 21. Tree and map icons

1 Tree icon
Used to represent views in the **Navigation Panel**. The default tree icon takes the form of a cloud. Network operators can customize these icons when defining a new network view in the Network Views GUI. To do this, they choose from a list of predefined icons.

2 Map icons
Used to represent views in the **Topology Display Panel**. The default map icon takes the form of a cloud.

Related tasks

Adding icons
Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the **Network Views** and **Network Hop View** GUIs.

Related reference

Configuring the display of extra information associated with a device
Information such as alert status and maintenance state of a device is displayed in a colored border around the device. You can configure the colors, icons, and positioning of the elements used to display this information.

Device class types

All device class are automatically categorized by *class type*. In topology maps, each class type is represented by a different icon, whereas each device class is not.

Class types are stored in the NCIM topology database, in the classType field of the entityType table.

The following class types apply:

- Core
- End Node
- Network Device
- Router

- Switch

All the class types consist of device classes. For example, the Network Device class type contains the Alcatel and Cisco device classes.

Device ToolTips

Device ToolTips appear when you roll your mouse over devices in topology maps.

Device ToolTips are defined by HTML entries in the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` configuration file on the server where the Network Manager GUI components are installed. You can specify the content of ToolTips associated with devices, subnets and links.

By default, the domain of a device is displayed in the ToolTip.

The `topoviz.properties` file is monitored every 60 seconds for changes, so that any changes are automatically detected by Topoviz.

Entries in the topoviz.properties file that control device ToolTips

The default settings for controlling device ToolTips are as follows:

```
topoviz.tooltip.map_item.entityType=HTML_statement
```

Where:

map_item
Takes one of the following values:

- `device`: For a chassis (main node device) or subnet ToolTip
- `link`: for a link ToolTip

entityType
Is the entityType number for a device, subnet, or link. It takes one of the following values:

- 1 (Chassis): For chassis (main node device) ToolTips.
- 2 (Link): For link ToolTips. Link ToolTips can display poll policy information.
- 15 (IP subnet): For subnet ToolTips.
- 68 (Probe Endpoint): For ToolTips on links between probe endpoints.
- 191 (Probe): For device ToolTips.

HTML_statement
Is any valid HTML code that is used to define the content and format of the ToolTip.

To insert the value from an NCIM topology database field use the following syntax: `{table.field}`

Restriction: The table must be in the `ncim` schema.

The table must contain a row whose `entityId` matches the `entityId` of the entity that the tooltip is for. For example, if you define a tooltip for chassis (`topoviz.tooltip.device.1`), and the user hovers the mouse over a chassis with `entityId = 20`, the GUI looks for a row whose entityId is 20 in the table or tables that the tooltip definition refers to.

Internationalization

If a tooltip definition contains a string of the form `{i18n.X}`, X is treated as a property name. The GUI looks it up in the localized version of the `$JazzSM_PROFILE_HOME/installedApps/JazzSMNode01Cell/isc.ear/ncp_topoviz.war/WEB-INF/classes/topoviz.properties` file. For example, if the user's locale is "de" (Germany), the GUI looks at the `topoviz_de.properties` file. If the GUI finds a match, it replaces the string in the tooltip definition with the value of the property X. If there is no match, it replaces `{i18n.X}` with X.

Example

The following example statement defines a chassis ToolTip:

```
topoviz.tooltip.device.1=<b>{entityData.displayLabel}</b><br><b>sysDescr:</b>
 {chassis.sysDescr}<br><b>sysContact:</b> {chassis.sysContact}
<br><b>sysLocation:</b> {chassis.sysLocation}<br><b>{i18n.netview_props.domain}</b> 
{mainNodeDetails.domainName}
```

Changing Dashboard Application Services Hub timeouts

When you are working in the Dashboard Application Services Hub, your GUI session is subject to timeouts. You can change the timeout settings.

About this task

Dashboard Application Services Hub provides the following default timeout settings:

Invalidation timeout
: If a user is logged into Network Manager using Dashboard Application Services Hub and closes the Dashboard Application Services Hub window, then the user session automatically times out after 30 minutes.

Lightweight Third Party Authentication (LTPA) timeout
: After a user is logged in for 24 hours, the Dashboard Application Services Hub login session is automatically closed down and the user is forced to log in again.

Changing the invalidation timeout setting

If a user is logged into Network Manager using Dashboard Application Services Hub and closes the Dashboard Application Services Hub window, then, by default, the user session automatically times out after 30 minutes. This is known as the invalidation timeout. You can modify the invalidation timeout setting.

About this task

To change the invalidation timeout setting:

Procedure

1. Log in to the server where the Network Manager GUI components are installed and edit the following file:

   `$JazzSM_HOME/profile/config/cells/JazzSMNode01Cell/applications/isclite.ear/deployments/isclite/deployment.xml`
2. Within this file find the `invalidationTimeout` value.

   By default, this value is set to 30 minutes.
3. Set the `invalidationTimeout` to the required value in minutes.
4. Save the `deployment.xml` file.
5. Restart the Dashboard Application Services Hub.

Changing the Lightweight Third Party Authentication (LTPA) timeout setting

After a user is logged in for a certain amount of time, by default 24 hours, the Dashboard Application Services Hub login session is automatically closed down and the user is forced to log in again. This is known as the Lightweight Third Party Authentication (LTPA) timeout. You can modify the LTPA timeout setting.

About this task

To change the LTPA timeout setting:

Procedure

1. Click **Security** > **Secure administration, applications, and infrastructure**.
2. In the **Secure administration, applications, and infrastructure** window, click **Authentication mechanisms and expiration**.
3. Set the **Timeout value for forwarded credentials between servers** value as required.

   The default value is 1440 minutes (24 hours).
4. Click **OK**.
5. Restart the Dashboard Application Services Hub.

Changing icons in the Network Views and Network Hop View GUIs

You can change the icons that represent device classes, class types, trees, and maps to make them more recognizable to users when users view topology maps within the Network Views and the Network Hop View.

Adding icons

Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the **Network Views** and **Network Hop View** GUIs.

About this task

To make custom tree and map icons available to network operators:

Procedure

1. Create your icon.

   For best results, use the following formats:

   - For the tree icon: 16 by 16 pixel PNG, GIF, or JPG image
   - For the map icon: PNG, GIF, JPG, or SVG image of any size

   You need only supply one image, because Topoviz scales the icon as appropriate.
2. Copy your icon to the `$NMGUI_HOME/profile/etc/tnm/resource/` directory on the server where the Web Applications are installed.

Related concepts

TopoViz icons

In a topology map, icons represent types of device or network elements. You can customize these icons.

Assigning icons to devices

You can change the icons for devices and other entities used in topology maps displayed within the **Network Views** and **Network Hop View** GUIs..

Assigning icons to device classes

To represent different device classes with different icons, assign each device class its own icon. This helps operators distinguish between device classes in topology maps, for example between Cisco and Alcatel devices.

Before you begin

Make custom icons available by adding icons as described in the related link.

About this task

To assign a custom icon to a device class:

Procedure

1. Assign the icon prepared earlier to a class type by modifying the line that describes the icon to the `topoviz.properties` file, as follows:
   a) Edit the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file.
   b) Find the section that specifies icon names for device types.
   c) Modify the relevant line of code as follows:

   ```
   topoviz.deviceicon.classname=iconname.extension
   ```

   Where

   - *classname* is the name of the device class. This must correspond to the `active object` parameter within the AOC file that defines the class. AOC files are contained in the `ITNMHOME/precision/aoc/` directory.
   - *iconname* is the name of your icon.
   - *extension* is the file extension.
2. Save the `topoviz.properties` file.

Assigning icons to entity types

Some network entities that display in the GUI are not devices and therefore do not have an associated class name. In order to be able to display an icon for these entities in the GUI, you can associate an icon to the related entity type to an icon.

Before you begin

Make custom icons available by adding icons as described in the related link.

About this task

To assign a custom icon to an entity type:

Procedure

1. Assign the icon prepared earlier to a class type by adding a line that describes the icon to the `topoviz.properties` file, as follows:
   a) Edit the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file.
   b) Find the section that specifies icon names for device types.
   c) Add the relevant line of code as follows:

   ```
   topoviz.image.entitytype=iconname.extension
   ```

   Where

   - *entitytype* is the entity type. This must exactly match the entity type name as listed in the NCIM `entityType` table. For more information on the `entityType` table, see the *IBM Tivoli Network Manager Reference*.
   - *iconname* is the name of your icon.
   - *extension* is the file extension.
2. Save the `topoviz.properties` file.

RAN GSM Cell

An example of a network entity that displays in the GUI but is not a device and therefore does not have an associated class name is the entity type 130: RAN GSM Cell. A RAN GSM Cell is a collection of elements, but does not have a class type or class name.

To associate the cloud icon for the RAN GSM cell in the GUI, the following line was added to the `topoviz.properties` file:

```
topoviz.image.RAN\ GSM\ Cell=cloud.svg
```

Note: The spaces in the entity name `RAN GSM Cell`must be escaped with a backslash (\).

Assigning icons to class types

Change the icons that are used to represent class types to make it easier for network operators to identify the class types in topology maps. Class types group together more than one class. For example, you might want a single icon that represents the class type CiscoSwitch, where the CiscoSwitch class type groups together multiple Cisco switch class icons.

Before you begin

Make custom icons available by adding icons as described in the related link.

About this task

To assign a custom icon to a class type:

Procedure

1. Identify the classes that make up your class type.
   For example, if you want a single icon for all Cisco switches (the Cisco switch class type), then identify each of the AOC files that represent individual Cisco switch classes.
2. Go to the directory that contains the active object class (AOC) files.
   AOC files define the device classes.

   ```
   cd $NCHOME/precision/aoc/
   ```

3. For each AOC file in your class type, modify the `visual_icon` parameter as follows:

   ```
   visual_icon = classtype;
   ```

   For example, in each Cisco switch AOC file, modify the `visual_icon` parameter as follows:

   ```
   visual_icon = CiscoSwitch;
   ```

   Restart the **ncp_class** process after changing AOC files. After **ncp_class** is restarted and running, restart the **ncp_model** process.
4. Assign the icon prepared earlier to a class type.
   For example, if you want to use a single icon for all Cisco switches (the Cisco switch class type), then edit the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file, find the section that specifies icon names for device types and modify the relevant line of code as follows:

   ```
   topoviz.image.CiscoSwitch=my_icon.svg
   ```

   Where *my_icon* is the name of your custom icon file for the Cisco switch class type.
5. Save the `topoviz.properties` file.

Assigning an icon for the RAN transmitter class type

An existing example is the class type for radio area network (RAN) transmitters. A number of RAN device classes fall into the transmitter type. For example, the RANBaseStation and RANNodeB classes both fall into the transmitter class type and are represented by a single transmitter icon. This is implemented using the following file settings:

AOC file for RANBaseStation

In this file, the `visual_icon` parameter is set to the generic class type `Transmitter`.

```
//************************************************************
//
//  File : RANBaseStation.aoc
//
//************************************************************


active object 'RANBaseStation'
{
    super_class = 'NetworkDevice';

    instantiate_rule = "ExtraInfo->ranBaseStation != NULL";

    visual_icon = 'Transmitter';
};
```

AOC file for RANNodeB

In this file, the `visual_icon` parameter is also set to the generic class type `Transmitter`.

```
//************************************************************
//
//  File : RANNodeB.aoc
//
//************************************************************


active object RANNodeB
{
    super_class = 'NetworkDevice';

    instantiate_rule = "ExtraInfo->ranNodeB != NULL";

    visual_icon = 'Transmitter';
};
```

topoviz.properties file

In this file, the icon `transmitter.svg` is assigned to any class that has the `visual_icon = 'Transmitter';` setting in its AOC file.

```
topoviz.image.Transmitter = transmitter.svg
```

Configuring topology map updates and appearance

You can change the way devices and alert status are displayed in the topology maps. You can also modify frequency of updates to topology and alert status.

Configuring the tabs displayed in the Network Views

You can configure how the Bookmarks and Libraries tabs are displayed.

About this task

The **Network Views** display the Bookmarks tab by default. You can show the Libraries tab by default instead. You can also hide one of the tabs.

To open a URL and set the default tab, add the `networkViewDefaultTab=bookview` or `networkViewDefaultTab=netview` parameter to the URL, for example: `https://xxxx :16311/ibm/console/ncp_topoviz/NetworkView.do?id=74&selectNode=1&`**`networkViewDefaultTab`**`=netview`

To configure the tab visibility for all users, complete the following steps:

Procedure

1. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file.

2. Locate the following line:

```
topoviz.netview.defaulttab=bookview
```

3. Set the property to `bookview` to have the Bookmarks tab displayed by default. Set the property to `netview` to have the Libraries tab displayed by default.
4. Locate the following line:

```
topoviz.netview.navtab.disable=none
```

5. Set the property to `bookview` to hide the Bookmarks tab. Set the property to `netview` to hide the Libraries tab. Set the property to `none` (the default) to display both tabs.
6. Save and close the file.

Appearance of nodes and lines in topology maps

By default nodes, representing, for example, devices, and other network entities, always appear before the lines showing connections between the nodes. You can change this default setting, but this can make it difficult to view and interact with the nodes.

By default nodes overlay lines in a topology map. The setting that controls this option can be found in the file `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` . To locate this setting, search for the relevant section that begins with the comment `# Specifies whether nodes are drawn before edges`.

```
# Specifies whether nodes are drawn before edges
#    true => Edges overlay nodes
#    false => Nodes overlay edges
topoviz.graph.nodesBeforeEdges=false
```

By default the setting `topoviz.graph.nodesBeforeEdges` is set to false, which means that nodes always overlay lines in a topology map.

Changing the frequency of topology update checks

TopoViz checks at regular intervals whether the topology shown in a network view has been updated. To change this frequency, change the topoviz.topologyupdateperiod value of the `topoviz.properties` file.

About this task

Any new nodes appear automatically in the topology maps; the new nodes are highlighted using handles.

The default frequency is 300 seconds (5 minutes). You can change this to any value between 300 and 3600 seconds. If you set the `topoviz.topologyupdateperiod` property to a value outside this range, the default value is used.

To change the check frequency:

Procedure

1. Open the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` configuration file and identify the following line:

```
topoviz.topologyupdateperiod=3600
```

2. Change the frequency to the required value in seconds. Save and close the `topoviz.properties` file.

Fix Pack 5 Changing the default topology layer for the Network Hop View

You can configure the default topology layer that is displayed by the **Network Hop View**.

About this task

When the **Network Hop View** is opened from the Dashboard Application Services Hub menu, **Structure Browser**, or **Event Viewer**, it displays layer 2 connectivity by default. You can change this default setting.

When the **Network Hop View** is opened from a Network View, it uses the same topology layer as the selected Network View.

To change the default topology layer, complete the following task:

Procedure

1. Open the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` configuration file and identify the following line:

   ```
   topoviz.hopview.connectivity.default=72
   ```

2. Change the layer to the required value.

   Allowed values are listed in the `ncp_layertypes.properties` file, and include the following:

   - 71: Layer 1
   - 72: Layer 2
   - 73: Layer 3

3. Save and close the `topoviz.properties` file.

Configuring the display of extra information associated with a device

Information such as alert status and maintenance state of a device is displayed in a colored border around the device. You can configure the colors, icons, and positioning of the elements used to display this information.

You control the display of extra information associated with a device using the settings in the following files:

- `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`
- `$NMGUI_HOME/profile/etc/tnm/status.properties`

The settings that you can configure using these files include the following:

Managed status of device
Icons that displays unmanaged and partially unmanaged status, position, and size of the icons.

Manually added device indication
Icon to indicate that this is a manually added device, position, and size of the icon.

Alert status of device
Whether to display an alert status icon, and if displayed, position of the alert status icon.

Frame around the device
Roundness of the corners of the frame around the device, height and width of the frame.

Device label text
Typeface, font size and font style of the device label text.

Example

The following figure shows a representation of a device display, showing a manually added device in unmanaged mode.

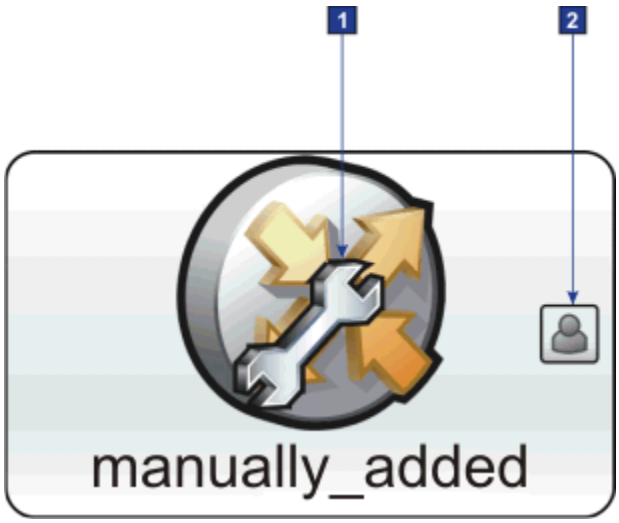

Figure 22. Representation of a device display, showing a manually added device in unmanaged mode

Configure the settings for the unmanaged status and manually added device icons as follows:

1 Unmanaged status icon, position, and size

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the relevant section that begins with the comment `# Overlay definitions.`.

```
# Overlay definitions.
topoviz.overlay.image.UNMANAGED=unmanaged.svg
topoviz.overlay.position.UNMANAGED=C
topoviz.overlay.size.UNMANAGED=25
topoviz.overlay.image.PARTIALMANAGED=partial_managed.svg
topoviz.overlay.position.PARTIALMANAGED=C
topoviz.overlay.size.PARTIALMANAGED=25
```

Table 33. Description of settings for the unmanaged status icons

Line	Description
2	Specifies the icon to use to indicate unmanaged status.
3	Specifies the position of the unmanaged status icon. The letter C means centered.
4	Specifies the size of the unmanaged status icon. The number is a relative value.
5	Specifies the icon to use to indicate partially unmanaged status.
6	Specifies the position of the partially unmanaged status icon. The letter C indicated centered.
7	Specifies the size of the partially unmanaged status icon. The number is a relative value.

2 Manually added device icon, position, and size

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the relevant section that begins with the comment `# Overlay definitions.`.

```
# Overlay definitions - Manual device
topoviz.overlay.image.MANUAL=manualoverlay.svg
topoviz.overlay.position.MANUAL=E
topoviz.overlay.size.MANUAL=10
topoviz.overlay.xoffset.MANUAL=-2
```

Table 34. Description of settings for the manually added device status icon	
Line	**Description**
2	Specifies the icon to use to indicate a manually added device.
3	Specifies the position of the manually added device icon. The letter E means east of center.
4	Specifies the size of the manually added device icon. The number is a relative value.
5	Specifies x-axis offset of the icon. The East of center positioning in line 2 would place the icon so that it is touching the frame surrounding the device. The -2 offset value moves the icon slightly to the left, so that it is positioned just inside the frame.

Example

The following figure shows a representation of a device display, showing an associated critical alert.

Figure 23. Representation of a device display, showing an associated critical alert

Configure the settings for the alert status icon, the device frame, and device label text as follows:

1 Alert status icon

The settings that control whether and where to display alert status icons in topology maps are as follows. Some settings are in the `topoviz.properties` file and others are in the `status.properties` file.

Whether to display alert status icons in the topology maps

The setting in the `status.properties` file that instructs the system to display alert status is `status.enabled=true`.

Position

The setting in the `topoviz.properties` file that specifies the position of the alert status icon.is `topoviz.status.position=NE`. This instructs the system to place the alert status icon in the north east (top right) corner of the frame containing the device.

2 Device frame

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the sections that begins with the comment `# Node dimensions` and `# Corner arc`.

```
# Node dimensions
topoviz.node.height=60
topoviz.node.width=100

# Node resizability
# Options:    LOCKED    (Fixed height and width)
#           TIGHT_HEIGHT (Fixed height, variable width)
topoviz.node.resizeability=TIGHT_HEIGHT

# Corner arc
topoviz.node.arc=10
```

Table 35. Description of settings for the device frame	
Line	**Description**
2	Specifies the height of the frame.
3	Specifies the width of the frame. **Note:** There is no wrapping of text for the device label, so if you want to show all of the device label text you must either increase this width value or decrease the text font size using the **topoviz.node.fontsize** setting.
8	Specifies how the **topoviz.node.height** and **topoviz.node.width** settings are handled. The default is TIGHT_HEIGHT. Using LOCKED means the values set in the **topoviz.node.height** and **topoviz.node.width** parameters are used for the device frame. Using TIGHT_HEIGHT maintains the **topoviz.node.height** setting, but does not maintain the **topoviz.node.width** setting, which means the device frame is automatically widened as necessary to accommodate the device label while keeping the width to the minimum.
11	Specifies the roundness of the corners of the frame. The higher the value, the more rounded the corners.

3 Device label

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the relevant section that begins with the comment `# Font settings`.

```
# Font settings
topoviz.node.font=Arial,Helvetica
topoviz.node.fontsize=10
topoviz.node.fontstyle=0
```

- Check with your system administrator that the font `Arial,Helvetica` is installed on the server.
- For `fontstyle` values, you can use the following values.

  0
  Plain font style.

  1
  Bold font style.

  2
  Italic font style.

Table 36. Description of settings for the device label text	
Line	**Description**
2	Specifies the typeface to use for the device label text.
3	Specifies the font size to use for the device label text.
4	Specifies the font style to use for the device label text.

Related concepts

TopoViz icons

In a topology map, icons represent types of device or network elements. You can customize these icons.

Configuring position of nodes in Network Views after rediscovery

You can configure how newly discovered and existing nodes are positioned in the network views after a rediscovery of the network.

About this task

By default, the TopoViz client changes the layout of a network view map as newly discovered nodes are added to the map. The position of existing nodes is not guaranteed when the map layout is updated because the layout is governed by factors such as connectivity information obtained during the discovery.

To change the default behavior and configure Network Manager to maintain the position of existing nodes and visually separate new nodes from nodes already present in the network views, edit the following parameters.

Note: This behavior works best with the **Symmetric Layout**. Other layout options take other factors into account which can affect the position of existing nodes. For example, the **Circular Layout** places greater emphasis on presenting nodes in a circular layout than maintaining node positions, while the **Hierarchical** and **Orthogonal** layouts place greater emphasis on routing the connections between nodes using orthogonal lines than maintaining exact node positions.

Procedure

1. Go to `$NMGUI_HOME/profile/etc/tnm/` and open the `topoviz.properties` file.
2. Locate the **`topoviz.node.freezeold`** parameter and change the value to `true` (the default value is `false`).

   The `true` setting maintains the position of existing nodes, while new nodes are placed in a row at the top of the map, clearly separating the new nodes from nodes not added during the last rediscovery. The new nodes are placed in one or more rows at the top of the map with a horizontal and vertical spacing of 20 pixels by default.
3. Log out of the Network Manager GUI and restart the browser. This is required for the `true` setting to take effect.
4. Optional: You can further adjust the positioning of new nodes using the following parameters in the `topoviz.properties`:
   - You can set whether the new nodes are placed at the top or bottom of the map using the **`topoviz.node.new.placement`** parameter. The default setting is `top`, change it to `bottom` to have the new nodes placed at the bottom of the network view map.
   - You can set the horizontal spacing between new nodes in pixels using the **`topoviz.node.new.spacing.horizontal`** parameter. The default setting is `20` pixels, change it to a different pixel count to position each new node closer to each other or further apart horizontally.
   - You can set the vertical spacing between new nodes in pixels using the **`topoviz.node.new.spacing.vertical`** parameter. The default setting is `20` pixels, change it to a different pixel count to position each new node closer to each other or further apart vertically.

   Note: All additional settings discussed in this step only take effect if the **`topoviz.node.freezeold`** is set to `true`.

Changing alert settings

If required, you can change the settings for alerts. You can change the frequency of updates to alert severity information, replace the default icons that represent alert severity, configure how alert status is retrieved, and configure other alert settings.

Changing the frequency of alert severity updates

If required, change how often the alert severity information is updated from the Tivoli Netcool/OMNIbus Web GUI.

About this task

To change the frequency with which the alert severity is updated:

Procedure

1. On the server where the Web Applications are installed, open the `$NMGUI_HOME/profile/etc/tnm/status.properties` file.
2. Make the following changes:
   - To change the frequency of alert severity updates in the network view tree, change the value of the `status.tree.updateperiod` property. The value is in seconds. For example:

     ```
     status.tree.updateperiod=60
     ```

   - To change the frequency of alert severity updates in the topology map, change the value of the `status.map.updateperiod` property. The value is in seconds. For example:

     ```
     status.map.updateperiod=60
     ```

3. Save and close the file.

Changing the timeout for event status updates for topology export

You can configure how long the network views wait for event status to be updated before exporting the topology.

About this task

When you click the **Export as CSV** button in the network views, the browser does not, by default, wait to check that the status of the events associated with the nodes in the current network view is downloaded before it exports the view. Fix Pack 12 In Fix Pack 11 and earlier versions, the Export as CSV button is displayed only if you have write access to the view. In Fix Pack 12 and later versions, by default the button is always displayed. The administrator can revert to the Fix Pack 11 behavior by setting `topoviz.table.export.allow.always` property in the `topoviz.properties` file to `false`.

You can configure the browser to wait. You can also configure how long it waits. These settings affect all topology layouts except the tabular layout. When the tabular layout is exported to a CSV file, the data is exported as it is seen on the screen.

To change the event status timeout, complete the following steps:

Procedure

1. On the server where the Web Applications are installed, open the `$NMGUI_HOME/profile/etc/tnm/status.properties` file.
2. Make the following changes:
   - To configure the browser to wait until event status is updated before downloading the view, change the value of the `status.table.export.wait.for.event.status` property to `true`. Allowable values are `true` and `false`. The default is `false`.
   - The browser waits for, at most, one update period for event status to load. If event status has not loaded after the specified time, the browser downloads the data which is available. The update period is the interval at which the browser polls the server for event status. It is defined by the

`status.map.updateperiod` property in the `status.properties` file. The value is in seconds. For example:

```
status.map.updateperiod=60
```

3. Save and close the file.

Changing the icons for alert severity levels

You can change the alert status icons used to represent alert severity levels in the Network Views GUI.

Changing icons for alert severity levels in the network views

If you want different alert status icons to represent alert severity levels in the Network View GUI, replace the default icons.

About this task

The required formats for replacement icons are as follows:

- For the network view tree: GIF or PNG files.
- For the topology map: GIF, PNG, or SVG files.

GIF or SVG files.

To replace a default icon:

Procedure

1. Create the image for the security icon that you want to replace and copy the image to `$NMGUI_HOME/profile/etc/tnm/resource/`.
2. Open the `$NMGUI_HOME/profile/etc/tnm/status.properties` file and make the following changes.
   a) In the `Tree status images` section of the files, point the property for the required severity to the new image.
   For example, to replace the default `critical.gif` file for severity level 5 with your own new image:

   ```
   status.tree.image.5=status/<filename for new critical icon>.gif
   ```

   b) In the `Map status images` section of the files, point the property for the required severity to the new image.
   For example, to replace the default `critical.gif` file for severity level 5 with your own new image:

   ```
   status.map.image.5=status/<filename for new critical icon>.gif
   ```

3. Repeat the steps for each default icon that you want to replace.
4. Save and close the file.

Changing icons for alert severity levels in topology map tabular layout

If you want different alert status icons to represent alert severity levels in the topology map tabular layout option, replace the default icons.

About this task

The required formats for replacement icons for the topology map table view are GIF or PNG files.

To replace a default icon:

Procedure

1. Create the image for the security icon that you want to replace and copy the image to `$NMGUI_HOME/profile/etc/tnm/resource/`.
2. Open the `$NMGUI_HOME/profile/etc/tnm/status.properties` file and in the `Net View Table status images` section of the files, point the property for the required severity to the new image.
   For example, to replace the default `ac16_critical04_24.gif` file for severity level 5 with your own new image:

   ```
   status.table.image.5=status/<filename for new critical icon>.gif
   ```
3. Repeat the steps for each default icon that you want to replace.
4. Save and close the file.

Configuring on-demand Event Viewer filters for the Network View tree

When you click on an alert status icon in the Network View tree, a filtered **Event Viewer** is displayed. You can configure the Network View tree to define these filters on demand, which uses less memory.

About this task

Configuring **Event Viewer** filters to be defined for all Network Views in the Network View Tree uses a large amount of heap memory, especially with deep, highly structured navigation trees with a large number of parent views, and might cause performance issues.

You can configure the Network View tree to define **Event Viewer** filters for only the Network View that is currently displayed. Defining filters on demand uses less memory. By default, on-demand filtering is disabled and filters are created for all views when the Network View tree is displayed.

Filters are always created for the leaf nodes in the Network View Tree. Leaf nodes are Network Views (not containers) that do not themselves contain other Network Views. Aggregated alert status is shown for all nodes in the Network View tree regardless of whether on-demand **Event Viewer** filters are enabled or not.

To configure on-demand **Event Viewer** filters in the Network View tree, complete the following steps:

Procedure

1. On the server where the Web Applications are installed, back up and edit the `$NMGUI_HOME/profile/etc/tnm/status.properties` file.
2. Make the following changes:
   - To enable on-demand **Event Viewer** filters in the Network View tree, change the value of the `status.tree.filterael` property to false. The filters are created only when you open a Network View. When you open an **Event Viewer** from a parent Network View in the Network View tree that has not been opened in the topology display pane, it shows events for all devices. If you click on the Network View, and then launch an **Event Viewer** from that view, the **Event Viewer** is filtered to show events on only those devices in that view.
   - To disable on-demand **Event Viewer** filters in the Network View tree, change the value of the status.tree.filterael property to true. **Event Viewer** filters are created for every view in advance. When you open an **Event Viewer** from any Network View, the **Event Viewer** is filtered to show events on only those devices in that view.
3. Save and close the file.

Alert status settings

The alert status settings control whether and how devices are displayed in topology maps, and the frequency with which the settings are updated.

The alert status settings are contained in the `$NMGUI_HOME/profile/etc/tnm/status.properties` file. You can control the following settings:

Table 37. Alert status settings

Setting	Description
`status.color.background.`*`severity`*	The `status.color.background.`*`severity`* property specifies background status color for each alert severity level.
`status.color.foreground.`*`severity`*	The `status.color.foreground.`*`severity`* property specifies the color of the device label text for each alert severity level.

`status.globalfilter`	The `status.globalfilter` property filters certain alerts from the status display of devices in the topology maps. This property filters on the `alerts.status` table of the ObjectServer.
	In versions of Network Manager prior to 4.2 Fix Pack 6, this property did not apply to the standalone **Structure Browser**. Starting with Fix Pack 6, the `status.globalfilter.apply.to.structurebrowser` property controls whether the value of `status.globalfilter` is applied to the standalone **Structure Browser**.
	The following example prevents ping fail events from affecting the displayed status of devices in the topology:
	`status.globalfilter=EventId<>'NmosPingFail'`
	The following example displays the status of only those devices in the topology views that have associated events with `EventId ='NmosPingFail'`:
	`viewsstatus.globalfilter=EventId='NmosPingFail'`
	The following example displays status of devices in the topology views that have associated events with `Severity` of `Minor`, `Major` or `Critical`:
	`status.globalfilter=Severity>2`

`status.globalfilter.apply.to.structurebrowser`	Fix Pack 6 If this property is set to `true`, the value of `status.globalfilter` is applied to the standalone **Structure Browser**, in addition to all other locations where alert status is shown. If this property is set to `false`, `status.globalfilter` is not applied to the standalone structure browser. The default value is `true`.
`status.hopview.linestyle`	The `status.hopview.linestyle` property indicates whether to display the alert status on links between nodes in the Hop View. By default, the status of links is set to `simple`, another possible value is `detailed`. Do not have a value of `none`. If `status.hopview.linestyle=none`, the show events tool displays an error for links because no status is registered for, nor requested.
`status.map.updateperiod`	The `status.map.updateperiod` property specifies how often the system updates the alerts status settings in the topology maps.
`status.map.maxnodes`	The `status.map.maxnodes` property indicates the maximum number of nodes for which alert status can be displayed in a single topology map.
`status.map.image.`*`severity`*	The `status.map.image.`*`severity`* property specifies the icons that are used to represent device alert status in the topology map. To customize these icons, create a GIF or SVG icon with the relevant name and save it to the following location: `$NMGUI_HOME/profile/etc/tnm/resource/`.

Table 37. Alert status settings (continued)

Setting	Description
`status.map.image.size.`*`severity`*	The `status.map.image.size.`*`severity`* property specifies the size of the icons to use to represent device alert status in topology maps.
`status.map.image.xoffset.`*`severity`* `status.map.image.yoffset.`*`severity`*	The `status.map.image.size.`*`severity`* and `status.map.image.yoffset.`*`severity`* properties specify x-axis and y-axis offset of the icon. The NE (northeast) positioning would place the icon so that it is touching the frame surrounding the device. The offset values moves the icon slightly down and to the left, so that it is positioned just inside the frame.
`status.map.topcolor.saturation.`*`severity`* `status.map.bottomcolor.saturation.`*`severity`* `status.map.topcolor.brightness.`*`severity`* `status.map.bottomcolor.brightness.`*`severity`*	The `status.map.topcolor.saturation.`*`severity`*, `status.map.bottomcolor.saturation.`*`severity`*, `status.map.topcolor.brightness.`*`severity`*, and `status.map.bottomcolor.brightness.`*`severity`* properties specify saturation and brightness adjustment controls that control the gradient of the background status color for each alert severity level.
`status.netview.linestyle`	The `status.netview.linestyle` property indicates whether to display the alert status on links between nodes in the Network Views. By default, the status of links is set to `simple`, another possible value is `detailed`. Do not have a value of `none`. If `status.netview.linestyle=none`, the show events tool displays an error for links because no status is registered for, nor requested.
`status.none.enabled`	The `status.none.enabled`property indicates whether the `none` status for a device is represented in the same way as the `clear` status. **Tip:** `none` status means that no events have been received for the device. `clear` status means that earlier events of severity level 1 or more have now been cleared on the device.
`status.registration.devicealert`	Set the `status.registration.devicealert` property to `true` to include alerts from devices in the alert status of views that are based on device components. For example, if you have an MPLS view that includes only interfaces, you might want to exclude alerts from the chassis of the devices containing those interfaces. To exclude alerts from the main nodes, set this property to `false`.

Table 37. Alert status settings (continued)

Setting	Description
`status.registration.threadscalefactor`	The `status.registration.threadscalefactor` property defines how many threads are used to register alert status. For example, if the `status.registration.threadlimit` property is set to 200 (the default), then one extra thread is used for each additional 200 views that a user has. This setting applies to all users. Increase the default setting if alert status takes a long time to appear on maps and in the Network View tree. More threads use more resources. Ensure that you have enough resources on the server to run the extra threads, based on your total number of users and views. Threads are increased up to the maximum defined by the `status.registration.threadlimit` property.
`status.registration.threadlimit`	The `status.registration.threadlimit` property defines the upper limit of the number of threads allowed per user to register alert status. Sets a limit for the scaling of threads defined by the `status.registration.threadlimit` property.
`status.table.image.`*`severity`*	The `status.table.image.`*`severity`* property specifies the icons that are used to represent device alert status in the topology map tabular layout. To customize these icons, create a GIF or SVG icon with the relevant name and save it to the following location: `$NMGUI_HOME/profile/etc/tnm/resource/`.
`status.table.image.sortUp` `status.table.image.sortDown`	The `status.table.image.sortUp` and `status.table.image.sortDown` properties specify how to sort alert severity icons in the topology map tabular layout.
`status.tree.bookmarks.enabled`	The `status.tree.bookmarks.enabled` property specifies whether device status is displayed in the Network View Bookmark tree. Set to `true` to enable and `false` to disable.
`status.tree.libraries.enabled`	The `status.tree.libraries.enabled` property specifies whether device status is displayed in the Network View Library tree. Set to `true` to enable and `false` to disable.
`status.tree.maxviews`	The `status.tree.maxviews` property specifies the maximum number of views that a Network View tree can contain and still display alert status.
`status.tree.registration.ondemand`	To enable on-demand **Event Viewer** filters in the Network View tree, change the value of the `status.tree.registration.ondemand` property to true. When you open an **Event Viewer** from a parent Network View in the Network View tree that has not been opened in the topology display pane, the **Event Viewer** shows events for all devices. If you click on the Network View, and then launch an **Event Viewer** from that view, the **Event Viewer** is filtered to show events on only those devices in that view. Enabling on-demand filters uses less heap memory. To disable on-demand **Event Viewer** filters in the Network View tree, change the value of the `status.tree.registration.ondemand` property to false. When you open an **Event Viewer** from any Network View, the **Event Viewer** is filtered to show events on only those devices in that view.
`status.tree.updateperiod`	The `status.tree.updateperiod` property specifies how often the system updates the alerts status settings in the Network Views and Structure Browser Navigation Panel.

Table 37. Alert status settings (continued)	
Setting	**Description**
`status.tree.image.`*`severity`* Where *severity* is a string or number specifying alert status severity	The `status.tree.image.`*`severity`* property specifies the icons that are used to represent device alert status in the network view tree. To customize these icons, create a GIF or SVG icon with the relevant name and save it to the following location: `$NMGUI_HOME/profile/etc/tnm/resource/`.
`status.view.enabled`	The `status.view.enabled` property specifies whether device status is displayed in Network Views, **Network Hop View**, and **Structure Browser**. Set to `true` to enable and `false` to disable.

Configuring visual differentiation between manually added and discovered devices

You can configure the topology views to highlight manually added devices in the topology map using an overlay icon.

About this task

To configure the system to highlight manually added devices:

Procedure

1. Edit the following file:
   `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`.
2. Within this file check the `topoviz.topologymanagement.differentiate_manual` value.
   - `topoviz.topologymanagement.differentiate_manual=true`: configures manually added devices and connections to be differentiated from discovered devices and connections.
   - `topoviz.topologymanagement.differentiate_manual=false`: manually added devices and connections are not differentiated from discovered devices and connections.

   By default, this value is set to `true`.
3. If the setting is `topoviz.topologymanagement.differentiate_manual=true`, then check the overlay image configuration for differentiation of manually added nodes.

   ```
   # Overlay definitions - Manual device
   topoviz.overlay.image.MANUAL=manualoverlay.svg
   topoviz.overlay.position.MANUAL=E
   topoviz.overlay.size.MANUAL=10
   topoviz.overlay.xoffset.MANUAL=-2
   ```

   This configuration snippet contains the following settings:

   - The overlay image used for is called `manualoverlay.svg`. This file is located at `$NMGUI_HOME/profile/etc/tnm/resource/`. You can change the overlay image used by copying a different .svg icon to `$NMGUI_HOME/profile/etc/tnm/resource/manualoverlay.svg`.
   - By default, the icon appears to the right (E stands for east) of the manually added device. Other options are N, S, W, NE, NW, SW, SEand C, where C means centred on the device.
4. Save the `topoviz.properties` file.

Configuring the zoom and pan tool

There is a zoom and pan tool within the **Network Hop View**, **Path Views**, and **Network Views**, use this tool to zoom to a preset percentage and to center or pan the topology.

About this task

The zoom and pan tool is enabled by default after a product installation. By default this zoom and pan tool displays in the north-east section within one of the following views.

Network Hop View
Network Views
Path Views

Users can zoom to preset zoom levels, for example `10%, 25%, 50%, 75%, 100%, 150%, 200%`.

The properties and property attributes for the zoom and pan tool are configured within `$ITNMHOME/profile/etc/tnm/topoviz.properties`. The `itnmadmin` user can modify property attributes within the `topoviz.properties` file, to either enable or disable this tool, or to reposition this tool within a view.

Procedure

1. As `itnmadmin` open `$ITNMHOME/profile/etc/tnm/topoviz.properties`.
2. With in the `topoviz.properties` file, modify the property value that you want to change.

```
#navigation control enablement (default true) true/false
topoviz.hopview.navigatecontrol.enabled=true
topoviz.networkview.navigatecontrol.enabled=true
topoviz.pathview.navigatecontrol.enabled=true

#navigation control placement (default NE)
#permissable values: NE, SE, SW, NW
#default is NE
topoviz.hopview.navigatecontrol.position=NE
topoviz.networkview.navigatecontrol.position=NE
topoviz.pathview.navigatecontrol.position=NE
```

3. Select **File** > **Save**.

What to do next

To zoom into the topology in your view, select either the **Zoom In**, **Zoom Out**, or select one of the preset zoom percentages. To pan around the topology in your view select either **Scroll To Center**, **Scroll Up**, **Scroll Down**, **Scroll Left**, or **Scroll Right.**.

Configuring the event view in composite topology views

You can configure the type of event view that is opened when a network node is clicked in one of the default views that combine network views and event views.

About this task

The Network Health View and the Fault-Finding View are composite topology views, that is, they combine a network views and an **Event Viewer**. When you click a node in the network view or a node in the network view tree, the **Event Viewer** refreshes to show any events for that node. You can configure the type of **Event Viewer** that is displayed.

You might want to configure the type of **Event Viewer** if you want to display an **Event Viewer** view that contains a subset of columns.

You can also use this procedure to troubleshoot errors with instances of the **Event Viewer** not appearing in composite views, if the error states that a particular **Event Viewer** view cannot be found.

To configure the view, complete the following steps:

Procedure

1. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` configuration file and identify the following section:

```
# Event viewer descriptions.
topoviz.webtop.view.name=Default
topoviz.webtop.view.type=global
```

2. Change the values to correspond to the type and name of the **Event Viewer** that you want to use.
3. Save and close the file.

Configuring the warning about number of devices in the Network Hop View

By default the **Network Hop View** presents a warning if the server determines that a Hop View search will return more than 500 devices. You can change this device limit from 500 to some other value, and you can also turn the warning off.

About this task

To configure the warning proceed as follows:

Procedure

1. Open the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` configuration file.
2. To configure the device limit, proceed as follows:
   a. Find the line that starts with: `topoviz.hopview.tooManyDevicesWarningLimit`.
   b. Change limit to a desired value.
3. To turn the warning off, proceed as follows:
   a. Find the line that starts with: `topoviz.hopview.tooManyDevicesWarningLimit`.
   b. Set the value to 0 to turn off the warning.
4. Save the file.

Configuring the presentation of events from unmanaged devices

You can configure the way events from unmanaged devices (devices that are not polled by Network Manager) are presented to network operators.

About this task

You can configure Network Manager to present unmanaged events in the **Event Viewer** in the following ways:

- Filtering out the unmanaged events so that they do not appear at all in the **Event Viewer**, or tagging these events in the **Event Viewer** so that you know that they come from unmanaged devices.
- Tagging these events in the **Event Viewer** so that the network operator knows that they come from unmanaged devices. In this case, the NmosManagedStatus field associated with an unmanaged event in the **Event Viewer** displays a value greater than zero.

Tivoli Netcool/OMNIbus probes and event sources from other network management systems can generate events on devices or interfaces that have been marked as Unmanaged in Network Manager. An unmanaged device is usually marked Unmanaged because it is undergoing maintenance and may therefore generate unnecessary network events. The following topics describe how to manage network events from an unmanaged device.

Remember: Unmanaged devices are shown in the network map with an overlaid double-ended wrench icon. Partially unmanaged devices (devices in which only certain interfaces are unmanaged) are shown in the network map using an overlaid single-ended wrench icon.

Filtering out events from unmanaged devices

You can filter events from unmanaged devices so that they do not appear in the **Event Viewer**.

Procedure

1. In the **Event Viewer**, select the **Filter Builder**.
2. Create a new filter or edit the existing filter to filter out all events where the NmosManagedStatus field is greater than zero (Managed).

What to do next

Once you have completed this operation and applied the filter to the **Event Viewer**, events from unmanaged devices no longer appear in the **Event Viewer**.

Tagging events from unmanaged devices

You can tag events in the **Event Viewer** so that you know that these events come from unmanaged devices.

Procedure

1. In the **Event Viewer**, select the **View Builder**.
2. Create a new view or edit the existing view to display the NmosManagedStatus field associated with an event. This field displays the managed status of the device or interface the event was raised for. For unmanaged devices, this field displays a value greater than zero.

What to do next

Once you have completed this operation and applied the view to the **Event Viewer**, each event in the **Event Viewer** will display the managed status of the associated network device or interface.

Configuring Internet Explorer 11 compatibility with Network Manager GUIs

If you use Internet Explorer 11, you must turn off Compatibility Mode and Enterprise Mode to ensure compatibility with Network Manager 4.2 GUIs. In previous versions of Network Manager, Compatibility Mode must be turned on.

About this task

Complete the following steps to ensure compatibility with Network Manager GUIs.

Procedure

1. In your Internet Explorer 11 browser, click **Tools** > **Compatibility View settings**.
2. Review the **Websites you've added to Compatibility View** list.

   If `ibm.com`, or your Network Manager server address or hostname is present in the list, remove it..
3. Deselect **Display intranet sites in Compatibility View**.
4. Ensure that Internet Explorer 11 is not running in Enterprise Mode IE (EMIE).

   Click **Tools**, and if **Enterprise Mode** is present in the menu, deselect it.

   To turn off Enterprise Mode for all users, refer to the information about *Enterprise Mode for Internet Explorer 11* in the Windows IT Center at https://technet.microsoft.com/en-us/windows.
5. Click **Close**.
6. Close your Internet Explorer 11 browser.

7. Launch your Internet Explorer 11 browser and clear the cache.

Results

Your Internet Explorer 11 browser is now fully compatible with Network Manager GUIs.

Chapter 14. Configuring non-English language settings for network visualization

If you want to display device labels or default network view names in languages other than English, you must perform some configuration steps.

About this task

If you want to use a language that does not have a country code, you have to request for the language without a country code.

For example: If you are in Mexico and want to use Spanish, you have to set your Locale to Spanish not Mexican Spanish. This is because Spanish is supported whereas Mexican Spanish, Spanish Spanish, or Argentinian Spanish are not supported.

Configuring non-English network view names

You can choose to display the default network view names in any supported language. You must configure which language you want them to appear in.

Procedure

1. Ensure that your NCIM database supports the character set used by your desired language.
2. Open the directory `$NMGUI_HOME/profile/etc/tnm/autoprovision/` .
3. Back up the `default.xml` file to a different location. (Network Manager attempts to create network views based on all files ending in `.xml` in the `autoprovision` directory.)

   Tip: Files that end in `.processed` are ignored by Network Manager. If the Network Manager GUI has been started at least once, the `default.xml` file is named `default.xml.processed`.
4. Edit the `default.xml` or `default.xml.processed` file.
5. Locate the `<dynamicViewTemplate>` tag and add the appropriate language and country attributes for your desired language.

   The following example specifies that network view names are displayed in Traditional Chinese:

   ```
   <autoProvision domain="*" accessLevel="user" accessId="itnmadmin">
           <dynamicViewTemplate id="ip_default" language="zh" country="TW"/>
   </autoProvision>
   ```
6. Save the file.
   - If the file is called `default.xml`, save it over the previous version.
   - If the file is called `default.xml.processed`, save it as `default.xml`.

     Note: If you do not save the file so that it ends with a `.xml` extension, it is not processed by Network Manager and your views are not created.

   All default network views owned by the itnmadmin user are now displayed in the chosen language. If you have previously accessed the network views, there are now two sets of network views: the original English views and a copy of these views named in your chosen language.
7. Optional: Log in to the network views as the itnmadmin user and delete the original English views.
8. Optional: Edit the `itnmuser.xml` file in the same way to configure the names of default network views owned by the itnmuser user.

Related tasks

Deleting network views

Delete existing network views if they are no longer required.

Configuring WebTools to correctly display in non-English languages

You must perform the following configuration tasks when running WebTools in non-English locales.

About this task

The following procedure shows how to configure WebTools for use in Japanese. Make the appropriate substitutions for your language.

Procedure

1. Configure the core server to run in the desired locale and UTF-8 character set.

   For example, for the Japanese locale, issue the following commands on the core server.

   ```
   export LANG=ja_JP.utf8
   export LC_ALL=ja_JP.utf8
   source /opt/IBM/netcool/core/env.sh
   ```

2. Restart the core server.
3. Configure the Dashboard Application Services Hub server to runs in same locale and UTF-8 character set as the core server.

   For example, for the Japanese locale, issue the following commands on the Dashboard Application Services Hub server.

   ```
   export LANG=ja_JP.utf8
   export LC_ALL=ja_JP.utf8
   ```

4. Restart the Dashboard Application Services Hub server.
5. Ensure that the locale character on your browser is set to Unicode.

Using multibyte (non-ASCII) characters in device attributes

You can use multibyte character strings from discovered devices in the device record in the topology. For example, you can display devices using non-ASCII characters in the display name.

About this task

Some devices can return data that contains multibyte data. Usually, this data is interpreted as ASCII data, and therefore corrupted. If you want to use multibyte data in device records you must first define the MIB variables as potentially containing multibyte data.

By default, sysName, sysDescr, sysLocation, and sysContact, are all defined as potentially containing multibyte data.

Defining non-ASCII MIB variables

You can specify MIB variables that might contain multibyte data. Multibyte data from these MIB variables is encoded as a space-delimited zero leading hex string.

About this task

If a MIB variable is defined as potentially holding multibyte data, the SNMP Helper checks whether the value contains bytes outside the ASCII range (1-127). If the variable does contain non-ASCII data the SNMP Helper encodes the value as a space-delimited zero leading hex string. By default, the following MIB variables are specified as capable of holding multibyte data:

- sysName
- sysDescr

- sysLocation
- sysContact

To define a MIB variable as capable of holding multibyte data, complete the following steps:

Procedure

1. Back up and edit the `SnmpStackSchema.cfg` configuration file.
2. Add a line like the following:

```
insert into snmpStack.multibyteObjects values ( 'sysDescr' );
```

3. Save and close the `SnmpStackSchema.cfg` configuration file.

Configuring device labels

If the SysName of a device contains multibyte data, follow these steps to use the SysName as the display label for devices in the topology maps.

About this task

If the SysName of a device does not contain multibyte data, you can set the SysName as the display label by selecting the **Enable SysName Naming** setting in the **Advanced** tab of the Discovery Configuration GUI.

If the SysName of a device contains multibyte data, you must not select the **Enable SysName Naming** setting in the Discovery Configuration GUI, because this results in the EntityName for the device containing encoded multibyte data. Instead, complete the following steps to use SysName as the display label for devices. For more information on the Discovery Configuration GUI, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Procedure

1. Back up and edit the `disco.config` configuration file for the appropriate domain.
2. Set the `m_DisplayMode` property:
   a) Set `m_DisplayMode` to `0` (the default) to use the EntityName as the display name.
   b) Set `m_DisplayMode` to `1` to use the SysName as the display name.
   The EntityName is not changed, but devices are displayed using the SysName.
3. Save and close the file.

Results

The settings are applied on the next discovery.

Changing the locale for the NCIM database

Set the same locale on the NCIM database as on the Network Manager server and the device from which you want to use multibyte data.

About this task

Because SNMP does not include locale information, Network Manager cannot automatically encode multibyte values from SNMP data from devices. Therefore, you must specify the expected locale of multibyte data.

If you are using a separate NCIM database, see the documentation for your database company and version. .

Limitations of using multibyte strings

Multibyte data cannot be processed by Network Manager. Multibyte data can only be passed into the NCIM database, without being changed.

About this task

Do not specify MIB variables as containing multibyte data if they are to be translated or changed by any Network Manager processes.

Part 4. Troubleshooting network problems

As a network operator, you are responsible for ensuring network and device availability. You can use Network Manager to visualize the network and quickly identify device alerts. You can then work with the alerts to locate, diagnose, and solve network problems in real time.

About this task

These tasks describe how to diagnose network problems and support problem resolution.

Chapter 15. About network troubleshooting

Network Manager provides several ways for troubleshooting network problems, including network views, event lists, Path Views, and the Structure Browser.

Network views and event lists provide a starting point for identifying network problems.

- Network views are displayed in the **Network Views** GUI. Network views show different views of your network based on geographical or other groupings. For example, network views can show subnets and VLAN groupings. Status icons within the **Network Views** GUI show event status of devices and device groups.
- Event lists are displayed in the **Event Viewer**. The **Event Viewer** provides lists of events on network devices and can be filtered to show events from selected devices only.
- The **Fault-Finding View** shows events in the **Event Viewer**. When you click on an event, the **Network Hop View** GUI displays connectivity for the device on which the event occurred.
- The **Network Health View** displays topology and event data in a composite GUI, where topology data in the form of network view libraries or bookmarks is shown in the top widget, and event data in the **Event Viewer** is shown in the lower widget. Selection of a device from the network view libraries or bookmarks generates a list of events for that device in the **Event Viewer**.

You can use the Path Views and the Structure Browser to investigate specific devices and routes between devices.

- The Path Views allows you to trace network paths. Network paths display every device and link encountered between the start and end devices. Issues affecting devices and links on that path are displayed graphically.
- The Structure Browser allows you to navigate the internal structure of a device. You can also use the Structure Browser to investigate the health of device components and isolate a fault within a network device.

Related tasks

Identifying problems using event lists
You can monitor all network events in a single event list. Use the **Fault-Finding View** to monitor network events.

Using the Network Health View
Use the Network Health View to display events on a device.

About topology

Network Manager provides the following GUIs to display topology: the **Network Hop View** GUI and the **Network Views** GUI. Use these GUIs to visualize the network and as a starting point for network troubleshooting.

Network Hop View GUI

Use the **Network Hop View** GUI to search the network for a specific device and display a specified network device. You can also use the **Network Hop View** as a starting point for network troubleshooting.

Use the **Network Hop View** GUI to create a topology map around a specified device. This is known as the seed device. You can also configure a number of hops from the seed device. The displayed topology consists of every device connected to the seed device, within the number of hops that you configure. The following examples describe how the content of the Hop Views changes as you vary the number of hops.

- **Example 1**: You specify Device A as the seed device and a number of hops equal to one. The Hop View shows you a network map consisting of Device A and all devices directly connected to Device A.

- **Example 2**: You specify Device A as the seed device and a number of hops equal to two. Device A is directly connected to two devices, Device B and Device C. The Hop View shows you Device A, Devices B and C, all devices directly connected to Device B, and all devices directly connected to Device C.

You can use the **Network Hop View** GUI to see events on devices in the network. The **Network Hop View** displays event status icons next to devices to show the severity of the most severe event on that device or on any component of that device.

Toolbar

Within a topology map, the event severity of a device is denoted by event severity icons. Double-click a device in the topology map to drill into the device and see its components in the **Structure Browser**.

To specify the required pivot device and draw the topology map, use the following buttons and fields:

Domain
Select the network domain containing the devices that you want to display.

Seed device

Type the IP address of the pivot device, or click **Search for seed device**  to search for a device in the database.

Hops
Select the number of hops that you want to display around the pivot device.

Connectivity
Select the type of topology view that you want to display:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

Apply Changes 
Applies your changes to the topology view.

To change the way the selected **Network Hop View** is displayed in the **Topology Display Panel**, use the following buttons:

Save as Image 
Saves the view or views as an image.

Print 
Prints the view or view container.

Find in Map 
Searches for a device in the topology map.

Select 
Changes the cursor to select mode. When the cursor is in select mode, if you click a device in the topology display panel that device is selected.

Pan 
Changes the cursor to pan mode. When the cursor is in pan mode, the cursor changes to the following icon:  . Click and hold the left mouse button to grab the topology; you can then use the mouse to move the topology.

Select Zoom 
Changes the cursor to select-zoom mode. When the cursor is in select-zoom mode, you can use the mouse to draw a rectangle over a particular area of the topology. When you release the mouse button, the screen zooms in to the rectangle you have drawn.

Interactive Zoom 
Changes the cursor to interactive-zoom mode. When the cursor is in interactive zoom mode, hold down the mouse button and move the cursor up to zoom out, and while hold down the mouse button and move the cursor down to zoom in.

Toggle Overview 
Displays a thumbnail of the whole view in the bottom right corner, with a box around the region that is currently visible.

Zoom In 
Zooms in to the view.

Zoom Out 
Zooms out of the view.

Fit in Window 
Fits the current view to the size of the **Topology Display** window.

Hierarchical Layout 
Changes the format of the view to a hierarchical layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Symmetric Layout 
Changes the format of the view to a symmetric layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Orthogonal Layout 
Changes the format of the view to an orthogonal layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Circular Layout 
Changes the format of the view to a circular layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Toggle End Nodes 
Shows or hides end nodes in the topology map. End nodes include devices such as workstations and printers.

Right-click tools

Right-click any entity in the **Network Hop View** to perform diagnostic actions with the following menu items:

Recenter Topology
Redraws the map in the **Network Hop View** centered around the selected device.

Show Events
Displays events for the selected device in the **Event Viewer**.

Show Device Structure
Displays internal structure of the selected device, including all components, in the **Structure Browser**.

Show Connectivity Information
Lists the interfaces on the selected device and associated connections for each interface in a separate window. You can also run this command on subnets.

Find in Network View
Displays the selected device in the **Network Views**. Prior to display, the system lists all the network views in which the selected device appears and asks you to select one of these network views.

Find in Path View
Displays the selected device in the **Path Views GUI**. Prior to display, the system lists all the path views in which the selected device appears and asks you to select one of these path views.

Trace IP Path
Opens the **Trace Network Path** window and populates it with the device or devices selected.

Note: You can only trace a path across a single domain. All devices specified in the **Trace Network Path** window must be in the same domain.

Add To View
Adds the selected device to a network view of your choosing.

Create a Poll Policy
Creates a poll policy for the selected device.

Browse SNMP MIB Data
Calls the **SNMP MIB Browser** where you can browse MIB data within the selected device.

Graph SNMP MIB Data
Calls the **SNMP MIB Grapher** where you can graph MIB data within the selected device.

Discovery...

Show Discovery Overview
Launches the Discovery Overview window for the selected device. The Discovery Overview window lists discovery status for a device, including when it was first discovered, last discovered, and last rebooted.

Unmanage
Places the selected device into maintenance (unmanaged) mode. Placing a device into maintenance mode deactivates Network Manager polling and event correlation for the device. You can also run this command on subnets.

Ping from this host
Pings one or more selected devices from your client machine to check connectivity to that device.

Ping from the server
Pings one or more selected devices from the Network Manager server to check connectivity to that device. You can also run this command on subnets.

Telnet
Enables you to log into a selected device using Telnet.

Configuration Management
Runs ITNCM configuration management reports on a selected device.

ITNCM Reports

Policy Compliance Grouped By Device
Runs the Netcool Configuration Manager Policy Compliance Grouped By Device report on the selected device.

Configuration and OS Change Summary
Runs the Netcool Configuration Manager Configuration and OS Change Summary report on the selected device.

Policy Compliance Score and Summary
Runs the Netcool Configuration Manager Policy Compliance Score and Summary report on the selected device.

Topology Management

Add Device
Manually adds a main node device to the current topology.

Delete Device
Deletes a selected manually added device from the current topology.

Add Connection
Adds a manual connection between selected device.

Launch To...
Launches the TADDM system, which provides extra information on devices and subnets.

TADDM/CCMDB

View Details
View details for a selected device in TADDM.

View History
View history for a selected device in TADDM.

Webtools
Launches the WebTools user interface so that you can run WebTools, such as ping, traceroute, and DNS lookup operations, against a selected device.

Related reference
Default event status icons

The **Structure Browser** in table mode, the **Network Views**, and the **Network Hop View** show the severity of events affecting a device or other network entity such as a card, by showing an alert icon adjacent to the entity.

Network Views GUI

The **Network Views** GUI displays hierarchically organized views of a discovered network. Use the **Network Views** to view the results of a discovery and to troubleshoot network problems.

By default, the network view tree contains a separate IP network view hierarchy per domain for each network technology; you will see an IP network view hierarchy only for each domain.

Optionally you can add an LTE network view hierarchy for each domain. Do this by creating a template-based dynamic view using the lte_default network view template, as described in the *IBM Tivoli Network Manager User Guide*.

IP network view tree hierarchy

Network views can display any set of device types, subnets, VLANs or other views, depending on how your network is organized.

The network view tree shows an icon next to each network view name that indicates the highest severity event on network entities within the network view. Unlike in the **Network Hop View**, where events from contained entities are also shown, the **Network Views** display status only for entities that match the view definition. Click on the icon to open an **Event Viewer** that shows all events on devices within the network view.

When the discovery completes, it automatically generates a top-level network views node. If your network is very large and consists of thousands of devices, then your administrator might have discovered it in multiple domains. In this case, you see a top-level network views node for each domain.

Note: By default the top-level network views node is called NCOMS, because NCOMS is the default Network Manager domain.

The contents of the top-level node depend on the devices and device collections within your network. All networks contain the following sub-nodes:

- Device classes: devices grouped by vendor, model, or other device characteristic.
- Subnets: all subnets in the current Network Manager domain.

If you have a large and more complex network, for example, if you are a service provider organization and you support customer VPNs using MPLS, the top-level node can also contain the following sub-nodes:

- VLANs: all virtual LANs in the current Network Manager domain
- HSRP groups: all Hot Standby Router Protocol router groups in the current Network Manager domain
- VTP domains: all VLAN Trunking Protocol domains in the current Network Manager domain
- MPLS: all MPLS core networks and Virtual Private Networks in the current Network Manager domain
- BGP Networks: all BGP autonomous systems (ASs) in the current Network Manager domain
- OSPF Routing Domains: all OSPF areas in the current Network Manager domain

Note: The subnodes listed are the default views that the system builds automatically following a discovery. You can also build custom network views.

Network view toolbar buttons

To change the way the selected network view is displayed, use the following buttons:

Refresh 

Refreshes the view. By default, the view refreshes every 20 seconds.

Save 
Saves the view or view container. This button appears only when a view is displayed.

Save as Image 
Saves the view or views as an image.

Print 
Prints the view or view container.

Find in Map 
Searches for a device in the topology map.

Select 
Changes the cursor to select mode. When the cursor is in select mode, if you click a device in the topology display panel that device is selected.

Pan 
Changes the cursor to pan mode. When the cursor is in pan mode, the cursor changes to the following icon:  . Click and hold the left mouse button to grab the topology; you can then use the mouse to move the topology.

Select Zoom 
Changes the cursor to select-zoom mode. When the cursor is in select-zoom mode, you can use the mouse to draw a rectangle over a particular area of the topology. When you release the mouse button, the screen zooms in to the rectangle you have drawn.

Interactive Zoom 
Changes the cursor to interactive-zoom mode. When the cursor is in interactive zoom mode, hold down the mouse button and move the cursor up to zoom out, and while hold down the mouse button and move the cursor down to zoom in.

Toggle Overview 
Displays a thumbnail of the whole view in the bottom right corner, with a box around the region that is currently visible.

Zoom In 
Zooms in to the view.

Zoom Out 
Zooms out of the view.

Fit in Window 
Fits the current view to the size of the **Topology Display** window.

Hierarchical Layout 
Changes the format of the view to a hierarchical layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Symmetric Layout 
Changes the format of the view to a symmetric layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Orthogonal Layout 
Changes the format of the view to an orthogonal layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Circular Layout 
Changes the format of the view to a circular layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Grid Layout 
Changes the format of the view to a grid layout. This option is only available for views that cannot contain connectivity information, such as Unassigned views.

Tabular Layout 
Changes the format of the view to a tabular layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Export as CSV 
Exports the current view to a downloaded Comma-Separated Values (CSV) file. The file contains the information about the devices that are displayed. If you export from the tabular layout, the exported data is in the same order as in the table, and is filtered using the same filters that are applied to the table. If you export from another view, the order of the data is undefined, and includes every device in the view. Fix Pack 12 In Fix Pack 11 and earlier versions, the Export as CSV button is displayed only if you have write access to the view. In Fix Pack 12 and later versions, by default the button is always displayed. The administrator can revert to the Fix Pack 11 behavior by setting `topoviz.table.export.allow.always` property in the `topoviz.properties` file to `false`.

Link Status Options 
Allows you to choose option to display whether the status (color) of links in the network view is determined by events on the links (the default) or by a poll policy. The button is not shown unless the administrator has enabled it. The button is also not shown in the tabular layout, because that does not show links.

Help 
Displays help for the portlet.

Related tasks

Searching for a network view
If you have many network views, you can search through the network view tree to find the view you want.

Related reference

Default network view nodes
Use this information to understand which nodes appear by default in your network view tree.

Default event status icons
The **Structure Browser** in table mode, the **Network Views**, and the **Network Hop View** show the severity of events affecting a device or other network entity such as a card, by showing an alert icon adjacent to the entity.

Network domains

A network domain is a collection of network entities to be discovered and managed. A single Network Manager installation can manage multiple network domains.

The default network domain is called NCOMS. If you add extra domains then you must give each domain a unique name.

Restriction: Use only alphanumeric characters and underscores (_) for domain names. Any other characters, for example hyphens (-), are not permitted.

By default the system uses the default NCOMS domain. The system provides the option to change the domain when you perform the following tasks:

- Configuring and running a discovery
- Configuring polls and poll definitions
- Querying management database data using OQL
- Visualizing the network using the **Network Views** and the **Network Hop View**.
- Browsing device MIBs using the **SNMP MIB Browser**

Device connectivity

You can display the network at different OSI layering levels in the network map. Change the connectivity layer setting if you wish to focus on subnet membership, OSI layer 2 connections, OSI layer 3 connections, Protocol Independent Multicast (PIM), or Internet Protocol Multicast (IPM) routes.

If link status has been configured, then connections between devices are displayed as colored, corresponding to the severity of events on the devices. Connections can be displayed with an associated event status icon, if configured.

Administrator can enable to links to display status from poll policies. If it is not enabled, Link status option button is not displayed.

Connectivity layer settings vary as follows:

Layer 1
Displays all physical connections.

Layer 2
Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3
Shows routers and the connections between routers. Switches are not normally displayed.

Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown as normal.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

IP subnets
Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

- **Layer 1** for transmission layer connections.
- **Layer 2** for data link connections.
- **Layer 3** to show all routers and connections between them.

OSPF
Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

No connections
Does not present any of the discovered connections for the nodes shown in the view.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

Related tasks
Monitoring links

By monitoring the links between devices, you can determine the status of the devices connected by the link. In addition, you can launch tools to diagnose the underlying problem.

IP Subnets connectivity

Use IP Subnets connectivity to display device membership by subnet in the network map.

The IP Subnets connectivity option shows all devices within a subnet connected to a subnet cloud. Using the IP Subnets connectivity option usually simplifies the network displayed in the network map and makes subnet membership clear. If you wish to see all connections, choose one of the following:

- Layer 1 for physical connections.
- Layer 2 for data link connections.
- Layer 3 to show all routers and connections between them.
- Converged Topology to show the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

Layer 1 connectivity

Use the Layer 1 connectivity option to display connections between layer 1 network elements.

Layer 2 connectivity

Use the Layer 2 connectivity option to display discovered Layer 2 connections, such as between routers, switches and other network devices in the topology. A layer 2 view typically shows switch and hub connections.

Layer 3 connectivity

Use the Layer 3 connectivity option to display discovered Layer 3 connections, such as between routers and other network devices. Switches are not normally displayed.

The connections between devices are displayed as follows:

- Connections between two layer 3 interfaces are shown.
- Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
- Connections between two layer 2 interfaces are not shown.

Note: Switches with routing capabilities are displayed if they have active connections involving layer 3 interfaces.

Network map and tree icons and symbols

Devices and device connectivity are represented in the network map and tree using the icons described here.

The following tables describe the device and device connectivity icons used in the network map and network tree. Within the network map solid line indicates a connection between devices and pale dashed line indicates membership; for example, membership of a subnet or of a BGP autonomous system.

- Table 38 on page 316: Describes general icons.
- Table 39 on page 318: Describes LTE icons.

Table 38. Icons used in network maps: general

Icon	Name	Description
	Cell icon	Represents a device that is designated as a radio area network cell.

Table 38. Icons used in network maps: general (continued)		
Icon	**Name**	**Description**
	Element management system (EMS) icon	Represents an EMS.
	End node icon	Represents end-node devices, including Windows, Linux, and Solaris workstations and printers.
	Generic logical collection icon	Represents a Generic logical collection.
	Geographical location icon	Represents a geographical location.
	Geographical region icon	Represents a geographical region.
	Manually added device or connection between devices	Used to indicate that the associated device or connection was added manually using the **Topology Management** right-click options.
	Probe icon	Used to represent a network probe.
	Radio area network (RAN) router icon	Represents a device that is designated as a radio area network router.
	Radio area network (RAN) switch icon	Represents a device that is designated as a radio area network switch.
	Router icon	Represents a device that is designated as a router.
	Subnet icon	Represents a subnet
	Switch icon	Represents a device that is designated as a switch.
	Unknown device icon	System is unable to identify the correct icon to use for this device. The most likely reason is failed SNMP access to the device.

Table 38. Icons used in network maps: general (continued)		
Icon	**Name**	**Description**
[4]	Number of connections indicator	This indicates either of the following: • In the case of a connection relationship between two devices, which is indicated by a solid line, this number indicates the number of interfaces participating in the connection between the devices. • In the case of a membership relationship, which is indicated by a pale dashed line, this number indicates the number of interfaces participating in membership, for example, of a subnet or OSPF area. The number of connections displayed is specific to the connectivity layer being displayed.
	Completely unmanaged device	The entire device, including all its interfaces, is unmanaged.
	Partially unmanaged device	Only certain components of this device are unmanaged.

Table 39. Icons used in network maps: LTE		
Icon	**Name**	**Description**
	Antenna icon	Represents an antenna.
	Equipment Identity Register (EIR) icon	Represents an Equipment Identity Register (EIR).
	Evolved NodeB (eNodeB) icon	Represents an Evolved NodeB (eNodeB) device.
	eUtranCell icon	Represents a eUtranCell.
	Home Subscriber Server (HSS) icon	Represents a Home Subscriber Server (HSS).
	LTE pool icon	Represents an LTE pool.
	LTE sector icon	Represents an LTE sector.
	LTE tracking area icon	Represents an LTE tracking area.

Table 39. Icons used in network maps: LTE (continued)		
Icon	**Name**	**Description**
	Mobility Management Entity (MME) icon	Represents a Mobility Management Entity (MME) device.
	Policy and Charging Rules Function (PCRF) icon	Represents a Policy and Charging Rules Function (PCRF).
	Packet Data Network Gateway (PGW) icon	Represents a Packet Data Network Gateway (PGW) device.
	Serving Gateway (SGW) icon	Represents a Serving Gateway (SGW) device.

OSPF and BGP network maps use the same devices icons as the standard network maps. Labels under the device icons indicate the function performed by the device within the BGP network or the OSPF routing domain. The following table provides examples of device icon labels and explains what the labels represent.

Table 40. Icons used in OSPF and BGP network maps		
Network view	**Example of label**	**Description**
BGP autonomous system	BGP Service172.20.1.4(RR)	Represents a route reflector device within a cluster. The label **RR** under the device indicates that this is a route reflector client.
BGP autonomous system	BGP Service172.20.1.7(RR Client)	Represents a route reflector client device within a cluster. The label **RR Client** under the device indicates that this is a route reflector client.
BGP network	BGP AS65530 (OPENTRANSIT)	Represents a BGP autonomous system. Pale dashed lines indicate devices that are members of this BGP AS.
OSPF routing domain	OSPF 172.20.65.31 (ABR)	Represents an area border router. The label **ABR** under the device indicates that this is an area border router.
OSPF routing domain	OSPF 172.20.1.6 (ASBR)	Represents an AS border router. The label **ASBR** under the device indicates that this is an AS border router.
OSPF routing domain	OSPF 172.20.81.12 (DR)	Represents a designated router. The label **DR** under the device indicates that this is a designated router.
OSPF routing domain	OSPF 172.20.1.4 (BDR)	Represents a backup designated router. The label **BDR** under the device indicates that this is a backup designated router.
OSPF routing domain	172.20.2.8 (Broadcast)R	Represents a type-2 Network Link State Advertisement (LSA) that is generated by designated routers on a broadcast or no-broadcast multi-access network segment.

Default network view nodes

Use this information to understand which nodes appear by default in your network view tree.

Default nodes in the network view tree

By default, the network view tree contains a separate IP network view hierarchy per domain for each network technology; you will see an IP network view hierarchy only for each domain.

Optionally you can add an LTE network view hierarchy for each domain. Do this by creating a template-based dynamic view using the lte_default network view template, as described in the *IBM Tivoli Network Manager User Guide*.

You might see only some of the default network view libraries. The nodes that appear in your network view tree vary depending on the types of devices in your network, on the technologies used in your network, and on how the network views have been configured. Access to network view libraries can also be restricted by the administrator for users, roles, or groups. If you have more than one network domain, then you might see one network view hierarchy for each domain, each hierarchy containing some or all of these network view nodes.

Note: Default network views that are based on alert severity are filtered such that they contain only devices that have one or more alerts of that severity. For example, the **Alert Views** > **Acknowledged Alerts** > **Major** view contains devices that have one or more Major alerts. However, those devices can also have alerts of other severities. For example, the **Major** view could contain device A, on which there is a Major alert and a Critical alert. All alerts on the device are included in that network view. All alerts on the device are shown when you use the **Show Events** tool. It is possible to edit the filters for the network views to include only devices that have a certain alert severity and no other alert severities. However, take care that devices that have multiple alerts with different severities are not accidentally omitted from your network view hierarchy.

Default network view nodes: IP network

The following table lists the default network view hierarchy for IP network devices.

Table 41. Default network view nodes: IP network

Network view node	Description of devices contained in this network views node
Alert Views > **Acknowledged Alerts**	Devices with associated acknowledged alerts. The network views are organized by severity of the alert.
Alert Views > **Acknowledged Alerts** > **Critical**	Devices that currently have acknowledged alerts of critical severity associated with them.
Alert Views > **Acknowledged Alerts** > **Major**	Devices that currently have acknowledged alerts of major severity associated with them.
Alert Views > **Acknowledged Alerts** > **Minor**	Devices that currently have acknowledged alerts of minor severity associated with them.
Alert Views > **Critical Ping Fail Events at least an hour old**	Devices that have any ping fail events that are at least one hour old and have a Severity of 5 (critical).
Alert Views > **PingFailRootCause**	Devices which have associated ping fail alerts and where the alert is a root cause alert.
Alert Views > **SNMP Poll Fail**	Devices that currently have SNMP fail (NmosSnmpPollFail) events associated with them. These devices have SNMP polls configured to run on them, but are unreachable using SNMP. If the devices are not SNMP-enabled, they should not have SNMP polls configured to run on them. If the devices are SNMP-enabled, an SNMP poll fail might indicate a fault on the device.

Table 41. Default network view nodes: IP network (continued)

Network view node	Description of devices contained in this network views node
Alert Views > **SnmpLinkInDiscards**	Devices with alerts of type NmosSnmpLinkInDiscards.
Alert Views > **Unacknowledged Alerts**	Devices with associated unacknowledged alerts. The network views are organized by severity of the alert.
Alert Views > **Unacknowledged Alerts** > **Critical**	Devices that currently have unacknowledged alerts of critical severity associated with them.
Alert Views > **Unacknowledged Alerts** > **Major**	Devices that currently have unacknowledged alerts of major severity associated with them.
Alert Views > **Unacknowledged Alerts** > **Minor**	Devices that currently have unacknowledged alerts of minor severity associated with them.
All Management Systems	All EMSs (Element Management Systems) that Network Manager has discovered. Each EMS network view displays the managed elements managed by that EMS, together with the connectivity between the managed elements.
All Routers	All devices with layer 3 connectivity, that is, all devices that Network Manager has classed as routers in the ncim.entityClass database table.
All Switches	All devices with layer 2 connectivity, that is, all devices that Network Manager has classed as switches in the ncim.entityClass database table.
BGP Networks	Devices grouped by membership of BGP networks.
Custom view	A custom collection of devices. You can add any devices or device collections to the custom view.
Device Classes	Devices grouped by the Network Manager device class hierarchy. Examples of device classes include Cisco and Juniper.
Discovered ASMs	An ASM agent running on a device corresponds to a commercial server or database product running on that device. These network views group devices within a network based on the commercial server or database products running on those devices.
HSRP Groups	All the Hot Standby Routing Protocol (HSRP) groups in the network domain.
IGMP Groups	All the discovered Internet Group Membership Protocol groups.
Manually Added Devices	An automatic collection of all devices that have been manually added to the topology. If a device is not discovered, you can add it to the topology manually. All devices that were added manually appear in this view.
Monitoring Views > **Devices that have at least one interface event for HighDiscardRate**	Shows devices that have interfaces that have a high rate of discarded packets.
Monitoring Views > **Initial Ping Fail Events**	Shows devices that have failed ping polls.
MPLS > **MPLS Core**	Shows the Multiprotocol Label Switching Path (MPLS) core network.
MPLS > **MPLS VPNs**	The MPLS Virtual Private Networks (VPNs) within your network domain.
MPLS TE	MPLS Traffic Engineering (TE) tunnels within your network domain.
Multicast Routing MDTs	Shows any discovered Multicast Distribution Trees (MDTs).

Table 41. Default network view nodes: IP network (continued)	
Network view node	**Description of devices contained in this network views node**
NAT Address Spaces	Devices grouped by membership of Network Address Translation (NAT) address spaces.
Fix Pack 3 **Network Probes**	Shows one subview for each probe type. The subviews hold devices that are configured as probe sources or targets.
OSPF Routing Domains	Devices grouped by membership of Open Shortest Path First (OSPF) areas and routing domains.
PIM network	Devices grouped by membership of Protocol Independent Multicast (PIM) networks.
SLA > **Network Probes** > **IPSLA**	Contains network views collecting probes of a certain type. For example, DHCP, DNS, echo, and so on. Also contains a view of all probes.
Subnets	Devices grouped by membership of IPv4 and IPv6 subnets.
Unassigned view	All devices in a domain that are not currently assigned to a network view. The view is updated dynamically as devices are added and removed from views in the domain.
VLAN Ports	All the Virtual Local Area Network (VLAN) ports in the network domain organized by VLAN identifier or by VLAN name. **Note:** The **Global VLANs** network view does not appear by default. However, you can create a **Global VLANs** network view manually.
VPLS > **MPLS Core**	Shows Virtual Private Label Switching paths through the MPLS core.
VPLS > **VPLS VPNs**	Shows Virtual Private Label Switching Virtual Private Networks.
VTP Domains	Devices grouped by membership of VLAN Trunking Protocol (VTP) domains.

Default network view nodes: LTE network

The following table lists the default network view hierarchy for LTE network devices.

Table 42. Default network view nodes: LTE network	
Network view node	**Description of devices contained in this node**
LTE Network Drilldown	Lists all the LTE network views available for listing out devices. All network views in this node are in tabular mode by default.
LTE Network Drilldown > **E-UTRAN**	Lists all eNodeB devices in the evolved UMTS Terrestrial Radio Access network (EUTRAN).
LTE Network Drilldown > **E-UTRAN by Vendor**	Lists all vendors for the eNodeB devices in the evolved UMTS Terrestrial Radio Access network (EUTRAN). Clicking a vendor name lists the eNodeB devices of that vendor type in the EUTRAN.
LTE Network Drilldown > **EPC**	Lists all devices in the evolved packet core (EPC) network.
LTE Network Drilldown > **EPC by Vendor**	Lists all vendors for devices in the evolved packet core (EPC) network. Clicking a vendor name lists the devices of that vendor type in the EPC.
LTE Network Drilldown > **PLMN**	Lists all public land mobile networks (PLMN) in the LTE hierarchy.
LTE Network Drilldown > **Tracking Areas**	Lists all tracking areas in the LTE hierarchy.

Table 42. Default network view nodes: LTE network (continued)	
Network view node	**Description of devices contained in this node**
LTE Network Drilldown > **Vendor**	Lists all vendors in the LTE hierarchy. Clicking a vendor name lists network views corresponding to the device types from that vendor in the LTE hierarchy.
LTE Network Geography	Shows devices in the LTE hierarchy grouped geographically. The geographical groupings vary depending on how the geographical locations and regions are defined in your system.
LTE Network Topology > **Control Plane by Tracking Area**	Lists network views containing sections of the control plane associated with a given tracking area. Each of these network views is given the name of the associated tracking area.
LTE Network Topology > **EPC Control Plane**	Provides a fully connected network view showing all control plane devices in the Evolved Packet Core section of the LTE network.
LTE Network Topology > **EPC User Plane**	Provides a fully connected network view showing all user plane devices in the Evolved Packet Core section of the LTE network.
LTE Network Topology > **User Plane by Tracking Area**	Lists network views containing sections of the user plane associated with a given tracking area. Each of these network views is given the name of the associated tracking area.
LTE Pools	Shows all pools in the LTE hierarchy. If you have no LTE pools then this node does not appear. Because the LTE Pools view is a dynamic distinct view, it will contain child views for whatever types of LTE pools exist in the NCIM topology database; for example, MME pools, PGW pools, SGW pools.

Related concepts

Network Views GUI

The **Network Views** GUI displays hierarchically organized views of a discovered network. Use the **Network Views** to view the results of a discovery and to troubleshoot network problems.

About events

Use events to help you identify faulty network devices and troubleshoot network problems.

Events are stored in the Tivoli Netcool/OMNIbus ObjectServer and are presented in the **Event Viewer**. From the **Event Viewer**, you can take actions on events to find out more information about the event.

Restriction: Regardless of where you are authenticated, your username must exist in the Tivoli Netcool/OMNIbus ObjectServer and have the necessary permissions in order to take actions on events.

Sources of events

When Tivoli Netcool/OMNIbus receives events and alarms from network devices, it generates and stores alerts. The ObjectServer receives events from Tivoli Netcool/OMNIbus probes, and potentially from many other network event sources.

Deduplication

Alerts are deduplicated. This means that if an event occurs multiple times, it only occupies a single alert row in the **Event Viewer**, with a count value indicating how many times the event occurred.

Related information

Tivoli Netcool/OMNIbus documentation

Default event status icons

The **Structure Browser** in table mode, the **Network Views**, and the **Network Hop View** show the severity of events affecting a device or other network entity such as a card, by showing an alert icon adjacent to the entity.

The following table shows the default event status icons.

Table 43. Default event status icons

Default icon in the Network Views	Severity or meaning	Color in the Event Viewer
	No status has been retrieved for this device. If this persists, there might be an error.	Not applicable
	5 (critical)	Red
	4 (major)	Orange
	3 (minor)	Yellow
	2 (warning)	Blue
	1 (indeterminate)	Purple
	0 (clear)	Green
	There are no events for this device. This icon is not used in the **Network Hop View**.	Not applicable
	This icon appears next to unmanaged devices or components.	Not applicable
	This icon appears next to devices that contain unmanaged components.	Not applicable

Related concepts

Network Hop View GUI

Use the **Network Hop View** GUI to search the network for a specific device and display a specified network device. You can also use the **Network Hop View** as a starting point for network troubleshooting.

Network Views GUI

The **Network Views** GUI displays hierarchically organized views of a discovered network. Use the **Network Views** to view the results of a discovery and to troubleshoot network problems.

Related tasks

Viewing events in the network views

You can use the network views to check that certain sections of the network or certain kinds of devices are free of problems.

About the Structure Browser

The Structure Browser allows you to navigate the internal structure of a device. You can also use the Structure Browser to investigate the health of device components and isolate a fault within a network device. The Structure Browser has two modes: tree and table.

You can change the **Structure Browser** from tree mode to table mode by editing the widget preferences. You can specify the default mode for the **Structure Browser** using the configuration files.

Restriction: If the **Structure Browser** is started from a right-click tool, it is always displayed in tree mode. Table mode is only available when the **Structure Browser** is displayed as a widget, for example, within the **Network Hop View** in a default installation.

Tree mode

In tree mode, the Structure Browser (labeled **Structure View**) displays the structure of a device in a tree form. Expand the nodes in the tree to pinpoint the cause of a network issue down to the component level and keep track of the alert status for a device..

You can use the **Expand All** button  to expand all of the nodes in the tree and use the **Collapse All** button  to collapse the expanded nodes. From the **Structure Browser** tree, perform these tasks:

- Examine the structure of a selected device and the data associated with its internal components. This data can be used to support the resolution of network problems.
- Search for a device, or any physical or logical components of a device, using the Search for Entity button  .
- Search through the nodes in the tree for a specific value.
- Keep track of the event status for each device. The **Structure Browser** displays the alert status for each component of a device, down to the interface level. For detailed event information, launch the **Event Viewer** from the **Structure Browser**.
- Test a selected device or component using the diagnostic and information retrieval tools.

Restriction: The **Structure Browser** can only be used for retrieving information. You cannot use the **Structure Browser** to modify information on devices and device components.

Table mode

In table mode, the Structure Browser displays summary information about the selected device in a table. The table is updated with new information each time you select a device. Use the table to view information about a selected device and to check the alert status for the device.

From the **Structure Browser** table, perform these tasks:

- Examine summary data that can be used to resolve network problems.
- Keep track of the event status for a device. For detailed event information, launch the **Event Viewer** from the **Structure Browser**.
- Test a selected device or component using the diagnostic and information retrieval tools.
- Refresh the information in the current table view using the Refresh button  .
- Pause the refresh of information using the Pause button  .

View information about a device from one of three table views: Device Information, Interfaces, and Device Connectivity.

Show device information

Device Information is the default view. Select a device to see information about the device. By default, the table is empty until you select a device unless you specify an entity ID to use by default when you open the Device Information view. You can specify an entity ID through widget preferences or by clicking on the Hop View to load device information immediately. The first time the widget is displayed, device information for the default entity ID is displayed. The column names vary depending on the type of entity selected.

Show interfaces

The Interfaces view shows all of the interfaces available on the device as well as their severity and managed status. You can configure the columns that you want to view in the table, but you cannot change the column names or the order in which the columns are displayed. The ncim.interfaces table in the NCIM database contains the list of columns to be displayed in the Interfaces view. If you want to hide a column that you do not need to view, set the column width to zero in the `structurebrowser.properties` file. You can filter the table to only show interfaces that match the filter. If there is no match, then no rows are displayed in the table.

In the Interfaces view, the following icon denotes unmanaged devices or components: . The alert status indicator denotes the alert severity level of each component.

Show device connectivity

The Connectivity view shows the severity and managed status of interfaces on the device. This view also shows interface data both for interfaces on the device, and for the interfaces that they are connected to, including connection type.

In the Connectivity view, the following icon denotes unmanaged devices or components: . The alert status indicator denotes the alert severity level of each component.

Related tasks

Searching the node text in the Structure Browser tree
You can search for a value within the nodes in the **Structure Browser** tree.

Identifying faulty components from the Structure Browser tree
Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Identifying faulty components from the Structure Browser table
Using the table mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Chapter 16. Finding network devices

Search for a specific device using its IP address or host name, or browse for a device in the network views.

About this task

In the **Network Health View** or **Network Views**, you can also switch between visualizing devices in a map and in a tabular layout.

Searching for devices using the Network Hop View GUI

Search for a seed device in the **Network Hop View** GUI to display that device and those devices connected to it.

About this task

The **Network Hop View** GUI displays a view of the network including all devices within a certain number of connections from a device that you choose. The device around which the view is based is called the seed device.

You can search for a seed device using either the basic search or the advanced search.

Note: Specifying a greater number of hops can dramatically increase the number of devices to display in the **Network Hop View** GUI, especially in LTE networks. Network hop views containing large numbers of devices can take a long time to draw. In order to avoid excessively long times for network hop view layout, the system first determines the number of devices that will be returned by a **Network Hop View** GUI search and provides a warning with an option to exit if the view will return more than a default value of 500 devices. You can change this value or, alternatively, turn the warning off. For more information on changing or turning off the device limit, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Related tasks

Configuring the warning about number of devices in the Network Hop View
By default the **Network Hop View** presents a warning if the server determines that a Hop View search will return more than 500 devices. You can change this device limit from 500 to some other value, and you can also turn the warning off.

Using the basic search

In the **Network Hop View**, use the basic search to find a device by IP address or device name.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. Select a network domain from the **Domain** list.
3. Check or uncheck the **Search all domains** checkbox to constrain the search to a particular domain or to search across all domains.

   If the **Search all domains** checkbox is checked, the **Domain** list is disabled. The default state of the **Search all domains** checkbox is controlled by the `topoviz.entitySearch.allDomains` property in the `topoviz.properties` file.
4. Click **Search for Seed Device**  to specify the device to search for.
5. In the **Entity Search** window, ensure that the **Basic** tab is selected and complete the search criteria fields.

Domain
Select the domain in which you want to search.

Note: If you opened the Entity Search window from the Path Views GUI, then you cannot change domain. This is done to prevent cross-domain path traces.

IP Address
Specify the IP address of the device. You can specify all of the address, or only the first part of the address. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets.

Device Name
Specify the name of the device. You can specify all of the name, or only the first part of the name. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets. Device names are not case-sensitive. If you specify both an IP address and a device name, the IP address takes precedence.

6. Click **Find**.

   The **Results** list box displays the devices resulting from your search, as a listing of IP addresses or entity names, along with the domain in which the devices exist.
7. Select the device you want from the **Results** list box, and click **Select & Close** to return to the **Network Hop View** main window.

   The **Seed device** field in the **Network Hop View** toolbar is populated with the seed device IP address or host name.
8. Select the maximum number of hops displayed from the seed device from the **Hops** list.

   This setting shows more or less devices connected to the seed device.
9. Specify how to display connectivity:

   Layer 1
   Displays all physical connections.

   Layer 2
   Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

   Layer 3
   Shows routers and the connections between routers. Switches are not normally displayed.

   Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

   The connections between devices are displayed as follows:

   - Connections between two layer 3 interfaces are shown as normal.
   - Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
   - Connections between two layer 2 interfaces are not shown.

   IP subnets
   Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

   - **Layer 1** for transmission layer connections.
   - **Layer 2** for data link connections.
   - **Layer 3** to show all routers and connections between them.

   OSPF
   Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

Fix Pack 3 **Probe**
Displays the probe topology, linking probe sources to probe targets.

Converged Topology
Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

PIM
Displays connections based on PIM adjacency information.

IPMRoute
Displays connections based on IP Multicast upstream and downstream routing information.

Microwave
Shows microwave connections only.

Logical RAN
Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

10. Click **Apply Changes**  .

    The topology you selected is displayed in the network map. Faulty devices are displayed with an associated event icon.

    Note: If you have configured cross-domain discovery, the **Network Hop View** results might include devices from a different domain to the domain in which the seed device is located. Hover the cursor over a device to see which domain it is located in.

Using the advanced search

In the **Network Hop View**, use the advanced search to find a device by any attribute of the device from the topology database.

About this task

To perform an advanced search for a device, complete the following steps:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.
2. Select a network domain from the **Domain** list.
3. Check or uncheck the **Search all domains** checkbox to constrain the search to a particular domain or to search across all domains.

   If the **Search all domains** checkbox is checked, the **Domain** list is disabled. The default state of the **Search all domains** checkbox is controlled by the `topoviz.entitySearch.allDomains` property in the `topoviz.properties` file.

4. Click **Search for Seed Device**  to specify the device to search for.
5. In the **Entity Search** window, ensure that the **Advanced** tab is selected and complete the search criteria fields.

   Domain
   Select the domain in which you want to search.

   Note: If you opened the Entity Search window from the Path Views GUI, then you cannot change domain. This is done to prevent cross-domain path traces.

   Table
   Select the database table that you want to search. The mainNodeDetails table lists network devices.

   Field
   Select the field whose value you want to search. The selection available for this field is automatically populated based on the chosen database.

   Comparator
   Select a comparator.

   Value
   Required. Type the value that you want to search for. You are unable to use wildcard characters like the percent character (%) or the asterisk (*) in the search facility within Path Views and Path View Administration, however you can use these character types as wildcards in the search facility for other widgets.

6. Click **Find**.

   The **Results** list box displays the devices resulting from your search, as a listing of IP addresses or entity names, along with the domain in which the devices exist.

7. Select the device you want from the **Results** list box, and click **Select & Close** to return to the **Network Hop View** main window.

   The **Seed device** field in the **Network Hop View** toolbar is populated with the seed device IP address or host name.
8. Select the maximum number of hops displayed from the seed device from the **Hops** list.

   This setting shows more or less devices connected to the seed device.
9. Specify how to display connectivity:

   Layer 1
   Displays all physical connections.

   Layer 2
   Displays all switched connections between devices in the topology. A layer 2 view typically shows switch and hub connections.

   Layer 3
   Shows routers and the connections between routers. Switches are not normally displayed.

   Note: If switches have active connections involving layer 3 interfaces, they are included in this layout.

   The connections between devices are displayed as follows:

   - Connections between two layer 3 interfaces are shown as normal.
   - Connections between a layer 3 and a layer 2 interface are shown as being between the layer 3 interface and the subnet to which the layer 2 interface belongs.
   - Connections between two layer 2 interfaces are not shown.

   IP subnets
   Shows all devices within a subnet connected to a subnet cloud. This layout helps to simplify the network map and also helps to make subnet membership clear. If you want to see all connections, select one of the following options:

   - **Layer 1** for transmission layer connections.
   - **Layer 2** for data link connections.
   - **Layer 3** to show all routers and connections between them.

   OSPF
   Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.

   Fix Pack 3 **Probe**
   Displays the probe topology, linking probe sources to probe targets.

   Converged Topology
   Displays the lowest layer links between devices based on all layer 1, 2 and 3 topology data available.

   PIM
   Displays connections based on PIM adjacency information.

   IPMRoute
   Displays connections based on IP Multicast upstream and downstream routing information.

   Microwave
   Shows microwave connections only.

   Logical RAN
   Shows logical RAN connectivity. RAN entities are usually connected by L1 or L2 connections, but this logical connectivity allows an overview of the main RAN entities to be seen. Connections are usually implicit in the discovered data. For example, a base station controller is connected at some level to the base stations it manages. Logical RAN connectivity shows this relationship without any intermediate devices, such as multiplexers.

LTE Control Plane
Displays a topology view of the LTE control plane.

LTE User Plane
Displays a topology view of the LTE user plane.

LTE S1-U
Displays a topology view of LTE S1-U connectivity.

LTE S5-U
Displays a topology view of LTE S5-U connectivity.

LTE S8
Displays a topology view of LTE S8 connectivity.

LTE S1-MME
Displays a topology view of LTE S1-MME connectivity.

LTE S10
Displays a topology view of LTE S10 connectivity.

LTE S11
Displays a topology view of LTE S11 connectivity.

LTE SGi
Displays a topology view of LTE SGi connectivity.

LTE Gx
Displays a topology view of LTE Gx connectivity.

LTE S3
Displays a topology view of LTE S3 connectivity.

LTE S4
Displays a topology view of LTE S4 connectivity.

LTE S6a
Displays a topology view of LTE S6a connectivity.

LTE S13
Displays a topology view of LTE S13 connectivity.

LTE X2
Displays a topology view of LTE X2 connectivity.

IMS Control Plane
Displays a topology view of IMS Control Plane connectivity.

IMX CX
Displays a topology view of IMX CX connectivity.

10. Click **Apply Changes**  .

    The topology you selected is displayed in the network map. Faulty devices are displayed with an associated event icon.

    Note: If you have configured cross-domain discovery, the **Network Hop View** results might include devices from a different domain to the domain in which the seed device is located. Hover the cursor over a device to see which domain it is located in.

Browsing the network using the Network Views GUI

Browse the network using the **Network Views** GUI in order to visualize the network based on geographical or other groupings. For example, you can browse subnets or device classes.

Before you begin

Before you can work with network views the following must be complete:

- The administrator must have successfully completed the first network discovery

- Network views must be configured for your user ID.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views**.
2. In the network views tree on the left of the widget, browse the network by expanding network view nodes of interest.
   Here are some examples:
   - To browse subnets, click the + symbol next to the Subnets node.
   - To browse VLANs, click the + symbol next to the Global VLANs node.
   - To browse device classes and see devices grouped into categories such as Linux, Sun, and Cisco, click the + symbol next to the Device Classes node.

     Note: Devices which the discovery process was unable to access using SNMP appear in the NoSNMPAccess sub-node, under the Device Classes node.
3. Click a network view.

   The network map displays subnets and devices in that network view. Faulty devices are displayed with an associated event icon.

Searching for devices within a view

Within the **Network Hop View** or **Network Views**, you can search for specific devices. For example, you can find devices that have high-speed interfaces.

About this task

If the device you want to find is not included in the current **Network Hop View** or Network View, you cannot find it using **Find in Map**  . You must search in another Network View or search for the device as a seed device.

Procedure

1. From the **Network Hop View** or **Network Views** network map, click **Find in Map**  .
2. From the **Find in Map** window, formulate search criteria by completing the relevant fields.

   For example, you can highlight all devices in the topology map that meet the following criteria.
   - Find all Cisco devices in the network map.
   - Find all devices with high speed interfaces.

   Table
   Select the database table that you want to search. The mainNodeDetails table lists network devices.

   Field
   Select the field whose value you want to search. The selection available for this field is automatically populated based on the chosen database.

   Comparator
   Select a comparator.

   Value
   Required. Type the value that you want to search for. You can use the percent character (%) or the asterisk (*) as wildcards.
3. Click **Find**. Devices that meet the criteria are highlighted with blue handles. The map is zoomed in to and centred on the devices, and the overview is toggled on.

Finding Cisco devices in the current view

Use this example query to find all Cisco devices in the current Hop View or Network View.

To formulate this query, select the `chassis` database table. This table contains properties of main node devices, such as switches and routers. Specify the `className` field from this table. Use the % wildcard character to indicate that the classname value must contain the letters "isco". The resulting query looks like this:

```
Table: chassis
Field: className
Comparator: like
Value: %isco%
```

This query finds devices with classnames such as the following:

- `Cisco26xx`
- `Cisco36xx`
- `Cisco72xx`
- `CiscoCat35xx`

Devices found by this query are highlighted in the network map using handles around the device.

Finding Ethernet interfaces in the current view

Use this example query to find interfaces in the current Hop View or Network View that are of type Ethernet.

To formulate this query, select the `Basic > interfaces` database table, and specify the `ifType` field from this table. Specify that the value of the `ifType` field must be equal to `ethernet-csmacd`.

```
Table: interfaces
Field: ifType
Comparator: =
Value: ethernet-csmacd
```

This query finds devices in the topology map that have Ethernet interfaces. Devices found by this query are highlighted in the network map using handles around the device.

Using quick search within a view

Within the **Network Hop View**, **Network Views** or **Path Views GUI** you can do a quick search for specific devices.

About this task

The quick search function searches data that is already showing in the map and does not require knowledge of database tables. The quick search is less complex and reaches results faster than other searches, as the quick search function does not search at the database level.

Procedure

1. Within either the **Network Hop View**, **Network Views** or **Path Views GUI**, click in the **Search** field that is located below the view.
2. In the **Search** field, enter a value or partial value for one of the following types of data attributes and press the return key. The value text is not case-sensitive by default.
   - Topology data
     - Display Name
     - IP Address

- Class Name
- Class Type
- Managed State
- Maximum Severity

- Tooltip data. When you hover over a node, tooltip information displays about the node. The information that is configured for tooltip can be used for a quick search.

3. A result pop-up menu displays devices that match your search and the matching data attribute. From the results pop-up menu, click one or multiple devices.

Results

The view displays the selected devices and the selected devices are highlighted.

Searching for a network view

If you have many network views, you can search through the network view tree to find the view you want.

About this task

To search for a particular network view name, complete the following steps.

Procedure

1. From the **Network Views** GUI, within the toolbar above the network view tree click the **Toggle search** button  in the toolbar.

   A search box is displayed below the toolbar, with a **Begin Search** button and **Clear Search** button.
2. Type a search query into the search box.

   Searches are not case-sensitive. You can use the percent character (%) or asterisk character (*) as a wildcard. Wildcards match zero or more characters.

   Remember: A wildcard can be used anywhere in the middle of the search phrase. If you do not specify a wildcard, a wildcard is automatically used at the front and end of the search phrase. Any wildcards actually specified at the font or the end will be silently ignored.
3. Click **Begin Search**  .

   Only views with names that match the search phrase are displayed. If a container matches the search, all its children are displayed. The search term is highlighted in the view names.
4. To display a network view, click the name of the view in the tree.
5. To clear the search and display the full tree with all nodes collapsed, click **Clear Search**  .

Visualizing devices in tabular layout

You can display the **Network Health View** and **Network Views** in a tabular layout. Displaying topology maps in tabular layout enables filtering and sorting of topology data.

About this task

In addition to the graphical views of your topology provided within the **Network Health View** and **Network Views**, you can also display the topology map in tabular layout.

Restriction: The following restrictions apply to the tabular layout:

- Network hop views cannot be displayed in tabular layout.

- The tabular layout lists nodes but does not display connections between network nodes. To view network connections, choose a different layout, such as symmetric or orthogonal.
- No hover help information is provided when you move your mouse over a node in the tabular layout. To view device hover help, choose a different layout, such as symmetric or orthogonal.
- When switching between tabular layout and other layouts, changes to device selection and column layout are not preserved.
- The tabular layout Fix Pack 5 can be exported as a Comma-Separated Values (CSV) file, but cannot be printed or saved as an image. To print the view, choose a different layout, such as symmetric or orthogonal.

To display the topology map in a tabular layout, complete the following steps.

Procedure

1. From the **Network Health View** or **Network Views**, click **Tabular layout** to display the topology map in table form.

   The following toolbar items are present when the network view is presented in tabular layout.

   Refresh
   Refreshes the view. By default, the view refreshes every 20 seconds.

   Save
   Saves the view or view container. This button appears only when a view is displayed.

   Hierarchical Layout
   Changes the format of the view to a hierarchical layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

   Symmetric Layout
   Changes the format of the view to a symmetric layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

   Orthogonal Layout
   Changes the format of the view to an orthogonal layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

   Circular Layout
   Changes the format of the view to a circular layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

   Grid Layout
   Changes the format of the view to a grid layout. This option is only available for views that cannot contain connectivity information, such as Unassigned views.

   Tabular Layout
   Changes the format of the view to a tabular layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

   Help
   Displays help for the portlet.

   Export as CSV
   Exports the current view to a downloaded Comma-Separated Values (CSV) file. The file contains the information about the devices that are displayed. If you export from the tabular layout, the exported data is in the same order as in the table, and is filtered using the same filters that are

applied to the table. If you export from another view, the order of the data is undefined, and includes every device in the view. Fix Pack 12 In Fix Pack 11 and earlier versions, the Export as CSV button is displayed only if you have write access to the view. In Fix Pack 12 and later versions, by default the button is always displayed. The administrator can revert to the Fix Pack 11 behavior by setting `topoviz.table.export.allow.always` property in the `topoviz.properties` file to `false`.

Pause 
Prevents the view from refreshing.

Tools 
Displays the context menu options for the device. These options are the same as in the right-click menu in other layouts. There is no right-click menu in the tabular layout.

Filter
Filter the contents of the table by entering a string in the **Filter** field and pressing the Return key. Delete the string to clear the filter.

For example, to find all rows that contain the string "snmp", type `snmp`. The search is case insensitive.

Note: If the table layout is refreshed by the system due to a change in data contained in the table, for example, updates to the **Maximum Severity** column, then the filter is reapplied before the refreshed view is displayed.

Restriction: You cannot use wildcard characters such as * or regular expressions in the **Filter**.

2. Sort and resize table columns using the following controls. Any settings made are valid for this session only.

Sort Column
Click the column header to sort that column in ascending order. Click the column a second time to sort the column in descending order. Further clicks toggle the column between descending and ascending order.

Resize a column
Click and drag the vertical line separator to the right of the column heading.

3. Fix Pack 5
Move columns by dragging them to the desired location.

4. Fix Pack 5
Ask your administrator if you need to add or change the columns that are displayed.

For more information on how to configure the columns that are displayed in the tabular layout, see “Configuring column display in the tabular view” on page 206.

Using entity smart search

Use entity smart search to search for an entity across all Network Manager domains or across a custom NCIM database table in an extended NCIM database.

An entity smart search has the following characteristics:

- Spans all Network Manager domains
- Provides for searches across an NCIM database table in an extended NCIM database
- Uses the entityName as the search parameter
- Uses a URL supplied to the Dashboard Application Services Hub.

An entity smart search has the following possible results:

- Single match -- The specified entityName is unique in the NCIM database.

- Multiple matches -- The specified entityName exists in more than one Network Manager domain and/or parent entity node.
- Zero matches -- No matching entities were found in the NCIM database.
- Error -- An error occurred and the entity smart search failed.

Performing an entity smart search across all domains

Use the entity smart search feature to search for an entity across all Network Manager domains.

Before you begin

An entity is a topology database concept. All devices and device components discovered by Network Manager are entities. You perform an entity smart search across all Network Manager domains by specifying a URL that contains the name of the entity. You specify this URL in the Dashboard Application Services Hub.

Note: You can use only the name of the entity when performing an entity smart search across all Network Manager domains.

About this task

To perform an entity smart search across all Network Manager domains specify the following URL to the Dashboard Application Services Hub:

```
http(s)://DASH_HOST:DASH_PORT/ibm/console/ncp_structureview/Search.do?
selectEntityName=entityName
```

where

- *DASH_HOST* -- Specifies the name of the host computer on which the Dashboard Application Services Hub server was installed.
- *DASH_PORT* -- Specifies the port number associated with the host computer on which the Dashboard Application Services Hub server was installed.
- *entityName* -- Specifies the name of the entity to search across all Network Manager domains. The *entityName* is case sensitive as it must match an existing value in the NCIM database.

  You can also specify spaces in the *entityName* by using the + (plus sign) or `%20` (percent sign followed by the number 20). For example, the space in the entity name `;SM 0001` can be specified as `;SM+0001` or `;SM%200001`.

  Note: The URL path is case sensitive (that is, all items in the path are lower case except for the upper case S in `Search`). The parameter name `selectEntityName` in the URL specification is also case sensitive.

Procedure

1. Log into the Dashboard Application Services Hub.
2. In the browser Location bar, specify the previously described URL.

   After the URL has been successfully submitted to the Dashboard Application Services Hub server there are four possible scenarios:

   - Single match -- The specified *entityName* is unique in the NCIM database. The **Structure Browser** is launched and the selected *entityName* is displayed in the context of the containing structure.
   - Multiple matches -- The specified *entityName* exists in more than one Network Manager domain and/or parent entity node. A new context page displays the results using the following format:

     ```
     $DOMAIN_NAME/$CONTAINMENT_PATH_BY_ENTITYNAME
     ```

     where

- *DOMAIN_NAME* -- Specifies the Network Manager domain in which the specified *entityName* resides.
- *CONTAINMENT_PATH_BY_ENTITYNAME* -- Specifies the list of entities that exist from the root entity to the entity specified in the entity smart search. Consider the following example where an entity smart search is performed on an entity called SM00189990:

  ```
  DOMAIN1 NAP02513002/SM02513016/SM00189990
  ```

  In the example, the containment path for the domain called DOMAIN1 specifies the following entities:

- Root entity -- The root entity is the first entity in the list. In this example, the root entity is NAP02513002.
- Repeater entity -- Zero or more repeater entities can follow the root entity. In the example, there is one repeater entity, SM02513016.
- Search entity -- This is the entity specified in the entity smart search. In the example, the search entity is SM00189990.

Note: For some search results there will only be a root entity and the entity specified in the entity smart search. For other search results there will be a root entity, one or more repeater entities, and the entity specified in the entity smart search.

- Zero matches -- A results page indicates there were no matches in the NCIM database for the specified *entityName*.
- Error -- A results page indicates an error has occurred and that the search should be attempted again.

Example

The following example shows the URL for an entity smart search across all Network Manager domains:

```
https://dash01.ibm.com:16311/ibm/console/ncp_structureview/Search.do?
selectEntityName=SM00071103
```

where

- dash01.ibm.com -- Specifies the host name of the computer on which the Dashboard Application Services Hub server was installed.
- 16311 -- Specifies the port number associated with the host computer on which the Dashboard Application Services Hub server was installed.
- SM00071103 -- Specifies the name of the entity to search across all Network Manager domains.

What to do next

Use the **Structure Browser** to navigate the internal structure of a device or to investigate the health of device components and isolate a fault within a network device. Specifically, the **Structure Browser** highlights the entity specified in the entity smart search.

Performing an entity smart search across a custom NCIM database table

Use the entity smart search feature to search for an entity across a custom NCIM database table in an extended NCIM database.

Before you begin

An entity is a topology database concept. All devices and device components discovered by Network Manager are entities. You perform an entity smart search across a custom NCIM database table by specifying a URL that contains the name of the entity and the name of the custom NCIM database table. You specify this URL in the Dashboard Application Services Hub.

About this task

To perform an entity smart search across a custom NCIM database table specify the following URL to the Dashboard Application Services Hub:

```
http(s)://DASH_HOST:DASH_PORT/ibm/console/ncp_structureview/Search.do?
selectEntityName=entityName&namespace=CUSTOM_TABLE.CUSTOM_FIELD
```

where

- *DASH_HOST* -- Specifies the name of the host computer on which the Dashboard Application Services Hub server was installed.
- *DASH_PORT* -- Specifies the port number associated with the host computer on which theDashboard Application Services Hub server was installed.
- *entityName* -- Specifies the name of the entity to search across a custom NCIM database table. The *entityName* is case sensitive as it must match an existing value in the specified NCIM custom database table. The *entityName* is linked to the entityId in the custom NCIM database table.

  You can also specify spaces in the *entityName* by using the + (plus sign) or `%20` (percent sign followed by the number 20). For example, the space in the entity name `;SM 0001` can be specified as `;SM+0001` or `;SM%200001`.

  Note: The URL path is case sensitive (that is, all items in the path are lower case except for the upper case S in `Search`). The parameter name `selectEntityName` in the URL specification is also case sensitive.
- *CUSTOM_TABLE* -- Specifies the name of the NCIM custom database table in the extended NCIM database in which to perform the search of the entity specified in *entityName*. This NCIM custom database table contains the two fields: entityId and *CUSTOM_FIELD*. The entityId is a foreign key to the entityNameCache table and must be unique for each entity across all domains. The entityId is automatically incremented.

  Note: You do not specify the entityId in the URL specification.
- *CUSTOM_FIELD* -- Specifies the name of the field to search within the NCIM custom database table. The entityId field in the NCIM custom database table in the extended NCIM database will reference the entityId field in the entityData table.

  Note: When using the extended namespace functionality, ensure that the NCIM custom database table forms a natural join to the NCIM.entityData table by entityId. After that, the user can put whatever data they want into the NCIM custom database table.

  The performance of the extended namespace search is dependent on the NCIM custom database having relevant up-to-date indexing.

  The following notes describe use of the `namespace` parameter and associated values:

  – The `namespace` parameter is not case sensitive
  – The parameter values, *CUSTOM_TABLE* and *CUSTOM_FIELD*, must be separated by a dot (.).
  – The parameter values, *CUSTOM_TABLE* and *CUSTOM_FIELD*, are not case sensitive and can include only alphabetic characters and the underscore (_) character. These parameter values must also begin with an alphabetic character.

Procedure

1. Log into the Dashboard Application Services Hub.
2. In the browser Location bar, specify the previously described URL.

   After the URL has been successfully submitted to the Dashboard Application Services Hub server there are four possible scenarios:

- Single match -- The specified *entityName* is unique in the NCIM custom database table. The **Structure Browser** is launched and the selected *entityName* is displayed in the context of the containing structure.
- Multiple matches -- The specified *entityName* exists in more than one Network Manager domain and/or parent entity node. A new context page displays the results using the following format:

  ```
  $DOMAIN_NAME/$CONTAINMENT_PATH_BY_ENTITYNAME
  ```

  where

  – *DOMAIN_NAME* -- Specifies the Network Manager domain in which the specified *entityName* resides.

  – *CONTAINMENT_PATH_BY_ENTITYNAME* -- Specifies the list of entities that exist from the root entity to the entity specified in the entity smart search. Consider the following example where an entity smart search is performed on an entity called `SM00189990`:

  ```
  DOMAIN1 NAP02513002/SM02513016/SM00189990
  ```

  In the example, the containment path for the domain called `DOMAIN1` specifies the following entities:

  – Root entity -- The root entity is the first entity in the list. In this example, the root entity is `NAP02513002`.

  – Repeater entity -- Zero or more repeater entities can follow the root entity. In the example, there is one repeater entity, `SM02513016`.

  – Search entity -- This is the entity specified in the entity smart search. In the example, the search entity is `SM00189990`.

  Note: For some search results there will only be a root entity and the entity specified in the entity smart search. For other search results there will be a root entity, one or more repeater entities, and the entity specified in the entity smart search.
- Zero matches -- A results page displays that indicates there were no matches in the NCIM custom database table for the specified *entityName*.
- Error -- A results page displays that indicates an error has occurred and that the search should be attempted again.

Example

The following example shows the URL for an entity smart search across an NCIM custom database table:

```
https://dash01.ibm.com:16311/ibm/console/ncp_structureview/Search.do?
selectEntityName=Tokyo&namespace=customns.location
```

where

- `dash01.ibm.com` -- Specifies the host name of the computer on which the Dashboard Application Services Hub server was installed.
- `16311` -- Specifies the port number associated with the host computer on which the Dashboard Application Services Hub server was installed.
- `customns` -- Specifies the name of the custom table in the extended NCIM database in which to perform the search of the entity specified in *entityName*.
- `location` -- Specifies name of the field to search within the `customns` custom table.
- `Tokyo` -- Specifies the name of the entity to search for in the `customns` custom table. (This entity is linked to the entityId in the `customns` custom database table.)

Chapter 17. Identifying network problems

You can identify network problems in two ways: using network views or using event lists.

About this task

Network views and event lists are presented in the GUI in the following ways:

Network view bookmarks
Subset of selected network views. Selection of network views to include in a bookmark is usually based on those network views the operator or operations group needs to monitor.

Network view libraries
Complete network views, showing all network devices and subnets as hierarchically organized views of a discovered network.

Event lists
Tivoli Netcool/OMNIbus Web GUI **Event Viewer** list displays device event data from the Tivoli Netcool/OMNIbus ObjectServer.

Network health view
The **Network Health View** displays topology and event data in a composite GUI, where topology data in the form of network view libraries or bookmarks is shown in the top widget, and event data in the **Event Viewer** is shown in the lower widget. Selection of a device from the network view libraries or bookmarks generates a list of events for that device in the **Event Viewer**.

Identifying problems using network view bookmarks

Use network view bookmarks to troubleshoot network problems.

Before you begin

Before you can work with network view bookmarks, you or the administrator must first create network view bookmarks by selecting network views from the existing network view libraries.

About this task

Network view bookmarks contain a subset of network views, tailored for the needs of the operator or operations group.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Bookmarks**.
2. In the **Network Views** tree on the left of the widget, expand the network view nodes by clicking the + symbols.
3. Select a network view with an event status icon of severity minor or higher.

   The network map displays subnets and devices in that network view. Faulty devices and subnets are marked with an event status icon. Names of faulty devices are highlighted in a color that corresponds to the event severity on that device. Hover over a device in a network view to display summary information about the device.

Identifying problems using network view libraries

Use network view libraries to view the results of a discovery or to troubleshoot network problems.

Before you begin

Before you can work with network view libraries the administrator must complete the following tasks:

- The first network discovery must have successfully completed.

- The administrator must configure network view libraries for you, either by dynamically generating network views or by creating custom network views.

About this task

You can use different types of network view libraries to monitor different types of devices or device technologies.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.

   By default, the network view tree contains a separate IP network view hierarchy per domain for each network technology; you will see an IP network view hierarchy only for each domain. Optionally you can add an LTE network view hierarchy for each domain. Do this by creating a template-based dynamic view using the lte_default network view template, as described in the *IBM Tivoli Network Manager User Guide*.
2. In the **Network Views** tree on the left of the widget, expand the network view nodes by clicking the + symbols.
3. Select a network view with an event status icon of severity minor or higher.

   The network map displays subnets and devices in that network view. Faulty devices and subnets are marked with an event status icon. Names of faulty devices are highlighted in a color that corresponds to the event severity on that device. Hover over a device in a network view to display summary information about the device.

Related tasks

Investigating faulty devices
You can perform a range of diagnosis tasks on devices and subnets. You can show related network events. You can also drill into faulty network devices, display SNMP MIB values, log into the faulty devices, and investigate the routes to devices.

Monitoring subnets

You can determine whether there are events on any of the devices in your subnets. Use the Subnets network view to monitor subnets for events.

About this task

To monitor subnets using the **Network Views**, proceed as follows:

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the Subnets network view nodes.
3. Determine the most severe event in each subnet based on the associated event status icon.
4. Select the Subnet node with an event status icon of severity minor or higher.

   The topology display panel displays devices in that network view and marks faulty devices with an event status icon. Names of faulty devices are highlighted in a color that corresponds to the event severity on that device.

What to do next

You can perform any of the following actions on this device:

- Investigate network routes to this device
- Drill into the device using the **Structure Browser** to investigate the health of device components
- Log into the device to examine processes running on the device

- Browse the MIB associated with this device

Related tasks

Displaying events on a subnet
You can display events on all devices in a subnet by running the **Show Events** command on a Subnet network view.

Monitoring device classes

You can determine whether there are events on any devices of a particular vendor or model. For example, you can monitor events on all your Sun devices or on all your Cisco28xx devices.

About this task

Use the Device Classes network view to monitor devices of a particular vendor or model for events. The device classes reflect the Active Object Class (AOC) hierarchy. AOCs are based on vendor, type, and model family. To monitor device classes such as Linux devices, Sun workstations, and Windows servers, proceed as follows.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the Device Classes network view nodes.
3. Identify a particular class of devices and locate the associated event status icon.

   This icon indicates the most severe event on that device class.

   For example, identify the Linux node and locate the associated event status icon. This icon tells you the most severe event on the Linux devices.
4. Select a faulty device class from the network view tree.
   For example, if the Linux node has an event status icon of severity minor or higher then select it.

   The topology display panel displays devices of the selected class and marks faulty devices with an event status icon.

What to do next

You can perform any of the following actions on this device:

- Investigate network routes to this device
- Drill into the device using the **Structure Browser** to investigate the health of device components
- Log into the device to examine processes running on the device
- Browse the MIB associated with this device

Related tasks

Displaying events on a device
Use this network troubleshooting procedure to display all events on a faulty device.

Monitoring links

By monitoring the links between devices, you can determine the status of the devices connected by the link. In addition, you can launch tools to diagnose the underlying problem.

Before you begin

Your administrator can configure links to display event information or link status information from poll policies Fix Pack 11. Links can be displayed as colored, or colored with an associated severity icon. They can also configure the thickness of the line based on the connection speed of the link. By default, these options are on.

About this task

The display of link status can be customized for each individual view.

Procedure

1. Open any view that displays the links between devices.

   An error status for a link is indicated by a line with a color corresponding to the alert status, as well as an associated severity status icon, if configured.
2. Hover over the link to display information about the link.
3. Click a link to select it.

   Fix Pack 4 If IP SLA discovery has been configured, selecting a link displays the probes that are monitoring the link.
4. Right-click a link to open the right-click menu.

What to do next

From the right-click menu, you can do any of the following tasks:

- Display the link events in the **Event Viewer**. If you change the severity status of an event in the **Event Viewer**, this status will be filtered back to the link.
- Ping the link end points.
- Diagnose an underlying problem. For example, you can ping the IP addresses either side of a link.
- Unmanage the link and associated devices to prevent the devices at the link's end points from being polled. Typically, you would unmanage a link while maintenance is carried out, and then manage it again once it has been restored to working order.

  Note: When you unmanage a link, you unmanage all connected interfaces. This is indicated by half-spanner icons at each end of the link.
- Manage the link and associated devices.

Related concepts

Device connectivity

You can display the network at different OSI layering levels in the network map. Change the connectivity layer setting if you wish to focus on subnet membership, OSI layer 2 connections, OSI layer 3 connections, Protocol Independent Multicast (PIM), or Internet Protocol Multicast (IPM) routes.

Related tasks

Customizing line thickness in topology maps

You can customize the thickness of the lines connecting network entities based on the speed of the connection between them.

Configuring Link status option

You can configure the information that is displayed on links between devices. You can choose to display information from events or poll policies.

Setting Link status option

You can change the settings for links status option for each network view. To enable the links to show poll policies, administrator has to enable the links to show policies. If it is not enabled, Link status option button is not displayed.

About this task

You can set Link status options on any view for which you have write permission. You can set this option on an ancestor view, which allows all the descendant views to inherit these settings from their ancestor. Then, you can set different options on a descendant view that overrides the ancestor view's settings. You can open the view for which you want to set the options and make the changes as required.

You can delete the Link status option on the views for which you have write permission. You can use delete button in the Link status options dialogue box to delete the Link status options for the current view. If the Link status options deleted and saved the view, then the view inherits the options from the nearest ancestor view. If no ancestor view has Link status options configured, then the view uses the defaults set by the administrator.

User can perform the following procedure to set poll policies:

Procedure

1. In the GUI, navigate to the **Network Views**. Click **Link status option** button to open the **Link status options** dialogue box.
2. If you color the links by poll policy value, you can select the policy you want to view by selecting the policy from **Color links by this poll policy** drop-down list.

   The list displays only the policies that are applicable to this view.

   The status line at the bottom right of the window displays which policy is being used to color links. If you are coloring the links on events, it displays as **Link Status: Events**.
3. To choose whether high or low values represent a more severe problem for the policy, select **High policy values are more severe** or **Low policy values are more severe** in the **Which policy values are more severe?** section.
4. You can choose the function that it uses to aggregate by selecting the following options:
   - Maximum: Highest value on any interface
   - Minimum: Lowest value on any interface
   - Sum: Total of the values on all the interfaces
   - Average: Arithmetic mean of the values on all the interfaces

   All of these functions ignore interfaces that do not currently have a value for the policy. When you hover the mouse over a link, the tooltip shows the aggregated policy value and the value of the policy on each interface.
5. Select the option **Thresholds scale to current values** (to let the GUI work out the thresholds automatically based on the current values of the policy within the network view) or **Thresholds are absolute** (to enter your own thresholds).

   When you select Thresholds scale to current values, the GUI divides the range between the maximum and minimum policy values into equally-sized intervals. The GUI converts the policy value to a color based on thresholds. The colors are the same as those used for events.
6. Click **Apply and Close** to save the options and exit the Link status options dialogue box.

   These settings are per-view, not per-user. If you have write permission on the view, you can save the settings to the database.

Related tasks

Configuring Link status option
You can configure the information that is displayed on links between devices. You can choose to display information from events or poll policies.

Monitoring Border Gateway Protocol (BGP) networks

You can determine whether there are events on any devices in your BGP networks. Use the BGP Network network view to monitor BGP networks for events.

About this task

To monitor BGP networks, proceed as follows.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the BGP Network node.

   For each top-level node, an event status icon to the right of the tree indicates the status of devices in that node.
3. Determine the most severe event in each BGP network based on the associated event status icon.
4. If a BGP network node has an event status icon of severity minor or higher then select it.

   The network map displays devices in that BGP network and marks faulty devices with an event status icon.
5. Check the status of the following devices within the network map.
   a) *EBGP speaker devices*:

      EBGP speaker devices connect BGP ASs and are essential for correct BGP network operation. In the network map, an EBGP speaker device appears as a member of one BGP AS but is also connected to a separate EBGP speaker device that is a member of a different BGP AS.
   b) *Route reflector (RR) devices*:

      Route reflector devices are responsible for communicating with a subset (cluster) of routers within an AS. Route reflectors perform peer operations with each other and hence avoid the need to fully mesh BGP ASs. Correct operation of route reflectors is therefore essential for correct connections within the BGP AS.

      Route reflectors are marked with the label RR within the network map.

Related tasks

Retrieving BGP information
Retrieve Border Gateway Protocol (BGP) information from devices in order troubleshoot BGP-related network issues.

Monitoring Open Shortest Path First (OSPF) routing domains

You can determine whether there are events on any devices in your OSPF routing domains and OSPF areas. Use the OSPF Routing Domains network view to monitor OSPF routing domains and OSPF areas for events.

About this task

To monitor OSPF routing domains and OSPF areas, proceed as follows.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the OSPF Routing Domains node.

   For each top-level node, an event status icon to the right of the tree indicates the status of devices in that node.
3. Determine the most severe event in each OSPF routing domain based on the associated event status icon.
4. If an OSPF routing domain node has an event status icon of severity minor or higher, then select it.

   The network map displays devices in that routing domain and marks faulty devices with an event status icon.
5. Check the status of the following devices within the network map.
   a) *Area border routers (ABRs)*:

      These routers connect two or more OSPF areas and provide routing to other OSPF areas via the backbone network.

      ABRs are marked with the label ABR within the network map.

b) *Autonomous system border routers (ASBRs)*:

These routers communicate with other networks using an IGP protocol.

ASBRs are marked with the label ASBR within the network map.

c) *Designated routers (DRs) and backup designated routers (BDRs)*:

DRs are OSPF router interfaces designated to provide a source for routing updates and so reduce the need to fully mesh connections when multi-access technologies, such as Ethernet, are used. A backup designated router (BDR) is always kept up to date to ease the transition should the primary DR fail.

DRs are marked with the label DR within the network map. Backup DRs are marked with the label BDR within the network map.

d) *Type 2 LSAs*:

Generated for every transit network within an area. A transit network has at least two directly attached OSPF routers. Ethernet is an example of a Transit Network. A Type 2 LSA lists each of the attached routers that make up the transit network and is generated by the DR.

Related tasks

Retrieving OSPF information

Retrieve Open Shortest Path First protocol (OSPF) information from devices in order to troubleshoot OSPF-related issues.

Monitoring multicast groups and routes

You can monitor multicast groups and routes to determine whether there are any events on the devices in those groups and routes.

About this task

PIM groups, IGMP groups, and IP Multicast routes can only be monitored if the discovery has been configured to discover them. Views for these groups and routes are created automatically; you can also create them manually.

To monitor multicast groups, complete the following tasks.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
   - In the navigation tree on the left of the widget, click the + symbol to expand the **IGMP Groups** node. A list of the IGMP groups that have been discovered is displayed.
   - In the navigation tree on the left of the widget, click the + symbol to expand the **PIM network** node. A list of the PIM groups that have been discovered is displayed.
   - In the navigation tree on the left of the widget, click the + symbol to expand the **Multicast Routing MDTs** node. A list of the IP multicast routes that have been discovered is displayed. Multicast Distribution Trees (MDTs) are named according to the (source, group address) notation. For example, an (S,G) notation of (172.20.1.6,224.0.0.1) shows that a device with an IP address of 172.20.1.6 is a source sending data to the 224.0.0.1 group.
2. Determine the most severe event in each group based on the associated event status icon.

Monitoring MPLS Traffic Engineered tunnels

You can monitor MPLS Traffic Engineered (TE) tunnels to determine whether there are any events on the devices that comprise the tunnels.

About this task

MPLS TE tunnels can only be monitored if the discovery has been configured to discover them.

To monitor MPLS TE tunnels, complete the following tasks.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the **MPLS TE** node.
   A list of the MPLS TE tunnels that have been discovered is displayed.
3. Determine the most severe event in each tunnel based on the associated event status icon.

Fix Pack 4 Monitoring IP Service Level Agreement (IP SLA) configurations

You can visualize probes that are configured to monitor IP SLA response times, and their source and destination devices, by using network views.

Before you begin

Before using IP SLA views, configure IP SLA discovery.

About this task

You can view the events status of devices that act as a network probe source or target. The IP SLA views also show network probes attached by a dotted line to the source and target, where known. IP SLA views are created automatically; you can also create them manually.

To monitor devices running IP SLA, complete the following tasks.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the **IPSLA views** node.
   A list of the IP SLA Probes that have been discovered is displayed.
3. Click the name of the Probe to open a network view showing devices that are monitored by that Probe type.
   If you configured the Netcool/OMNIbus Knowledge Library for use with the SNMP Probe, IP SLA events are shown on the devices. The links between sources and targets are colored according to event severity.
4. Select a link between devices, in the network views or in the **Network Hop View**, to display the Probes that are monitoring the link.
5. Double-click a Probe icon, in the network views or in the **Network Hop View**, to open the Probe in the **Structure Browser**.

Monitoring VPLS VPNs

You can monitor Virtual Private LAN Service Virtual Private Networks (VPLS VPNS) to determine whether there are any events on the devices in the networks.

About this task

VPLS VPNs can only be monitored if the discovery has been configured to discover them. VPLS VPN views are created automatically; you can also create them manually.

To monitor VPLS VPNs, complete the following tasks.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.

2. In the navigation tree on the left of the widget, click the + symbol to expand the **VPLS VPN views** node.

   A list of the VPLS VPNs that have been discovered is displayed.
3. Determine the most severe event in each VPN based on the associated event status icon.

Monitoring aggregated network domains

You can monitor events from multiple domains within the same network view.

Before you begin

In order to monitor cross-domain network views, you must first create some cross-domain network views.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand a network view that was created in the AGGREGATION domain.
3. Determine the most severe event based on the associated event status icon. You can hover the cursor over a device to see what domain the device is in.

Monitoring LTE networks

You can monitor events from devices in LTE networks.

Before you begin

In order to monitor LTE network views, you must first create a template-based dynamic view using the lte_default network view template. For more information see the *IBM Tivoli Network Manager User Guide*.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Views** > **Libraries**.
2. In the navigation tree on the left of the widget, click the + symbol to expand the top-level LTE network view container.
3. Navigate the LTE network view hierarchy to find a network view of interest.
4. Determine the most severe event in each LTE network view based on the associated event status icon. The topology display panel displays devices in the selected view and marks faulty devices with an event status icon.

Identifying problems using event lists

You can monitor all network events in a single event list. Use the **Fault-Finding View** to monitor network events.

About this task

The **Fault-Finding View** shows events in the **Event Viewer**. When you click on an event, the **Network Hop View** GUI displays connectivity for the device on which the event occurred.

To monitor all network events, complete the following steps.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Fault-Finding View**.

   The **Fault-Finding View** page appears with the **Event Viewer** widget above and the **Network Hop View** widget below.

Note: When you first open the **Fault-Finding View** page, the **Event Viewer** widget displays all events in the ObjectServer and the **Network Hop View** widget is empty.

2. Select an event of interest in the **Event Viewer**, or right-click an event and then click **Broadcast Topology Context**.

   The **Network Hop View** GUI now displays the network topology related to the selected event.

   Restriction: Results vary if you select multiple events in the **Event Viewer**.

   - If all the selected events occurred on the same network device, then the **Network Hop View** widget only displays the network topology related to that device.
   - If the selected events occurred on different devices, then the **Network Hop View** widget does not display any network topology .

Related concepts

About network troubleshooting

Network Manager provides several ways for troubleshooting network problems, including network views, event lists, Path Views, and the Structure Browser.

Related tasks

Investigating events

Use features of the **Event Viewer** to support network troubleshooting. You can use the **Event Viewer** to show affected network devices, identify root-cause events, and identify events that have a major service impact.

Using the Network Health View

Use the Network Health View to display events on a device.

About this task

The **Network Health View** displays topology and event data in a composite GUI, where topology data in the form of network view libraries or bookmarks is shown in the top widget, and event data in the **Event Viewer** is shown in the lower widget. Selection of a device from the network view libraries or bookmarks generates a list of events for that device in the **Event Viewer**.

Note: When you first open the **Network Health View** page, the **Event Viewer** widget displays all events in the ObjectServer.

To open the **Network Health View**, complete the following steps.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Health View**.
2. Display a network view of interest in the **Network Views** widget.
3. Select a single device in the network map.

   The contents of the **Event Viewer** widget are filtered to display only the events that occurred on the selected device.

   Restriction: The contents of the **Event Viewer** widget are not filtered in the following cases:

   - Multiple devices are selected in the **Network Views** widget.
   - A device is found and selected in the network map following a Find in Map operation.

   In these cases, no filter is applied and the **Event Viewer** displays all events in the ObjectServer.

Related concepts

About network troubleshooting

Network Manager provides several ways for troubleshooting network problems, including network views, event lists, Path Views, and the Structure Browser.

Fix Pack 2 Viewing devices in geographical context

Use the **GIS Device Map** to view devices and events in their geographical context. The **GIS Device Map** is like a Network View that is superimposed on a geographical map.

About this task

Procedure

1. Open the **GIS Device Map**:
   - From the **Network Views**, **Network Hop View**, or **Path Views GUI** that contains devices with geographical information, select one or more devices and right-click. Choose **Show on Map**.
   - Click **Incident** > **Network Geography** > **GIS Device Map**.

   The **GIS Device Map** is displayed.

   Fix Pack 3 When the **GIS Device Map** is displayed full screen, some mapping providers display an overview map.
2. Review the device and location icons to see events on devices or locations.

   The following icons are available:

   Devices
   Devices are represented by the same icons that are used in network views. The status of devices is shown on the map in the same way as in a Network View. Hover over a device to view details about the device, including events on the device, location data, and discovery data. Right-click on the information window to show more information. For example, you can open the Structure Browser or Hop View for a device. You can also show events on the device.

   Links
   The status of links is shown on the map in the same way as in a Network View. Hover over a link to display information about the link, including the topology layer over which the link runs, and event status. Click on any row within the information window to show more information. For example, you can open the Structure Browser or Hop View for a device on one end of the link. You can also show events on the link.

   Locations
   Locations are represented by building icons. Locations are groups of devices in the same physical location. You can take the following actions on devices:

   Display contained devices
   To display all the devices in a location, double-click the location. A window displays that shows the devices in the location, and the aggregate event status of those devices.

   Filter contained devices
   Click the **Filter** icon to chose which devices to display for that location. You can filter by any of the available columns. You can create multiple filter conditions.

   View device details
   Hover over a device to view details about the device, including events on the device, location data, and discovery data.

   Loopback links
   Links to all devices in a location are represented by a loopback link icon (a circle). Click on a location loopback link to view the constituent links.
3. To filter the items that are shown in the map, click the **Map Configuration** icon in the upper left of the **GIS Device Map**. Select the **Topology Filtering** tab in the **Map Configuration** window.
   a) Select domains in the **Domain** section to include and exclude devices by domain.

b) Select device classes in the **Device Class** section to include and exclude devices by class.

c) Select the option in the **Connectivity** section to display or hide links between devices or locations.

d) Select the option in the **Connectivity** section to enable or disable links within locations.

e) Select network layers in the **Connectivity** section to include and exclude links on a particular network layer.

4. To configure how event status is shown on the **GIS Device Map**, click the **Topology Status** tab in the **Map Configuration** window.
   a) Select the option to enable or disable event status.
   b) Select a severity less than which status is not displayed for devices and locations.
   c) Select a severity less than which status is not displayed for links.
5. To configure how the topology is displayed, click the **Topology Rendering** tab in the **Map Configuration** window.

   Settings last for the current session.
   a) If regional aggregation has been configured, select **Aggregate Locations to Regions** > **Enable** to group devices automatically to the highest regional hierarchy available in the geographical view.
   b) Select the base layer to display from the **Base Layer** list.
   c) Select the custom layers to display from the **Custom Layers** list.

Related tasks

Enabling regional aggregation for geographical views
You can group locations into cities, group cities into states, and group states into countries. This grouping is called regional aggregation.

Scoping and filtering geographical views
To improve visibility and performance, you might want to limit the devices that are displayed in geographical views.

Fix Pack 2 Showing events in geographical context

Use the **GIS Device Health View** to view events and devices in their geographical context. The **GIS Device Health View** consists of the **GIS Device Map** displayed above the **Event Viewer**.

About this task

You can view events in the **Event Viewer** section of the **GIS Device Health View** by using the standard controls for the **Event Viewer**.

Procedure

1. Click **Incident** > **Network Geography** > **GIS Device Health View**.

   The **GIS Device Health View** is displayed.
2. Select one or more devices in the **GIS Device Map** to display events for those devices in the **Event Viewer**.
3. Select a location in the **GIS Device Map** to display events for the devices contained by that location in the **Event Viewer**.
4. Select an event in the **Event Viewer** to update the map to show the affected device.

   This feature can be disabled by an administrator.
5. Review the device and location icons to see events on devices or locations.

   The following icons are available:

   Devices
   Devices are represented by the same icons that are used in network views. The status of devices is shown on the map in the same way as in a Network View. Hover over a device to view details about

the device, including events on the device, location data, and discovery data. Right-click on the information window to show more information. For example, you can open the Structure Browser or Hop View for a device. You can also show events on the device.

Links

The status of links is shown on the map in the same way as in a Network View. Hover over a link to display information about the link, including the topology layer over which the link runs, and event status. Click on any row within the information window to show more information. For example, you can open the Structure Browser or Hop View for a device on one end of the link. You can also show events on the link.

Locations

Locations are represented by building icons. Locations are groups of devices in the same physical location. You can take the following actions on devices:

Display contained devices

To display all the devices in a location, double-click the location. A window displays that shows the devices in the location, and the aggregate event status of those devices.

Filter contained devices

Click the **Filter** icon to chose which devices to display for that location. You can filter by any of the available columns. You can create multiple filter conditions.

View device details

Hover over a device to view details about the device, including events on the device, location data, and discovery data.

Loopback links

Links to all devices in a location are represented by a loopback link icon (a circle). Click on a location loopback link to view the constituent links.

6. To filter the items that are shown in the map, click the **Map Configuration** icon in the upper left of the **GIS Device Map**. Select the **Topology Filtering** tab in the **Map Configuration** window.
   a) Select domains in the **Domain** section to include and exclude devices by domain.
   b) Select device classes in the **Device Class** section to include and exclude devices by class.
   c) Select the option in the **Connectivity** section to display or hide links between devices or locations.
   d) Select the option in the **Connectivity** section to enable or disable links within locations.
   e) Select network layers in the **Connectivity** section to include and exclude links on a particular network layer.
7. To configure how event status is shown on the **GIS Device Map**, click the **Topology Status** tab in the **Map Configuration** window.
   a) Select the option to enable or disable event status.
   b) Select a severity less than which status is not displayed for devices and locations.
   c) Select a severity less than which status is not displayed for links.

Related tasks

Scoping and filtering geographical views

To improve visibility and performance, you might want to limit the devices that are displayed in geographical views.

Chapter 18. Diagnosing network problems

Diagnose network problems using the network troubleshooting tools available in Network Manager.

Investigating faulty devices

You can perform a range of diagnosis tasks on devices and subnets. You can show related network events. You can also drill into faulty network devices, display SNMP MIB values, log into the faulty devices, and investigate the routes to devices.

About this task

Related tasks

Investigating network connections
Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

Retrieving device information
Retrieving device information provides important information on the devices in your network to support troubleshooting. Device information includes device configuration information, domain information, and detailed interface, protocol, and routing information.

Investigating the health of device components
Investigate the health of device components in order to isolate the fault within a network device.

Retrieving MIB information
Retrieve MIB variable information from network devices to diagnose network problems.

Using the Device View

Use the **Device View** to display events, poll data, and interface information about a particular device.

About this task

The **Device View** is a composite GUI tab that is composed of the following widgets, listed clockwise from the top left:

- **Network Hop View**
- **Top Performers**
- **Event Viewer**
- **Structure Browser**

In order to view the **Device View**, your user must have the `ncp_networkview` role. You must also have the appropriate roles for the portlets within the page. To administer the page, you must have the `ncp_networkview_edit` user role.

To view device information in the **Device View**, complete the following steps.

Procedure

1. Open the **Device View** using one of the following methods:
   - Click the **Incident** icon and select **Network Availability** > **Device View**.
   - Right-click a device in the **Network Views** or **Network Hop View** and select **Find in** > **Device View**.

   If the **Device View** was opened from a specific device, that device is displayed in the **Network Hop View** widget. If you opened the **Device View** from the **Incident** menu, the **Network Hop View** is empty and you must search for a device in order to display information.

2. Select a device in the **Network Hop View** widget.

   The other widgets update to display information about the device that is selected in the **Network Hop View**.

   - The **Top Performers** widget shows poll data for the device.
   - The **Event Viewer** widget shows events for the device.
   - The **Structure Browser** widget shows the containment of the device.

Displaying related events

You can retrieve event data associated with faulty devices and subnets.

Displaying events on a device

Use this network troubleshooting procedure to display all events on a faulty device.

About this task

To display events on a device:

Procedure

1. From the **Network Hop View** or **Network Views**, identify a faulty device in the network map.
2. Right-click the faulty device and click **Show Events**.

   An **Event Viewer** opens in a separate browser window containing the events on the selected device.

What to do next

You can now perform any of the following actions on these events:

- Identify the root cause of any of these events.
- Identify service-affected events within this event list.

Related tasks

Investigating events

Use features of the **Event Viewer** to support network troubleshooting. You can use the **Event Viewer** to show affected network devices, identify root-cause events, and identify events that have a major service impact.

Displaying events on a subnet

You can display events on all devices in a subnet by running the **Show Events** command on a Subnet network view.

About this task

To display events on devices in a subnet:

Procedure

1. In the network view tree in the **Network Views**, expand the Subnets node.
2. Determine the most severe event in each subnet based on the associated event status icon.
3. In the network map, right-click a subnet and choose **Show Events**.

   An **Event Viewer** appears in a separate browser window containing the events on the selected subnet.

What to do next

You can perform any of the following actions on these events:

- Identify the root cause of any of these events.

- Identify service-affected events within this event list.

Related tasks

Investigating events

Use features of the **Event Viewer** to support network troubleshooting. You can use the **Event Viewer** to show affected network devices, identify root-cause events, and identify events that have a major service impact.

Displaying events for a network view

Display events for all devices in a network view by clicking the icon next to the view name.

About this task

The event icon next to each network view shows the highest level of alert on a device in the network view.

To view all events on devices in a network view, click the event icon next to the view name. An **Event Viewer** opens in a separate browser window containing the events on the selected network view.

Displaying a Network Hop View related to a network view

You can switch from a network view containing a device to a **Network Hop View** containing the same device. Switch from a network view to a **Network Hop View** to navigate around the network by specifying increasing numbers of hops, or connections, from the faulty device.

About this task

To switch from a network view to a **Network Hop View**.

Procedure

1. In the **Network Views** network map identify a device.
2. Right-click the device and click **Find in Network Hop View**.

   The **Network Hop View** appears in a separate browser window centred around the selected device.

What to do next

You can perform any of the following actions on this device:

- Investigate network routes to this device
- Drill into the device using the **Structure Browser** to investigate the health of device components
- Log into the device to examine processes running on the device
- Browse the MIB associated with this device

Displaying network views related to a Network Hop View

You can determine which subnets, VLANs, or other network collections a device forms part of by switching from the **Network Hop View** to the **Network Views**.

About this task

To switch from the **Network Hop View** to the **Network Views**:

Procedure

1. In the **Network Hop View** topology display panel right-click a device and click **Find in Network View**.
2. Proceed as follows:

   - If a network view appears in a separate browser window, this means that the device is found only in one network view.

- If you are presented with a list of network views, this means that the device is found in more than one network view. Select the network view of interest and click **OK**.

Investigating events

Use features of the **Event Viewer** to support network troubleshooting. You can use the **Event Viewer** to show affected network devices, identify root-cause events, and identify events that have a major service impact.

About this task

Note:

Unmanaged events are events received from Tivoli Netcool/OMNIbus probes (and possibly from other event sources) on devices or interfaces that have been marked as Unmanaged in Network Manager or Tivoli Netcool/OMNIbus.

An unmanaged device is usually marked Unmanaged because it is undergoing maintenance and may therefore generate unnecessary network events. Unmanaged interfaces might exist on a manged device but were not discovered by Network Manager. Network Manager can filter out unmanaged events from the **Event Viewer** in the following ways:

- Filtering out the unmanaged events so that they do not appear at all in the **Event Viewer**.
- Configuring the **Event Viewer** to display the NmosManagedStatus field. Any value greater than zero indicates an unmanaged device.

Check with your network administrator on how the system is configured to handle the presentation of unmanaged events in the **Event Viewer**.

Related tasks

Viewing events in the Event Viewer
You can use the **Event Viewer** to see all network events.

Displaying related topology views

Topology views show the network devices affected by an event. You can display two types of topology view: network views and the **Network Hop View**.

Displaying the Network Hop View related to an event

Display the **Network Hop View** related to an event to see the affected network device in context. This shows the network device affected by an event together with a network map of the connected devices. You can also specify a number of hops, or device connections, from the affected device.

Before you begin

Before you display a related **Network Hop View**, ensure that the event to investigate is selected in the **Event Viewer**.

About this task

To display the **Network Hop View** related to an event:

Procedure

1. From an **Event Viewer** window, right-click an event and click **Find in Network Hop View**.

   The **Network Hop View** opens in a separate browser window. The network map is centered around the device affected by the selected event. The **Seed device** field is populated with the IP address of the device on which the alert was raised.
2. Use the navigation features in the **Network Hop View** toolbar to move around the network.

What to do next

You can perform any of the following actions on this device:

- Investigate network routes to this device
- Drill into the device using the **Structure Browser** to investigate the health of device components
- Log into the device to examine processes running on the device
- Browse the MIB associated with this device

Related tasks

Investigating network connections
Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

Retrieving device information
Retrieving device information provides important information on the devices in your network to support troubleshooting. Device information includes device configuration information, domain information, and detailed interface, protocol, and routing information.

Retrieving MIB information
Retrieve MIB variable information from network devices to diagnose network problems.

Investigating the health of device components
Investigate the health of device components in order to isolate the fault within a network device.

Displaying network views related to an event

Display network views related to an event to see the affected network device in context. For example, the affected device may belong to a VLAN (one network view) and may also belong to the Sun device class (another network view).

Procedure

1. Select an event in the **Event Viewer**.
2. In the **Event Viewer** window, right-click and then click **Find in Network View**.
3. Proceed as follows:
   - If a network view appears in a separate browser window, this means that the affected device is found only in one network view.
   - If you are presented with a list of network views, this means that the affected device is found in more than one network view. Select the network view of interest and click **OK**.
4. Use the features in the **Network Views** toolbar to examine the devices in the network map.

What to do next

You can perform any of the following actions on this device:

- Investigate network routes to this device
- Drill into the device using the **Structure Browser** to investigate the health of device components
- Log into the device to examine processes running on the device
- Browse the MIB associated with this device

Related tasks

Investigating network connections
Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

Retrieving device information

Retrieving device information provides important information on the devices in your network to support troubleshooting. Device information includes device configuration information, domain information, and detailed interface, protocol, and routing information.

Retrieving MIB information
Retrieve MIB variable information from network devices to diagnose network problems.

Investigating the health of device components
Investigate the health of device components in order to isolate the fault within a network device.

Investigating root cause

A single network problem may generate multiple events. Use root-cause analysis tools to determine a device that is causing other devices to show faults.

About this task

The event record contains a field that indicates whether an event is a root-cause or a suppressed event. The network administrator can configure the **Event Viewer** to display this field.

For information on root-cause scenarios and examples, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

About event correlation and root-cause analysis

Events received from network devices are correlated with the network topology. This enables the system to determine root-cause events and provides the ability to switch between event data and network topology data.

Event correlation is the ability to analyze an event on one device and calculate the impact on each connected device in the network topology. By performing event correlation on each event received by the Tivoli Netcool/OMNIbus ObjectServer, the system is able to provide the following capabilities:

- Root-cause analysis
- Ability to switch between event data and network topology data

Root-cause analysis

Based on knowledge of the network topology, the system determines which devices are inaccessible due to other network failures. The system suppresses the events on these inaccessible devices and marks them in the **Event Viewer** as symptom events. The system marks the non-symptom events as root cause events.

Root cause events are differentiated from symptom events in the **Event Viewer** in the following ways:

- Root-cause events have a higher severity than symptom events. This ensures that root-cause events are given higher priority.
- The system marks root-cause events and symptom events using a field in the event record held in the ObjectServer. This provides the ability to identify the root cause event related to symptom events.

Ability to switch between event data and network topology data

This capability provides two approaches to network troubleshooting.

- You can initially identify network problems using events. Starting from an event in the **Event Viewer**, you can display a network map showing the affected device and the topology around that device.
- Alternatively, you can initially identify network problems using topology data. Starting from a network view or the **Network Hop View** containing a faulty device, you can display an **Event Viewer** showing all the events for that device.

Identifying root cause events

A single network problem may generate multiple events. You can use the **Event Viewer** to identify the root-cause event.

Before you begin

Before you issue the command to identify the root-cause event, ensure that at least one event is selected in the **Event Viewer**.

About this task

To identify root-cause events:

Procedure

1. From an **Event Viewer** window, right-click an event and click **Show Root Cause**.
   An **Event Viewer** opens in a separate browser window containing the root-cause event.
2. Use the features in the **Event Viewer** to further investigate this event.

What to do next

You can perform any of the following actions on this event:

- Display related topology views
- Drill into the affected device to investigate the health of device components
- Browse the MIB associated with the affected device

Related tasks

Displaying related topology views
Topology views show the network devices affected by an event. You can display two types of topology view: network views and the **Network Hop View**.

Retrieving related MIB information
As part of network troubleshooting activity, you can retrieve MIB information for the device associated with a specified event in the **Event Viewer**.

View the structure of the network device related to an event
As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Event Viewer**.

Investigating symptom events

Starting from a root-cause event you can use the **Event Viewer** to identify the symptom events.

Before you begin

Before you issue the command to identify the symptom events, ensure that at least one event is selected in the **Event Viewer**.

Procedure

1. From an **Event Viewer** window, right-click an event and click **Show Symptoms**.
   An **Event Viewer** opens in a separate browser window containing symptom events.
2. Use the features in the **Event Viewer** to further investigate these events.

What to do next

You can perform any of the following actions on these events:

- Display related topology views

- Drill into the affected device to investigate the health of device components
- Browse the MIB associated with the affected device

Related tasks

Displaying related topology views
Topology views show the network devices affected by an event. You can display two types of topology view: network views and the **Network Hop View**.

Retrieving related MIB information
As part of network troubleshooting activity, you can retrieve MIB information for the device associated with a specified event in the **Event Viewer**.

View the structure of the network device related to an event
As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Event Viewer**.

Investigating service-affected events

Service-Affected Events (SAEs) are events generated by Network Manager that indicate that a network service, such as an MPLS VPN, has been affected as a result of events from a device that supports the service.

Identifying service-affected events

Use the SAEs in the **Event Viewer** to quickly identify network service-affecting events.

About this task

Network Manager uses the discovered topology and event data to create SAEs. An SAE is generated on a service when a severity 5 (Critical) event occurs on a device or interface that is essential to that service. The SAEs themselves have a severity of 4 (Major) and are colored orange in the **Event Viewer**. The **Summary** field contains text indicating that the event is an SAE.

Procedure

1. Click on the color-coded severity indicator box corresponding to severity 5 (Major).

   The severity indicator boxes are located at the bottom of the **Event Viewer** and the corresponding color is orange.
2. Examine the **Summary** field of the Major severity events to determine whether any of the events is an SAE.

Example

Network Manager models MPLS Layer 3 VPNs and identifies the Provider-Edge to Customer-Edge facing interfaces for each discovered VPN. When an event is raised against one of these interfaces, Network Manager calculates that a specific VPN instance could be affected by the event. Network Manager raises an SAE on the VPN and does not delete the original event.

What to do next

You can perform any of the following actions on this event:

- Display network events that contributed to a service-affected event.
- Display related topology views
- Drill into the affected device to investigate the health of device components
- Browse the MIB associated with the affected device

Related tasks

Identifying contributing events

Identify which events contributed to a service-affected event (SAE) in order to perform further troubleshooting activities to resolve the SAE.

Identifying contributing events

Identify which events contributed to a service-affected event (SAE) in order to perform further troubleshooting activities to resolve the SAE.

Before you begin

Before identifying the contributing events, first identify the relevant SAE.

About this task

To identify contributing events:

Procedure

1. From an **Event Viewer** window, right-click an SAE and click **Show SAE Related Events**.

   An **Event Viewer** opens in a separate browser window containing the events that contributed to the SAE.
2. Use the features in the **Event Viewer** to further investigate these events.
3. To identify contributing services, click **Show SAE Related Services**.

What to do next

You can perform any of the following actions on these events:

- Display related topology views
- Drill into the affected device to investigate the health of device components
- Browse the MIB associated with the affected device

Related tasks

Displaying related topology views
Topology views show the network devices affected by an event. You can display two types of topology view: network views and the **Network Hop View**.

Retrieving related MIB information
As part of network troubleshooting activity, you can retrieve MIB information for the device associated with a specified event in the **Event Viewer**.

View the structure of the network device related to an event
As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Event Viewer**.

Retrieving related MIB information

As part of network troubleshooting activity, you can retrieve MIB information for the device associated with a specified event in the **Event Viewer**.

About this task

To retrieve MIB information related to an event:

Procedure

1. Select an event in the **Event Viewer**.
2. From an **Event Viewer** window, right-click the selected event and click **Show SNMP MIB Browser**.

   The **SNMP MIB Browser** appears in a separate browser window with the **Host** field populated with the IP address or device name of the affected device.

3. Use the features in the **SNMP MIB Browser** to further investigate this event.

Related tasks

Issuing an SNMP MIB query
Issue a MIB query to retrieve MIB variables from network devices and subsequently diagnose problems on those devices.

View the structure of the network device related to an event

As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Event Viewer**.

Before you begin

Before you issue the command to drill into the affected device, ensure that the event to investigate is selected in the Active Event List.

Procedure

1. Select an event in the **Event Viewer**.
2. From an **Event Viewer** window, right-click an event and click **Show Device Structure**.

   The **Structure Browser** opens in a separate browser window in tree mode populated with component details for the affected device. The table mode of the **Structure Browser** is not available from the right-click menu.
3. Use the features in the **Structure Browser** tree to explore the device structure and investigate the health of device components.

Related tasks

Identifying faulty components from the Structure Browser tree
Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Investigating network connections

Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

Showing device connectivity

Run this command on a device in the network map to see the interfaces on that device and associated connections for each interface. The command retrieves connections that are on the same layer as the view from which the command was launched.

Procedure

1. From the **Network Hop View** GUI or the **Network Views** GUI select a device in the network map.

   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and click **Show Connectivity Information**.

   A new browser window is displayed for each of the selected devices. The window contains a table with the following connectivity information. Each row in the table represents a device connection.

   Local node
   Specifies connectivity information for the selected device.

   Entity name
   Specifies the IP address or hostname of the selected device.

   Interface description
   Specifies descriptive information for a connected interface on the selected device.

Interface type
Specifies the interface type for the connected interface.

Neighbor node
Specifies connectivity information for devices connected to the selected device.

Entity name
Specifies the IP address or hostname of a device connected to the selected device. Click this hyperlink to open a separate browser window showing connectivity information for this device.

Interface description
Specifies descriptive information for an interface connected to the selected device.

Interface type
Specifies the interface type for an interface connected to the selected device.

Tracing the route to devices

Trace the route to devices in the network in order to troubleshoot connectivity. You can trace the route from your local client machine, from the Network Manager server, or perform a remote traceroute from any Cisco or Juniper network

About this task

The following topics describe how to trace the route to devices.

Tracing the route from the server

Trace the route to devices from the Network Manager Server in order to check network paths.

About this task

The following topics describe how to trace the route to devices from the Network Manager Server.

Tracing the route to devices

Trace the route to devices in the network map from the Network Manager to check network paths.

Before you begin

To perform this procedure, you must be in the **Network Views** or in the **Network Hop View**.

Procedure

1. From the **Network Hop View** GUI or **Network Views** GUI, select the device to which to trace the route.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Advanced Traceroute**.
   The results of the traceroute operation appear in one or more separate browser windows.

What to do next

It is also possible to perform a custom traceroute by customizing the traceroute settings.

Related tasks

Performing a custom traceroute

Trace the route to one or more devices in the network map from the Network Manager to check the path to that device.

Performing a custom traceroute

Trace the route to one or more devices in the network map from the Network Manager to check the path to that device.

About this task

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to ping.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Launch WebTools GUI...**.
3. From the **WebTools Menu** click **traceroute**.
4. In the **Advanced Traceroute Tool** window, complete the relevant fields.

   Target
   Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses or hostnames to traceroute. The tool will attempt to ping each address or hostname specified.

   Send
   Specify the number of packets at each hop. The default value is 3.

   Packet Size
   Specify the size in bytes of each packet to send to the specified targets. The default value is 40.

   Minimum TTL
   Specify the minimum time to live (TTL) in hops for the packets used for this traceroute operation. The default value is 1.

   Maximum TTL
   Specify the maximum TTL in hops for the packets used for this traceroute operation. The default value is 64.

   Show: ASN at each hop
   Specify whether the Autonomous System Number (ASN) should be resolved at each hop. This option is selected by default.

   Show: Do not resolve IP addresses
   Specify whether IP addresses must be resolved by the domain name system (DNS). This option is not selected by default.

   Show: DNS SOA
   Specify whether to include DNS Start of Authority (SOA) record. The SOA record includes information about the name of the server that supplied the data for the zone and the administrator of the zone. This option is selected by default.

   Show: Delay statistics at each hop
   Specify whether to calculate and display statistics for minimum, average and maximum delay for each hop. This option is not selected by default.

   Show: Microsecond timestamps
   Specify whether to use microsecond timestamps. This option is not selected by default.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

   Use: Next hop on Any Success
   Specify whether the tool should go to the next hop on any success. This option is not selected by default.

   Use: Parallel Probing
   Specify whether or tool should use parallel probing to increase the speed of the traceroute. This option is selected by default.

   Use: Abort after 10 hops without Response
   Specify whether the tool should abort the traceroute after ten consecutive hops without answer. This option is selected by default.

Use: RFC1191 Path MTU Discovery
Specify whether the tool should determine the Maximum Transmission Unit (MTU) of the path on which the traceroute operation is being performed. This option is not selected by default.

5. Click **Start** to launch the tool with the parameters specified.

   The results of the operation appear in one or more separate browser windows.

Performing remote traceroute operations

Perform remote traceroute operations from Cisco and Juniper devices to troubleshoot device availability and latency issues.

About this task

The following topics describe how to perform remote traceroute operations.

Related tasks

Setting up login credentials

Configure login credentials in order to log into Cisco and Juniper devices, and various network troubleshooting activities from these devices; for example, remote ping and remote traceroute.

Performing a remote traceroute from Cisco or Juniper devices

Perform a remote traceroute from one or more Cisco or Juniper devices to a target device in order to troubleshoot device availability and latency issues.

Before you begin

If you want to automatically login into Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the Cisco or Juniper device from which to perform the remote traceroute.

   To select multiple devices, press Ctrl.

   When selecting multiple devices, ensure that they are all Cisco or all Juniper devices.

2. Right-click one of the selected devices and select one of the following menu options.

Type of device	Menu option
Cisco	Select **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **Traceroute from this device...**
Juniper	Select **WebTools** > **Juniper Tools...** > **Diagnostic Tools...** > **Traceroute from this device...**

3. From the Cisco or Juniper Traceroute Tool window, complete the relevant fields.

   Note: This operation does not support IPv6 addresses.

   From
   Cisco or Juniper device or devices from which to traceroute. Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses or hostnames.

   To
   Target device for the traceroute. Specify a single IP address or hostname.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Performing a remote traceroute to a device within an LSP

Perform a remote traceroute to a device within a Multiprotocol Label Switching (MPLS) label-switched path (LSP) from a specified Cisco provider-edge (PE) router in order to troubleshoot the MPLS core network.

Before you begin

In order to perform this procedure, first ensure the following:

- You are in an MPLS VPN network view.
- If you want to automatically log into the Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. In the network map, select the Cisco PE router from which you wish perform the LSP traceroute.

   To select multiple devices, press Ctrl.
2. Right-click on one of the selected devices and choose the menu option **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **LSP Traceroute from this device...**.
3. Complete the fields in the **Cisco LSP Traceroute Tool** window.

   From
   Specify the Cisco device or devices to LSP traceroute from. This field accepts a comma-separated list of IP addresses or hostnames.

   Target FEC and Mask
   Specify the forward-equivalency class (FEC) and netmask. The FEC is a classification of a group of packets. All packets assigned to an FEC receive the same routing treatment. This tool accepts FECs based on IP address. Therefore, this field accepts a single IP address and a netmask.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Performing a remote traceroute to a device within a VPN

Perform a remote traceroute to a device within a virtual private network (VPN) from a specified Cisco provider-edge (PE) router in order to troubleshoot VPN connectivity.

Before you begin

In order to perform this procedure, first ensure the following:

- You are in an MPLS VPN network view.
- If you want to automatically log into the Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. In the network map, select the Cisco PE router from which you wish perform the VPN traceroute.

   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **VRF Traceroute from this device...**.
3. Complete the fields in the **Cisco VRF Traceroute Tool** window.

   From
   Specify the Cisco device or devices from which to perform a VRF traceroute. This field accepts a comma-separated list of IP addresses or hostnames.

   To
   Specify a target device for the traceroute. This field accepts a single IP address or hostname.

   VRF
   Specify the Virtual Routing and Forwarding table (VRF) that contains the device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.
   The results of the ping operation appear in one or more separate browser windows.

Visualizing a network path

A network path view displays every device and link encountered between the start and end devices. Issues affecting devices and links on that path are displayed graphically. You can edit the path view manually by excluding devices from the view. You can retrace a path, or edit it before retracing it. You can also copy a path view to another view container, or delete it.

Before you begin

Before you can work with network paths, the administrator must have successfully completed the first network discovery, and network views must be configured for your user ID.

About this task

You can only edit or retrace IP paths. MPLS TE paths are populated during discovery and cannot be edited or retraced.

Note: MPLS TE paths are displayed by default under the itnmadmin views. This can be altered by editing the `$NMGUI_HOME/profile/etc/tnm/topoviz.properties` file and changing the values for the following view attributes:

- topoviz.pathview.accesslevel
- topoviz.pathview.accessid

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Path Views**.
   The **Path Views** window opens. Any network paths that have been created are shown.
2. To interact with network paths, use the following buttons:

   Views drop-down
   Use to find and display a specific path view. Path views are arranged in a tree structure based on path view container types, for example, 'AUTO', 'IP Paths', 'itnmadmin', or 'Client Views'.

   Each path view displays the view name, the number of hops in the path, and the highest severity alert (if any) associated with that path view.

   Note: You can click the severity icon to launch the Active Event List with that event selected. You can also select a device, and then click **Find In Network View** or **Find In Hop View** from the context menu.

New path 

Opens the **Trace Network Path** window, where you can create a new path view.

Note: IP path views only.

Note: You can only trace a path across a single domain. All devices specified in the **Trace Network Path** window must be in the same domain.

Depending on the user roles set by your administrator for your user ID, you may be able to save the new path to your list of path views.

Edit path 

Click here to edit a path view that is currently being displayed. The **Trace Network Path** window opens populated with the details for the path, any of which can be changed. You trace and display the edited path by clicking **Save and Trace**.

Note: IP path views only.

Note: You can only trace a path across a single domain. All devices specified in the **Trace Network Path** window must be in the same domain.

Retrace path 

Click here to retrace the path between the devices in the currently selected path view. Paths between devices in a network are dynamic, and therefore trace results may be different each time a path is retraced.

Note: IP path views only.

Copy or move path 

Opens the **Copy or Move Path** dialog. Use to copy or move a selected path to a different view container.

Delete path 

Click here to delete the path view that is currently being displayed. If the path view is the last view in a container, the container will be deleted as well.

Note: The path stored in the NCIM database is not deleted. If any user recreates the deleted path with the same settings, a new trace occurs and the existing path in the NCIM database is updated with the new trace results.

Toggle search 

Displays a search box below the toolbar from which you can search for a view.

Save 

Saves the view or view container. This button appears only when a view is displayed.

Save as Image 

Saves the view or views as an image.

Print 

Prints the view or view container.

Find in Map 

Searches for a device in the topology map.

Select 

Changes the cursor to select mode. When the cursor is in select mode, if you click a device in the topology display panel that device is selected.

Pan 
Changes the cursor to pan mode. When the cursor is in pan mode, the cursor changes to the following icon:  . Click and hold the left mouse button to grab the topology; you can then use the mouse to move the topology.

Select Zoom 
Changes the cursor to select-zoom mode. When the cursor is in select-zoom mode, you can use the mouse to draw a rectangle over a particular area of the topology. When you release the mouse button, the screen zooms in to the rectangle you have drawn.

Interactive Zoom 
Changes the cursor to interactive-zoom mode. When the cursor is in interactive zoom mode, hold down the mouse button and move the cursor up to zoom out, and while hold down the mouse button and move the cursor down to zoom in.

Toggle Overview 
Displays a thumbnail of the whole view in the bottom right corner, with a box around the region that is currently visible.

Zoom In 
Zooms in to the view.

Zoom Out 
Zooms out of the view.

Fit in Window 
Fits the current view to the size of the **Topology Display** window.

Hierarchical Layout 
Changes the format of the view to a hierarchical layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Symmetric Layout 
Changes the format of the view to a symmetric layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Orthogonal Layout 
Changes the format of the view to an orthogonal layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

Circular Layout 
Changes the format of the view to a circular layout. This option is not available for views that cannot contain connectivity information, such as Unassigned network views.

If you chose to create a new path or retrace an existing path, then **Path View** window displays the devices resulting from your search.

What to do next

If the path was not successfully traced, then you get a path trace error, indicating the reason that the path could not be traced. To see more detailed path trace output, click the error at the top of the **Trace Network Path** window. Detailed path trace output opens in a second window. To troubleshoot the path trace, refer to the related information on troubleshooting path views.

Pinging devices and subnets

Ping devices in the network in order to check connectivity. You can ping from your local client machine, from the Network Manager server, or remote ping from any Cisco or Juniper network device.

About this task

The following topics describe how to ping devices and subnets.

Pinging from the local client

Ping one or more devices in the network map from your client machine to check connectivity to that device.

Procedure

1. From the **Network Hop View** or **Network Views** network map select the device to ping.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **Ping from this host**.
   This launches the generic ping tool on the local machine and pings the selected device or devices.

Pinging from the server

Ping devices and subnets, from the Network Manager Server in order to check connectivity.

About this task

The following topics describe how to ping devices and subnets from the Network Manager server. The ping from the server uses TCP echo and not ICMP.

Pinging devices

Ping one or more devices in the network map from the Network Manager server to check connectivity to that device.

Procedure

1. From the **Network Hop View** or **Network Views** network map select the device to ping.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Advanced Ping**
   The results of the ping operation appear in one or more separate browser windows.

What to do next

It is also possible to perform a custom ping by customizing the ping settings.

Related tasks

Performing a custom device ping

Ping one or more devices in the network map from the Network Manager server using custom settings to check connectivity to that device.

Performing a custom device ping

Ping one or more devices in the network map from the Network Manager server using custom settings to check connectivity to that device.

About this task

Procedure

1. From the **Network Hop View** or **Network Views** network map select the device to ping.

To select multiple devices, press Ctrl.

2. Right-click one of the selected devices and choose **WebTools** > **Launch WebTools GUI...**.
3. In the **WebTools Menu** click **ping**.
4. In the **Advanced Ping Tool** window complete the relevant fields.

   Target
   Specify the IP addresses or hostnames of the devices that you wish to ping. Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses or hostnames. The tool will attempt to ping each address or hostname specified.

   Send
   Specify the number of ping packets to send to each of the specified devices. The default value is 1.

   Packet Size
   Specify the size in bytes of each packet to send to the specified targets. The default value is 56.

   No. Retries
   Specify the number of retries to make for each target specified. The default value is 3.

   Show: DNS Resolved IP Addresses
   Specify whether or not IP addresses must be resolved by the domain name system (DNS). This option is selected by default.

   Show: Elapsed Time on Return Packets
   Specify whether or not elapsed times to complete the ping operation should be displayed. This option is not selected by default.

   Show: Final Summary
   Specify whether or not to include a final summary. This option is selected by default.

   Send: E-Mail To...
   Specify whether or not the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.
5. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Pinging subnets (UNIX only)

Ping one or more subnets in the network map from the Network Manager server to check connectivity to that subnet.

About this task

Restriction: This task is only available if your Network Manager server is running on UNIX.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select any device.
2. Right-click the selected device and choose **WebTools** > **Launch WebTools GUI...**.

   The **WebTools Menu** appears
3. From the **WebTools Menu** click **subnet ping**.
4. In the **Advanced Subnet Ping Tool** window, complete the relevant fields.

   CIDR Subnet
   Subnets to ping. Specify a single subnet in Classless Inter-Domain Routing (CIDR) notation; for example,10.1.1.0/24. The tool will attempt to ping each IP address within the specified subnet.

   Send
   Specify the number of ping packets to send to each of the specified devices. The default value is 1.

Packet Size
Specify the size in bytes of each packet to send to the specified targets. The default value is 56.

No. Retries
Specify the number of retries to make for each target specified. The default value is 3.

Show: DNS Resolved IP Addresses
Specify whether IP addresses must be resolved by the domain name system (DNS). This option is selected by default.

Show: Elapsed Time on Return Packets
Specify whether elapsed times to complete the ping operation should be displayed. This option is not selected by default.

Show: Final Summary
Specify whether to include a final summary. This option is selected by default.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

5. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Performing remote ping operations

Perform remote ping operations from Cisco and Juniper devices to troubleshoot device availability and latency issues.

About this task

The following topics describe how to perform remote ping operations.

Related tasks

Setting up login credentials

Configure login credentials in order to log into Cisco and Juniper devices, and various network troubleshooting activities from these devices; for example, remote ping and remote traceroute.

Performing a remote ping from Cisco or Juniper devices

Perform a remote ping from one or more Cisco or Juniper devices to a target device to troubleshoot device availability and latency issues.

Before you begin

If you want to automatically login into Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the Cisco or Juniper device from which you wish perform the remote ping.

   To select multiple devices, press Ctrl.

   When selecting multiple devices, ensure that they are all Cisco or all Juniper devices.

2. Right-click one of the selected devices and select one of the following menu options.

Type of device	Menu option
Cisco	Select **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **Ping from this device...**.
Juniper	Select **WebTools** > **Juniper Tools...** > **Diagnostic Tools...** > **Ping from this device...**

3. In the Cisco or Juniper Ping Tool window complete the relevant fields.

Note: This operation does not support IPv6 addresses.

From
Cisco or Juniper device or devices to ping from. Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses or hostnames.

To
Target device for the ping. Specify a single IP address or hostname.

Automatic Login
Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

Username
Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.
   The results of the ping operation appear in one or more separate browser windows.

Remote pinging a device within an LSP

Ping a device within a Multiprotocol Label Switching (MPLS) label-switched path (LSP) from a specified Cisco provider-edge (PE) router in order to troubleshoot the MPLS core network.

Before you begin

In order to perform this procedure, first ensure the following:

- You are in an MPLS VPN network view.
- If you want to automatically log into the Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. In the network map, select the Cisco PE router from which you wish perform the LSP ping.
   To select multiple devices, press Ctrl.
2. Using the right mouse button, click on one of the selected devices and choose the menu option **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **LSP Ping from this device...**
3. Complete the fields in the **Cisco LSP Ping Tool** window.

From
Specify a Cisco device or devices to LSP ping from. This field accepts a comma-separated list of IP addresses or hostnames.

Target FEC and Mask
Specify the IPv4 forward-equivalency class (FEC) and netmask. The FEC is a classification of a group of packets. All packets assigned to an FEC are routed in the same way. This tool accepts FECs based on IP address. Therefore, this field accepts a single IP address and a netmask.

Automatic Login
Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

Username
Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Remote pinging a device within a VPN

Ping a device within a virtual private network (VPN) from a specified Cisco provider-edge (PE) router in order to troubleshoot VPN connectivity.

Before you begin

In order to perform this procedure, first ensure the following:

- You are in an MPLS VPN network view.
- If you want to automatically log into the Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. In the network map, select the Cisco PE router from which you wish perform the VPN ping.

   To select multiple devices, press Ctrl.
2. Right-click on one of the selected devices and choose **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **VRF Ping from this device...**.
3. Complete the fields in the **Cisco VRF Ping Tool** window.

From
Specify the Cisco device or devices to VRF ping from. This field accepts a comma-separated list of IP addresses or hostnames.

To
Specify the target device for the ping. This field accepts a single IP address or hostname.

VRF
Specify the Virtual Routing and Forwarding table (VRF) that contains the device of interest.

Automatic Login
Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

Username
Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Retrieving Cisco and Juniper route information

Retrieve routing information from Cisco and Juniper devices to troubleshoot routing issues.

About this task

The following topics describe how to retrieve routing information from Cisco and Juniper devices.

Related tasks

Setting up login credentials

Configure login credentials in order to log into Cisco and Juniper devices, and various network troubleshooting activities from these devices; for example, remote ping and remote traceroute.

Retrieving Cisco route information

Retrieve route information from a selected Cisco device to a specific target (device or subnet) in order to troubleshoot device availability and latency issues.

Before you begin

If you want to automatically log into Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the Cisco device at the beginning of the route.

   To select multiple devices, press Ctrl.

   When selecting multiple devices, ensure that they are all Cisco devices.
2. Right-click one of the selected devices and choose **WebTools** > **Cisco Tools...** > **Diagnostic Tools...** > **View a route...**.
3. In Cisco Route Information Tool window complete the required fields.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses, hostnames, or subnets.

   Note: If you are retrieving route information for a device within a virtual private network (VPN), then the content of this field must be the IP address or hostname of a single provider-edge (PE) router adjacent to the relevant VPN. The option to retrieve route information for a device within a VPN only applies to Cisco devices.

   Route
   Specify IP address or hostname of a target device. The tool provides route information from the device or devices specified in the **Query** field, to this target device.

   Show VRF Route
   Specify that you wish to retrieve route information for a device within a specified virtual routing and forwarding table (VRF). Selecting this option toggles the **VRF** field, where you can specify the relevant VRF.

   Note: This option is only available for Cisco devices.

   VRF
   Specifies a VRF related to the VPN containing the device for which to obtain routing information.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Password
   Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Passcode
   Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

   Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the operation appear in one or more separate browser windows.

Retrieving Juniper route information

Retrieve route information from a selected Juniper device to a specific target (device or subnet) to troubleshoot device availability and latency issues.

Before you begin

If you want to automatically login into Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the Juniper device at the beginning of the route.

   To select multiple devices, press Ctrl.

   When selecting multiple devices, ensure that they are all Juniper devices.
2. Right-click one of the selected devices and choose **WebTools** > **Juniper Tools...** > **Diagnostic Tools...** > **View a route...**.
3. In the Juniper Route Information Tool window complete the required fields.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses, hostnames, or subnets.

   Route
   Specify IP address or hostname of a target device. The tool provides route information from the device or devices specified in the **Query** field, to this target device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Password
   Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Passcode
   Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

   Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.
4. Click **Start** to launch the tool with the parameters specified.

   The results of the operation appear in one or more separate browser windows.

Retrieving VRF route information

Retrieve information on a specific VRF instance to troubleshoot routes from the PE router.

Before you begin

In order to perform this procedure, first ensure the following.

- You are in an MPLS VPN network view.
- If you want to automatically log into the Cisco or Juniper devices, you must first configure login credentials.

Procedure

1. In the network map, select the Cisco PE router from which you wish retrieve VRF route information.

   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Cisco Tools...** > **Information Tool...** > **View VRF Information...**.
3. Complete the fields in the **Cisco VRF Information Tool** window.

   Query
   Specify the IP address or hostname or a Cisco PE router containing the VRF of interest.

   VRF
   Specify the VRF for which you wish to retrieve information.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Password
   Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Passcode
   Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

   Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.
4. Click **Start** to launch the tool with the parameters specified.

   The results of the ping operation appear in one or more separate browser windows.

Setting up login credentials

Configure login credentials in order to log into Cisco and Juniper devices, and various network troubleshooting activities from these devices; for example, remote ping and remote traceroute.

About this task

You can configure Telnet login details (username and password) using the XML configuration file provided for each WebTool. One set of login details can be configured for each WebTool. Passwords specified in the WebTools configuration files are plain-text . If you configure Telnet login details within these files, then it is recommended that you apply appropriate security measures to the WebTools directory, `NCHOME/precision/scripts/webtools/etc`.

You can configure multiple usernames and passwords in the XML configuration file. To configure login details:

Procedure

1. Open the XML configuration file for the web tool you want to configure.

   These configuration files are held at the following location: `NCHOME/precision/scripts/webtools/etc`.
2. Within the XML code, locate the login section.
3. Specify login details as follows:
   a) Username: within the username section, specify one or more usernames.
   b) Password: within the password section, specify one or more passwords.

      If you configure a single username and password for a WebTool then the tool uses these same login details when performing a Telnet login into all the devices specified.

      Note: If the login details vary across the devices you wish to log into and you wish to run the same web tool on multiple devices simultaneously, then you must configure multiple usernames and passwords. In this case, the web tool attempts to log into each device using each combination of username and password until it finds a successful combination. This can have an impact on the time taken for the web tool to log into all devices.
4. Save the XML configuration file.

What to do next

Now that you have configured login details for a specific WebTool then you can automatically access these details by clicking the **Automatic** checkbox in the tool window.

Related tasks

Performing remote ping operations
Perform remote ping operations from Cisco and Juniper devices to troubleshoot device availability and latency issues.

Performing remote traceroute operations
Perform remote traceroute operations from Cisco and Juniper devices to troubleshoot device availability and latency issues.

Retrieving Cisco and Juniper route information

Retrieve routing information from Cisco and Juniper devices to troubleshoot routing issues.

Retrieving device information

Retrieving device information provides important information on the devices in your network to support troubleshooting. Device information includes device configuration information, domain information, and detailed interface, protocol, and routing information.

About this task

The following topics describe how to retrieve device information.

Querying domain registration information

Query domain registration information in order to determine the organization or individual responsible for a specified IP address or IP address range or to resolve IP addresses or hostnames.

About this task

The following topics describe how to query domain registration information.

Querying Internet registry databases

Query Internet registry databases in order to determine the organization or individual responsible for a specified IP address or IP address range. You can also retrieve other information, including contact details, and server and IP addressing information.

About this task

The following topics describe how to query Internet registry databases.

Issuing a standard Internet registry database query

Query an Internet registry database in order to determine the organization or individual responsible for a specified IP address or IP address range.

About this task

By default, this operation queries the RIPE database. This is the Réseaux IP Européens, which is the regional Internet registry for Europe, the Middle East and parts of Central Asia,

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Whois Lookup**.
   The results of the lookup operation appear in one or more separate browser windows.

What to do next

You can also query Internet registries for other geographies, by issuing a custom Internet registry database query.

Related tasks

Issuing a custom Internet registry database query

Query an Internet registry database in order to determine the organization or individual responsible for a specified IP address or IP address range. Using custom queries, you can retrieve information from Internet registries for geographies other than the default Réseaux IP Européens (RIPE) registry, which is the regional Internet registry for Europe, the Middle East and parts of Central Asia.

Issuing a custom Internet registry database query

Query an Internet registry database in order to determine the organization or individual responsible for a specified IP address or IP address range. Using custom queries, you can retrieve information from Internet registries for geographies other than the default Réseaux IP Européens (RIPE) registry, which is the regional Internet registry for Europe, the Middle East and parts of Central Asia.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **WebTools** > **Launch WebTools GUI...**.
3. From the **WebTools Menu** click **Whois lookup**.
4. In the **Whois Lookup Tool** window complete the relevant fields.

   Query for
   Specify the IP addresses or hostnames of the devices to query. Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses or hostnames. This field also accepts a search string.

   Database
   Specify the Internet registry database to query. The following databases may be queried:

   - AFRINIC: Africa Network Information Center, the regional Internet registry for Africa.
   - ARIN: American Registry for Internet Numbers, the regional Internet registry for Canada, many islands in the Caribbean and North Atlantic ocean, and the United States
   - APNIC: Asia Pacific Network Information Centre, the regional Internet registry for the Asia-Pacific region.
   - JPIRR: Japan Network Information Center, the regional Internet registry for Japan.
   - LACNIC: Latin American and Caribbean Internet Addresses Registry, the regional Internet registry for Latin America and the Caribbean.
   - RADB: Routing Assets Database is a public registry of routing information for networks in the Internet.
   - RIPE: Réseaux IP Européens, the regional Internet registry for Europe, the Middle East and parts of Central Asia
   - VERIO: Verio is a global IP service provider.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.
5. Click **Start** to launch the tool with the parameters specified.
   The results of the operation appear in one or more separate browser windows.

Performing DNS lookups

Perform DNS lookups in order to resolve IP addresses or hostnames.

About this task

The following topics describe how to perform DNS lookups.

Issuing a standard DNS lookup

Issue a Domain Name System (DNS) lookup in order to resolve IP addresses or hostnames.

About this task

By default, this operation retrieves DNS address (A) records only.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose the menu option **WebTools** > **DNS Lookup**.
   The results of the lookup operation appear in one or more separate browser windows.

What to do next

You can also retrieve other record types, such as mail exchange (MX) records by issuing a custom DNS lookup.

Related tasks

Issuing a custom DNS lookup

Issue a Domain Name System (DNS) lookup in order to resolve IP addresses or hostnames. Using custom DNS lookups, you can retrieve non-standard DNS record types, such as mail exchange (MX) records.

Issuing a custom DNS lookup

Issue a Domain Name System (DNS) lookup in order to resolve IP addresses or hostnames. Using custom DNS lookups, you can retrieve non-standard DNS record types, such as mail exchange (MX) records.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.
   To select multiple devices, press Ctrl.
2. Right-click on one of the selected devices and choose **WebTools** > **Launch WebTools GUI...**.
3. From the **WebTools Menu** click **DNS lookup**.
4. In the **DNS Lookup Tool** window complete the relevant fields.

   Query for
   Specify the IP addresses or hostnames of the devices to query. Specify a single IP address, hostname, or subnet, or a comma-separated list of IP addresses and/or hostnames. This field also accepts a search string.

   Type
   Specify the type of record to query in DNS. You can query any of the following types:

   - ANY: any record
   - A: address records
   - CNAME: canonical name records
   - HINFO: host information records
   - MINFO: mailbox information records
   - MX: mail exchange records
   - NS: name server records
   - PTR: pointer records
   - SOA: start of authority records
   - TXT: text records

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

5. Click **Start** to launch the tool with the parameters specified.

   The results of the operation appear in one or more separate browser windows.

Retrieving protocol information from Cisco and Juniper devices

Retrieve detailed interface, protocol, and routing information from Cisco and Juniper devices in order to support troubleshooting activities.

About this task

The following topics describe how to retrieve detailed interface, protocol, and routing information from Cisco and Juniper devices.

Retrieving interface administrative and operational status

Retrieve interface information in order to determine the operational and administrative status of interfaces on selected devices.

About this task

You can only launch this command on Cisco and Juniper devices.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.

   To select multiple devices, press Ctrl.

2. Right-click one of the selected devices and select one of the following menu options.

Type of device	Menu option
Cisco	Select **WebTools** > **Cisco Tools...** > **Information Tools...** > **View BGP Information...**
Juniper	Select **WebTools** > **Juniper Tools...** > **Information Tools...** > **View BGP Information...**

3. In the Cisco or Juniper Information Tool window complete the relevant fields.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or a comma-separated list of IP addresses or hostnames. IP addresses for selected devices automatically appear in this field.

   View
   Specify the type of information to retrieve from the device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the operation appear in one or more separate browser windows.

Retrieving BGP information

Retrieve Border Gateway Protocol (BGP) information from devices in order troubleshoot BGP-related network issues.

About this task

You can only launch this command on Cisco and Juniper devices.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.

   To select multiple devices, press Ctrl.

2. Using the right mouse button, click on one of the selected devices and select one of the following menu options.

Type of device	Menu option
Cisco	Select **WebTools** > **Cisco Tools...** > **Information Tools...** > **View BGP Information...**
Juniper	Select **WebTools** > **Juniper Tools...** > **Information Tools...** > **View BGP Information...**

3. In the Cisco or Juniper Information Tool window complete the relevant fields.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or a comma-separated list of IP addresses or hostnames. IP addresses for selected devices automatically appear in this field.

   View
   Specify the type of information to retrieve from the device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

Username
Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.
   The results of the operation appear in one or more separate browser windows.

Retrieving ISIS information

Retrieve ISIS information from devices in order to troubleshoot ISIS-related issues.

About this task

You can only launch this command on Cisco and Juniper devices.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and select one of the following menu options.

Type of device	Menu option
Cisco	Select **WebTools** > **Cisco Tools...** > **Information Tools...** > **View BGP Information...**
Juniper	Select **WebTools** > **Juniper Tools...** > **Information Tools...** > **View BGP Information...**

3. In the Cisco or Juniper Information Tool window complete the relevant fields.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or a comma-separated list of IP addresses or hostnames. IP addresses for selected devices automatically appear in this field.

   View
   Specify the type of information to retrieve from the device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

Username
Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   The results of the operation appear in one or more separate browser windows.

Retrieving MBGP information

Retrieve MBGP information from devices in order to troubleshoot MBGP-related issues.

Before you begin

To perform this procedure, you must be in the **Network Views** or in the **Network Hop View**.

About this task

You can only launch this command on Cisco devices.

Procedure

1. In the network map select the device to query.

   To select multiple devices, press Ctrl.
2. Using the right mouse button, click on one of the selected devices and select the appropriate menu option:

Type of device	Menu option
Cisco	Choose the menu option **WebTools > Cisco Tools...> Information Tools...> View MBGP Information...**
Juniper	Choose the menu option **WebTools > Juniper Tools...> Information Tools...> View MBGP Information...**

   The Cisco or Juniper Information Tool window appears.
3. Complete the fields in the window.

   Note: This operation does not support IPv6 addresses.

Query
Specify a single IP address, hostname, or a comma-separated list of IP addresses or hostnames. IP addresses for selected devices automatically appear in this field.

View
Specify the type of information to retrieve from the device.

Automatic Login
Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

Username
Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Password
Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

Passcode
Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

Send: E-Mail To...
Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

Recipients
Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.
   After a few moments the results of the operation appear in one or more separate browser windows.

Retrieving MPLS information

Retrieve MPLS information from devices in order to troubleshoot MPLS-related issues.

Before you begin

To perform this procedure, you must be in the **Network Views** or in the **Network Hop View**.

About this task

You can only launch this command on Cisco and Juniper devices.

Procedure

1. In the network map select the device to query.
   To select multiple devices, press Ctrl.
2. Using the right mouse button, click on one of the selected devices and select the appropriate menu option:

Type of device	Menu option
Cisco	Choose the menu option **WebTools > Cisco Tools...> Information Tools...> View MPLS Information...**

Type of device	Menu option
Juniper	Choose the menu option **WebTools > Juniper Tools...> Information Tools...> View MPLS Information...**

The Cisco or Juniper Information Tool window appears.

3. Complete the fields in the window.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or a comma-separated list of IP addresses or hostnames. IP addresses for selected devices automatically appear in this field.

   View
   Specify the type of information to retrieve from the device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Password
   Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Passcode
   Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

   Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.

   After a few moments the results of the operation appear in one or more separate browser windows.

Retrieving OSPF information

Retrieve Open Shortest Path First protocol (OSPF) information from devices in order to troubleshoot OSPF-related issues.

About this task

You can only launch this command on Cisco and Juniper devices.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.

   To select multiple devices, press Ctrl.

2. Right-click one of the selected devices and select one of the following menu options.

Type of device	Menu option
Cisco	Select **WebTools** > **Cisco Tools...** > **Information Tools...** > **View OSPF Information...**
Juniper	Select **WebTools** > **Juniper Tools...** > **Information Tools...** > **View OSPF Information...**

3. In the Cisco or Juniper Information Tool window complete the required fields.

   Note: This operation does not support IPv6 addresses.

   Query
   Specify a single IP address, hostname, or a comma-separated list of IP addresses or hostnames. IP addresses for selected devices automatically appear in this field.

   View
   Specify the type of information to retrieve from the device.

   Automatic Login
   Specify that you have already specified Telnet login credentials to use when running this tool. This is not selected by default.

   Username
   Specify a username to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Password
   Specify a password to use for Telnet access to the devices specified in the Query field. If you have specified multiple devices, then the login credentials that you specify must be valid for all of these devices.

   Passcode
   Specify an optional security authentication measure. Complete this field only if your network administrator has applied RSA SecurID two-factor user authentication to the devices you wish to log into. Type the passcode from your RSA SecurID token.

   Note: Your passcode changes at regular 30 second intervals. Ensure that you launch the tool immediately after supplying the passcode.

   Send: E-Mail To...
   Specify whether the results should be emailed to one or more listed recipients. This option is not selected by default.

   Recipients
   Specify a comma-separated list of recipients to which the results of the tool should be sent. This field is only displayed if **Send: E-Mail To...** is selected.

4. Click **Start** to launch the tool with the parameters specified.
   The results of the operation appear in one or more separate browser windows.

Retrieving Virtual Private LAN Service (VPLS) information

Retrieve Virtual Private LAN Service (VPLS) information from devices in order to troubleshoot VPLS-related issues.

About this task

You can only launch this command on Cisco and Juniper devices.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device to query.
   To select multiple devices, press Ctrl.

2. Right-click one of the selected devices and select **Webtools** > **Launch Webtools GUI**.
3. Select one of the following menu options.

Type of device	Menu option
Cisco	Select **Cisco Tools...** > **Information Tools...** > **View VPLS Information...**
Juniper	Select **Juniper Tools...** > **Information Tools...** > **View VPLS Information...**

4. For Cisco devices, select one of the following menu options.

Option	Description
Show vfi	Displays VPLS information.
Show xconnect all	Displays information about cross connects configured on the device.
Show mpls l2transport vc	Displays information about all pseudowires configured on the device.

5. For Juniper devices, select one of the following menu options.

Option	Description
Show vpls connections	Displays VPLS-related pseudowires.
Show vpls mac-table	Displays MAC table entries associated with corresponding VFI and VPLS instances.
Show vpls statistics	Displays statistical information about all VPLS configured on the device.

Displaying poll data from a topology view by using the Top Performers widget

Users can display historical poll data from a topology view to diagnose network problems.

About this task

As well as using the reports function to display poll data, users can also display the poll data from within any of the following views for a device, multiple devices, a subview or a subnet.

Network Views
Network Hop View
Path Views

Procedure

1. Within either the **Network Views**, the **Network Hop View** or the **Path Views**, open a view. The topology map for your selected view displays in the main pane.
2. Within the topology map, right-click the devices or subnet you want to diagnose. A menu is displayed.
3. From the menu select **Show `polling data`**. Depending on your browser settings, either a tab or pop-out window **Top Performers** displays with the poll data for your selected devices or subnet.

   Note: If you would prefer to see a **Top Performers** pop-out window display instead of a **Top Performers** tab display, or visa versa, refer to your browser documentation to modify this preference.

What to do next

Select from the following controls to display chart, table, or trace data in the **Top Performers** widget.

Metric
Click this drop-down list to display a selected set of poll data metrics. The metrics that are displayed in the drop-down list depend on which poll policies are enabled for the selected network view. Select one of these metrics to display associated data in the main part of the window.

Order
Click this drop-down list to display what statistic to apply to the selected poll data metric.

- Statistics available for all metrics, except the `SnmpLinkStatus` metric.

  From Top: Displays a bar chart or table that shows the 10 highest values for the selected metric. The devices or interfaces with these maximum values are listed in the bar chart or table.

  From Bottom: Displays a bar chart or table that shows the 10 lowest values for the selected metric. The devices or interfaces with these minimum values are listed in the bar chart or table.

- Statistics available for the `SnmpLinkStatus` metric. In each case, a bar chart or table displays and shows devices for the selected statistic.

  Unavailable: This statistic displays by default. Devices with this statistic are problematic.

  Admin Down Devices with this statistic are not problematic as Administrators change devices to this state.

  Available Devices with this statistic are not problematic.

Note: The widget lists devices or interfaces depending on which metric was selected:

- If the metric selected applies to a device, such as memoryUtilization, then the top 10 list contains devices.
- If the metric selected applies to an interface, such as ifInDiscards, then the top 10 list contains interfaces.

 **Show Chart**
Displays a bar chart with the 10 highest or lowest values. Show Chart is the display option when you first open the widget.

 **Show Table**
Displays a table of data associated with the 10 highest or lowest values.

 **Define Filter**

This button only appears if you are in **Show Table**  mode. Click here to define a filter to apply to the Top Performers table data.

The main part of the window contains the data in one of the following formats:

Chart
Bar chart with the 10 highest or lowest values. Click any bar in the chart to show a time trace for the corresponding device or interface.

Table
Table of data associated with the 10 highest or lowest values. The table contains the following columns:

- **Entity Name**: Name of the device or interface.
- **Show Trace**: Click a link in one of the rows to show a time trace for the corresponding device or interface.
- **Last Poll Time**: Last time this entity was polled.
- **Value**: Value of the metric the last time this entity was polled.

Trace
Time trace of the data for a single device or interface. Navigate within this trace by performing the following operations:

- Zoom into the trace by moving your mouse wheel forward.
- Zoom out of the trace by moving your mouse wheel backward.
- Double click to restore the normal zoom level.

- Click within the trace area for a movable vertical line that displays the exact value at any point in time.

Click one of the following buttons to specify which current or historical poll data to display in the main part of the window. This button updates the data regardless of which mode is currently being presented: bar chart, table, or time trace.

Restriction: If your administrator has opted not to store poll data for any of the poll data metrics in the **Metric** drop-down list, then historical poll data will not be available when you click any of the following buttons:

- **Last Day**
- **Last Week**
- **Last Month**
- **Last Year**

Current
Click this button to display current raw poll data. When in time trace mode, depending on the frequency of polling of the associated poll policy, the time trace shows anything up to two hours of data.

Last Day
Click this button to show data based on a regularly calculated daily average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a daily exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 24 hours is shown, based on the average values.

In the **Last Day** section of the widget EWMA values are calculated by default every 15 minutes and are based on the previous 15 minutes of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every 15 minutes.

Last Week
Click this button to show data based on a regularly calculated weekly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a weekly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 7 days is shown, based on the average values.

In the **Last Week** section of the widget EWMA values are calculated by default every 30 minutes and are based on the previous 30 minutes of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every 30 minutes.

Last Month
Click this button to show data based on a regularly calculated monthly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a monthly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 30 days is shown, based on the average values.

In the **Last Month** section of the widget EWMA values are calculated by default every two hours and are based on the previous two hours of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every two hours.

Last Year
Click this button to show data based on a regularly calculated yearly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a yearly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 365 days is shown, based on the average values.

In the **Last Year** section of the widget EWMA values are calculated by default every day and are based on the previous 24 hours of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every day.

Select from the following controls to display chart, table, or trace data in the **Top Performers** widget.

Metric
Click this drop-down list to display a selected set of poll data metrics. The metrics that are displayed in the drop-down list depend on which poll policies are enabled for the selected network view. Select one of these metrics to display associated data in the main part of the window.

Order
Click this drop-down list to display what statistic to apply to the selected poll data metric.

- Statistics available for all metrics, except the `SnmpLinkStatus` metric.

  From Top: Displays a bar chart or table that shows the 10 highest values for the selected metric. The devices or interfaces with these maximum values are listed in the bar chart or table.

  From Bottom: Displays a bar chart or table that shows the 10 lowest values for the selected metric. The devices or interfaces with these minimum values are listed in the bar chart or table.

- Statistics available for the `SnmpLinkStatus` metric. In each case, a bar chart or table displays and shows devices for the selected statistic.

  Unavailable: This statistic displays by default. Devices with this statistic are problematic.

  Admin Down Devices with this statistic are not problematic as Administrators change devices to this state.

  Available Devices with this statistic are not problematic.

Note: The widget lists devices or interfaces depending on which metric was selected:

- If the metric selected applies to a device, such as memoryUtilization, then the top 10 list contains devices.
- If the metric selected applies to an interface, such as ifInDiscards, then the top 10 list contains interfaces.

 **Show Chart**
Displays a bar chart with the 10 highest or lowest values. Show Chart is the display option when you first open the widget.

 **Show Table**
Displays a table of data associated with the 10 highest or lowest values.

 **Define Filter**

This button only appears if you are in **Show Table**  mode. Click here to define a filter to apply to the Top Performers table data.

The main part of the window contains the data in one of the following formats:

Chart
Bar chart with the 10 highest or lowest values. Click any bar in the chart to show a time trace for the corresponding device or interface.

Table
Table of data associated with the 10 highest or lowest values. The table contains the following columns:

- **Entity Name**: Name of the device or interface.
- **Show Trace**: Click a link in one of the rows to show a time trace for the corresponding device or interface.
- **Last Poll Time**: Last time this entity was polled.
- **Value**: Value of the metric the last time this entity was polled.

Trace
Time trace of the data for a single device or interface. Navigate within this trace by performing the following operations:

- Zoom into the trace by moving your mouse wheel forward.
- Zoom out of the trace by moving your mouse wheel backward.
- Double click to restore the normal zoom level.
- Click within the trace area for a movable vertical line that displays the exact value at any point in time.

Click one of the following buttons to specify which current or historical poll data to display in the main part of the window. This button updates the data regardless of which mode is currently being presented: bar chart, table, or time trace.

Restriction: If your administrator has opted not to store poll data for any of the poll data metrics in the **Metric** drop-down list, then historical poll data will not be available when you click any of the following buttons:

- **Last Day**
- **Last Week**
- **Last Month**
- **Last Year**

Current
Click this button to display current raw poll data. When in time trace mode, depending on the frequency of polling of the associated poll policy, the time trace shows anything up to two hours of data.

Last Day
Click this button to show data based on a regularly calculated daily average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a daily exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 24 hours is shown, based on the average values.

In the **Last Day** section of the widget EWMA values are calculated by default every 15 minutes and are based on the previous 15 minutes of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every 15 minutes.

Last Week
Click this button to show data based on a regularly calculated weekly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a weekly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 7 days is shown, based on the average values.

In the **Last Week** section of the widget EWMA values are calculated by default every 30 minutes and are based on the previous 30 minutes of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every 30 minutes.

Last Month
Click this button to show data based on a regularly calculated monthly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a monthly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 30 days is shown, based on the average values.

In the **Last Month** section of the widget EWMA values are calculated by default every two hours and are based on the previous two hours of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every two hours.

Last Year
Click this button to show data based on a regularly calculated yearly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a yearly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 365 days is shown, based on the average values.

In the **Last Year** section of the widget EWMA values are calculated by default every day and are based on the previous 24 hours of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every day.

Investigating the health of device components

Investigate the health of device components in order to isolate the fault within a network device.

About this task

Use the **Structure Browser** to investigate the health of device components.

Viewing the structure of a network device

Use the **Structure Browser** to view the internal structure of the device and investigate the health of the device components.

About this task

The following topics describe how to use the **Structure Browser** to view the internal structure of a device.

Using the Structure Browser with the Network Hop View

View the structure of a device displayed in the Hop View and investigate the health of the device components using the **Structure Browser**.

About this task

When you launch the **Network Hop View**, the **Structure Browser** widget also opens. The **Structure Browser** opens in either tree or table mode, depending how it has been configured.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **Network Hop View**.

   The **Network Hop View** page opens and the following two widgets display within the page.

   The **Network Hop View** widget.
   The **Structure Browser** widget.

   Note: When you first open the **Network Hop View**, the **Structure Browser** is empty.
2. Display a device in the **Network Hop View**.

   For information about displaying devices in the **Network Hop View**, see the *IBM Tivoli Network Manager User Guide*.
3. From the **Network Hop View**, select the device for which you wish to show the structure.

   The **Structure Browser** is automatically updated to show a tree or table for the selected device. You can now investigate faulty components using the tree or table mode.

Related tasks

Customizing Structure Browser preferences
The administrator can change configuration settings for the Structure Browser. Edit the configuration files to change the appearance of the Structure Browser.

Switching between tree and table mode in the Structure Browser
If the **Structure Browser** is displayed as a widget, you can choose to display the **Structure Browser** in tree mode or table mode.

Identifying faulty components from the Structure Browser tree

Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Identifying faulty components from the Structure Browser table
Using the table mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Searching the node text in the Structure Browser tree
You can search for a value within the nodes in the **Structure Browser** tree.

Viewing the structure of a device from the Network Views

Show the structure of devices from a network map in order to view the device components.

Procedure

1. In the **Network Views** network map, select a device to view components for the selected device.

   Press the Ctrl key to select multiple devices.
2. Right-click one of the selected devices and choose **Show Device Structure**.

   The **Structure Browser** tree displays the structure of the selected device.

   Note: The **Structure Browser** table is only available when the **Structure Browser** is viewed as a widget.

Related tasks

Searching the node text in the Structure Browser tree
You can search for a value within the nodes in the **Structure Browser** tree.

Identifying faulty components from the Structure Browser tree
Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Showing events for a device or component
Show events for a device or component from within the **Structure Browser** to isolate the fault within a network device.

Opening the Structure Browser from the event list

Launch the **Structure Browser** from an **Event Viewer** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

Before you begin

To perform this procedure, you must be in the **Event Viewer**.

Procedure

1. In the event list, select the event of interest.

   To select multiple events, press Ctrl while you click. To select continuous events, select the first event in a continuous list and then press Shift while you click the last event in the continuous list.
2. Right-click anywhere in the event list and select **Show Device Structure**.

   After a few moments the **Structure Browser** opens in one or more separate browser windows. Each **Structure Browser** appears in tree mode preloaded with the structure of the device associated with the selected event.

What to do next

You can now perform any of the following actions:

- Identify faulty components
- Show events for faulty components

- Navigate within the structure of this device

Related tasks

Customizing Structure Browser preferences
The administrator can change configuration settings for the Structure Browser. Edit the configuration files to change the appearance of the Structure Browser.

Identifying faulty components from the Structure Browser table
Using the table mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Switching between tree and table mode in the Structure Browser
If the **Structure Browser** is displayed as a widget, you can choose to display the **Structure Browser** in tree mode or table mode.

Searching the node text in the Structure Browser tree
You can search for a value within the nodes in the **Structure Browser** tree.

Identifying faulty components from the Structure Browser tree
Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Showing events for a device or component
Show events for a device or component from within the **Structure Browser** to isolate the fault within a network device.

Identifying faulty components from the Structure Browser tree

Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

About this task

The **Structure Browser** has two modes: `tree` and `table`. When the Structure Browser is opened from an event list or from the Network Views, it always opens in tree mode and cannot be displayed in table mode. When the **Structure Browser** is displayed as a widget, it can be configured to display in either tree mode or table mode.

Procedure

1. In the **Structure Browser** window, go to the **Device Structure Tree** on the left hand side and look for the critical alert in the alert status indicator column.

   The alert status indicator column is on the right-hand side of the tree.

   Remember: The most severe alert affecting a device component is displayed at the main node level in the tree. From here, you can drill down into the device components and see what the most severe alert is on each component.
2. Expand the tree and locate a faulty component.
   For example, a device fault might be caused by a faulty Ethernet Gigabit port interface.
3. Select the faulty component. When highlighted, all information available about the faulty interface is displayed in the **Component Detail Table**.
   You can use the information in the **Component Detail Table** to provide exact details of the device component that is failing in a trouble ticket. Also, make a note of the containment path displayed in the **Component Path** area. This is useful as a quick reference to the faulty component, and can be added to the trouble ticket.
4. Use the following items in the **Tools** menu to perform actions on the component.

   Show Events
   Starts the **Event Viewer**to display all alerts for the selected device or component.

Find in Network View
Starts the **Network Views** in a new window and displays the network topology, with the device that contains the selected component highlighted.

Find in Network Hop View
Starts the **Network Hop View** in a separate window and displays the network topology, with the device containing the selected component highlighted.

Find in Path View
Displays any paths to which the selected device belongs.

Trace IP Path
You can select a device in the Network Hop View and launch the **Trace IPv4 network path** window with that device already defined as the start point of a path. If you select two devices before launching the **Trace IPv4 network path** window from these interfaces, the end point will also be populated.

Create a Poll Policy
Creates a new network poll for the selected device. Only create a new poll if you are a network administrator and you are familiar with the network.

Browse SNMP MIB Data
Starts the **SNMP MIB Browser** in a separate window where you can perform SNMP queries on the selected device.

Graph SNMP MIB Data
Opens the MIB Grapher with a historical display of snmpInBandwidth. To define the information that is displayed, open the **Graph Properties** window.

Discovery > Show Discovery Overview
Displays discovery information about one or more selected entities, including when the entity was first discovered, last discovered, and last rebooted.

Manage/Unmanage
Puts the selected device or component into a managed or unmanaged state.

Ping from this host
Starts the generic ping tool on the local workstation and pings the currently-selected device.

Telnet
Starts a Telnet window from which you can log into the currently-selected workstation.

Reports
Lists the available reports for the device.

Webtools
Lists the deployed webtools.

Related concepts

About the Structure Browser
The Structure Browser allows you to navigate the internal structure of a device. You can also use the Structure Browser to investigate the health of device components and isolate a fault within a network device. The Structure Browser has two modes: tree and table.

Related tasks

Using the Structure Browser with the Network Hop View
View the structure of a device displayed in the Hop View and investigate the health of the device components using the **Structure Browser**.

Switching between tree and table mode in the Structure Browser
If the **Structure Browser** is displayed as a widget, you can choose to display the **Structure Browser** in tree mode or table mode.

Searching the node text in the Structure Browser tree
You can search for a value within the nodes in the **Structure Browser** tree.

Showing events for a device or component

Show events for a device or component from within the **Structure Browser** to isolate the fault within a network device.

Creating polls
Create a poll if existing monitoring of network devices does not meet your requirements. You can configure ping, link state, and threshold polls directly from the network map.

Retrieving MIB information
Retrieve MIB variable information from network devices to diagnose network problems.

Identifying faulty components from the Structure Browser table

Using the table mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

About this task

The **Structure Browser** has two modes: `tree` and `table`. When the **Structure Browser** is displayed as a widget, it can be configured to display in either tree mode or table mode. Complete these steps in table mode.

Procedure

1. Select the faulty entity in the Hop View.
2. In the **Structure Browser** table, click the **Show device information** button  .
3. Find a faulty interface in one of two ways.
   - Browse the table.
   - Sort the status field by clicking the column header.
   - Click the **Filter On** drop-down list and select the columns that you want to filter on. Type a value to filter on in the box.
4. Click the **Show interfaces** button  or the **Show device connectivity** button  .

   Note: You can also double-click on the interface to open the **Structure Browser** tree in a stand-alone window and access **Tools** from the tree.
5. Select a row and right-click to select **Tools**.
6. Use the following items in the **Tools** menu to perform actions on the component.

   Show Events
   Starts the **Event Viewer**to display all alerts for the selected device or component.

   Find in Network View
   Starts the **Network Views** in a new window and displays the network topology, with the device that contains the selected component highlighted.

   Find in Network Hop View
   Starts the **Network Hop View** in a separate window and displays the network topology, with the device containing the selected component highlighted.

   Find in Path View
   Displays any paths to which the selected device belongs.

   Trace IP Path
   You can select a device in the Network Hop View and launch the **Trace IPv4 network path** window with that device already defined as the start point of a path. If you select two devices before launching the **Trace IPv4 network path** window from these interfaces, the end point will also be populated.

Create a Poll Policy
Creates a new network poll for the selected device. Only create a new poll if you are a network administrator and you are familiar with the network.

Browse SNMP MIB Data
Starts the **SNMP MIB Browser** in a separate window where you can perform SNMP queries on the selected device.

Graph SNMP MIB Data
Opens the MIB Grapher with a historical display of snmpInBandwidth. To define the information that is displayed, open the **Graph Properties** window.

Discovery > Show Discovery Overview
Displays discovery information about one or more selected entities, including when the entity was first discovered, last discovered, and last rebooted.

Manage/Unmanage
Puts the selected device or component into a managed or unmanaged state.

Ping from this host
Starts the generic ping tool on the local workstation and pings the currently-selected device.

Telnet
Starts a Telnet window from which you can log into the currently-selected workstation.

Reports
Lists the available reports for the device.

Webtools
Lists the deployed webtools.

Related concepts

About the Structure Browser
The Structure Browser allows you to navigate the internal structure of a device. You can also use the Structure Browser to investigate the health of device components and isolate a fault within a network device. The Structure Browser has two modes: tree and table.

Related tasks

Using the Structure Browser with the Network Hop View
View the structure of a device displayed in the Hop View and investigate the health of the device components using the **Structure Browser**.

Opening the Structure Browser from the event list
Launch the **Structure Browser** from an **Event Viewer** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

Searching the node text in the Structure Browser tree

You can search for a value within the nodes in the **Structure Browser** tree.

About this task

You can enter a string to be matched against the following set of predefined database fields:

- ifName, ifDescr, ifAlias, ifTypeString, ifPhysAddress, accessIPAddress, accessProtocol, duplex, and entPhysicalVendorType in the interface table
- address, protocol, subnet, and DNSName in the ipEndPointTable table

To search within the **Device Structure Tree** in the **Structure Browser**:

Procedure

1. Enter the search string in the field located to the right of the **Expand All**  and **Collapse All**  buttons.

Note: The search string is case-insensitive and can be a complete value (for an exact search) or a wildcard. The supported wildcards, which can be appended to a search string, are * and %. For example, to search for IP addresses that begin with 172, you can enter 172* or 172%.

2. Ensure that the root node is selected in the tree.

   Tip: The tree is traversed from the selected node, with the search being performed from top to bottom.

3. Click **Find/Find Next**  in turn to find the first and subsequent matching nodes.

   Each matching node is selected in turn within the tree, and the associated information is displayed in the **Component Detail Table**.

Related concepts

About the Structure Browser

The Structure Browser allows you to navigate the internal structure of a device. You can also use the Structure Browser to investigate the health of device components and isolate a fault within a network device. The Structure Browser has two modes: tree and table.

Related tasks

Using the Structure Browser with the Network Hop View

View the structure of a device displayed in the Hop View and investigate the health of the device components using the **Structure Browser**.

Viewing the structure of a device from the Network Views

Show the structure of devices from a network map in order to view the device components.

Opening the Structure Browser from the event list

Launch the **Structure Browser** from an **Event Viewer** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

Identifying faulty components from the Structure Browser tree

Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Switching between tree and table mode in the Structure Browser

If the **Structure Browser** is displayed as a widget, you can choose to display the **Structure Browser** in tree mode or table mode.

About this task

Restriction: If the **Structure Browser** is started from a right-click tool, it is always displayed in tree mode. Table mode is only available when the **Structure Browser** is displayed as a widget, for example, within a **Network Hop View** in a default installation.

To change the display mode of a **Structure Browser** widget, complete the following steps.

Procedure

1. From the **Structure Browser** widget, click **Edit**  .
2. Select `Tree` or `Table` from the **View Mode** list.

   This setting overrides the default set by the administrator.

Related tasks

Using the Structure Browser with the Network Hop View

View the structure of a device displayed in the Hop View and investigate the health of the device components using the **Structure Browser**.

Opening the Structure Browser from the event list

Launch the **Structure Browser** from an **Event Viewer** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

Identifying faulty components from the Structure Browser tree
Using the tree mode of the **Structure Browser**, you can identify a faulty component in order to retrieve further details about the critical alert.

Showing events for a device or component

Show events for a device or component from within the **Structure Browser** to isolate the fault within a network device.

About this task

Procedure

1. Open the **Structure Browser** in either tree or table mode.
2. Select a faulty device or component.
3. Click **Tools** > **Show Events**.

Results

An **Event Viewer** appears in a separate browser window containing the events on the selected device or component.

Note:

All alerts on the device are shown when you use the Show Events tool. It is possible that, for example, Critical alerts are shown when you use the Show Events tool on a device from the default Major alerts view. Default network views that are based on alert severity are filtered such that they contain only devices that have one or more alerts of that severity. However, those devices can also have alerts of other severities. It is possible to edit the filters for the network views to include only devices that have a certain alert severity and no other alert severities. However, take care that devices that have multiple alerts with different severities are not accidentally omitted from your network view hierarchy.

Customizing Structure Browser preferences

The administrator can change configuration settings for the Structure Browser. Edit the configuration files to change the appearance of the Structure Browser.

About this task

The configuration files are located in the `$NMGUI_HOME/profile/etc/tnm/` directory. The `structurebrowser.properties` file controls settings that are related to the Structure Browser window. The `status.properties` file controls all status indicator settings for both the Topoviz views and the Structure Browser window. The `ncp_structurebrowser_menu.xml` file controls what tools are available from the Structure Browser.

Note: The configuration files are monitored for changes every 60 seconds, so changes are automatically detected by the Structure Browser.

Procedure

1. From the command line, navigate to the `$NMGUI_HOME/profile/etc/tnm/`directory.
2. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/structurebrowser.properties` file.

Structure Browser property	Description
structurebrowser.default.viewMode	Specifies the default mode for the Structure Browser when it is opened as a widget. The default mode determines how data is

Structure Browser property	Description
	displayed when the Structure Browser is opened as a widget. The two options are `tree` or `table`. The default mode can be overriden by a user's widget preferences. **Note:** The Structure Browser table is only available when the Structure Browser is opened as a widget. The table cannot be launched as a stand-alone window.
structurebrowser.showManagedStatus	Specifies whether to show the managed status of a device from the tree or the interface or connectivity tables. If the value is set to `false`, then managedStatus is hidden.
structurebrowser.table.connectivity.style.*columnName*	Aligns text in a particular column in the Structure Browser Connectivity Table to the left, right, or center. For example: `structurebrowser.table.connectivity.style.severity=text-align: left`
structurebrowser.table.connectivity.width.local*ColumnName*	Specifies the width of individual columns for the local interface in the Connectivity view of the Structure Browser in table mode in units of em or px.
structurebrowser.table.connectivity.width.connectivity	Specifies the width of the Connectivity column in units of em or px.
structurebrowser.table.connectivity.width.*columnName*	Specifies the width of individual columns for the remote interface in the Connectivity section of the Structure Browser in table mode in units of em or px.
structurebrowser.table.default.view	Fix Pack 6 Specifies the view in which the Structure Browser portlet opens when a single device is displayed. The following values are allowed: • `devicetable`: opens the device view. This is the default value. • `interfacestable`: opens the interfaces view. • `connectivitytable`: opens the connectivity view. This property has no effect when the portlet displays a connection between devices, because only one view is available in this case.
structurebrowser.table.device.style.*columnName*	Fix Pack 8 Aligns text in a particular column in the Structure Browser Device Table to the left, right, or center. For example: `structurebrowser.table.device.style.severity=text-align: left`
structurebrowser.table.device.width.*columnName*	Fix Pack 8 Specifies the width of individual columns in the Devices view of the Structure Browser in table mode. The width is measured in units of em or px.
structurebrowser.table.interfaces.style.*columnName*	Aligns text in a particular column in the Structure Browser Interfaces Table to the left, right, or center. For example: `structurebrowser.table.interface.style.severity=text-align: left`

Structure Browser property	Description
structurebrowser.table.interfaces.width.*columnName*	Specifies the width of individual columns in the Interfaces view of the Structure Browser in table mode. The width is measured in units of em or px.

structurebrowser.tree.device.icon.x	Specifies the managed status icon to display in the tree and the table, where x is the entity type, as defined in the ncim.entityTypes database table.
	For example, to change the icon displayed for a PSU, save your new icon as a .PNG file of size 18x18 pixels with a file name of `psu2_18.png` into the `$INSTALL/tipv2/profiles/TIPProfile/installedApps/TIPCell/isc.ear/ncp_structureview.war/styles/images/devices` directory, then edit the following line and change the value `psu` to `psu2`. Note that the file names of all Structure Browser icon files must end in `_18.png`:
	`# PSU`
	`structurebrowser.tree.device.icon.6=psu`

structurebrowser.tree.device.node.display	Fix Pack 9 Set this property to `ifAlias`, as in the following example, in order to append the interface alias to the interface name in the Device Structure Tree. `structurebrowser.tree.device.node.display=ifAlias`
structurebrowser.tree.device.node.ifType	Fix Pack 9 Set this property to the value of the interface type for which you want to append the interface alias to the interface name. For this property to take effect, you must also configure the `structurebrowser.tree.device.node.display` property. If you do not specify a value, the interface alias is appended to the interface name for every type. The following example shows the property configured for multiple interface types: `structurebrowser.tree.device.node.ifType=6,53`
structurebrowser.tree.device.node.separator	Fix Pack 9 Specifies the separator to be used between the interface name and interface alias, if you have configured the `structurebrowser.tree.device.node.display` property to append the alias. Allowed values are any one of the following: `$ @ % * & + = - _` The following example uses the $ character as a separator: `#structurebrowser.tree.device.node.separator=$`

Restriction: The features available depend on the version of the product installed. If the latest version is installed and the lines to set the default view mode and the column widths are not present in the configuration file, copy the lines into the `$NMGUI_HOME/profile/etc/tnm/`

`structurebrowser.properties` file from the `$NMGUI_HOME/profile/etc/tnm/default/structurebrowser.properties` file.

3. Save and close the file.
4. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/status.properties` file.

Status property	Description
status.enabled	Specifies whether the status field is visible from the interface and connectivity tables.
status.none.enabled	Specifies whether an icon is displayed when the status is Clear.
status.tree.updateperiod	Specifies how often the table and the tree are updated or refreshed. This property also controls status updates.
status.tree.image.x	Specifies the status icons for the table and the tree.

5. Save and close the file.

Related tasks

Using the Structure Browser with the Network Hop View
View the structure of a device displayed in the Hop View and investigate the health of the device components using the **Structure Browser**.

Opening the Structure Browser from the event list
Launch the **Structure Browser** from an **Event Viewer** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

Fix Pack 6 Configuring column display in the Structure Browser

You can configure which columns are displayed in the **Structure Browser** table mode. You can also configure the horizontal alignment of displayed text.

About this task

You can configure which columns are displayed, and how text is aligned, in the device table, interfaces table, or both, when the **Structure Browser** is in table mode.

To configure which columns are displayed, complete the following steps:

Procedure

1. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/ncimMetaData.xml` file.
2. Locate the following section and add or remove any columns that you want to display in the device table.

```
<columnView tableMode="devicetable">
    <columnName tableAlias="e" column="displayLabel"/>
    <columnName tableAlias="c" column="accessIPAddress"/>
    <columnName tableAlias="m" column="classType"/>
    <columnName tableAlias="c" column="className"/>
</columnView>
```

The `tableAlias` and `column` attributes must match a `<dataField>` tag in the `<entityMetaData>` tag whose entityType attribute equals 1 (chassis). The `<listDataField>` and `<extraInfo>` tags are not supported.

If the `<entityMetaData entityType="1">` tag does not contain a `<columnView tableMode="devicetable">` tag, the device view displays all configured columns from that `<entityMetaData>` tag.

If you add `<columnView tableMode="devicetable">` to entityType 1, you must also add the tag and its child tags to the `<entityMetaData>` tags for entityType 8 (daughter card) and entityType 191 (probe).

Important:

You must use the correct tableAlias for the table.

- c = physicalChassis
- e = entityDatal = lingerTime
- m = mainNodeDetails
- os = operating System
- cs = computerSystem
- ss = snmpSystem
- vm = virtualMachine
- vs = virtualSwitch
- bsc = ranBaseStationController
- bs = ranBaseStation
- wap = wlanAccessPoint
- lteaf = antennaFunction

3. Locate the following section and add or remove any columns that you want to display in the interfaces table.

```
<columnView tableMode="interfacestable">
    <statusColumn statusColumn="severity"/>
    <statusColumn statusColumn="managedStatus"/>
    <columnName tableAlias="e" column="entityId"/>
    <columnName tableAlias="e" column="entityName"/>
    <columnName tableAlias="e" column="displayLabel"/>
    <columnName tableAlias="n" column="accessProtocol"/>
    <columnName tableAlias="n" column="ifDescr"/>
    <columnName tableAlias="n" column="ifType"/>
    <columnName tableAlias="n" column="ifTypeString"/>
</columnView>
```

   The table displays the columns in the order specified here.

   The `entityId` column must be present, but can be in any position.

   The following columns must be specified using `statusColumn`, as in the default example above:

   - `severity`
   - `managedStatus`

   The `tableAlias` and `column` attributes must match a `<dataField>` tag in the `<entityMetaData>` tag whose entityType attribute equals 2 (interface). The `<listDataField>` and `<extraInfo>` tags are not supported.

   If the `<entityMetaData entityType="2">` tag does not contain a `<columnView tableMode="interfacestable">` tag, the device view displays all configured columns for interfaces.

4. Save and close the `$NMGUI_HOME/profile/etc/tnm/ncimMetaData.xml` file.
5. You can also configure various properties in the `$NMGUI_HOME/profile/etc/tnm/structurebrowser.properties` file such as column widths and text alignment. See “Customizing Structure Browser preferences” on page 407 for more information.

Showing device connectivity

Run this command on a device in the network map to see the interfaces on that device and associated connections for each interface. The command retrieves connections that are on the same layer as the view from which the command was launched.

Procedure

1. From the **Network Hop View** GUI or the **Network Views** GUI select a device in the network map.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and click **Show Connectivity Information**.
   A new browser window is displayed for each of the selected devices. The window contains a table with the following connectivity information. Each row in the table represents a device connection.

Local node
Specifies connectivity information for the selected device.

Entity name
Specifies the IP address or hostname of the selected device.

Interface description
Specifies descriptive information for a connected interface on the selected device.

Interface type
Specifies the interface type for the connected interface.

Neighbor node
Specifies connectivity information for devices connected to the selected device.

Entity name
Specifies the IP address or hostname of a device connected to the selected device. Click this hyperlink to open a separate browser window showing connectivity information for this device.

Interface description
Specifies descriptive information for an interface connected to the selected device.

Interface type
Specifies the interface type for an interface connected to the selected device.

Retrieving MIB information

Retrieve MIB variable information from network devices to diagnose network problems.

About this task

The following topics describe how to retrieve MIB information.

About the SNMP MIB Browser

Use the **SNMP MIB Browser** to retrieve MIB variable information from network devices to support diagnosis of network problems.

The **SNMP MIB Browser** obtains MIB data from devices in the discovered topology. Using the **SNMP MIB Browser**, you can navigate within the MIB for the selected device and retrieve the value of any MIB variables.

The **SNMP MIB Browser** enables you to issue SNMP MIB queries on a specified network device and display the results of these queries.

The **SNMP MIB Browser** enables you to perform diagnostic work when trying to resolve problems on network devices. In particular, the **SNMP MIB Browser** enables you to perform the following tasks:

- View values of MIB objects for any device on your network. You can browse the MIB tree, issue SNMP queries – using SNMP `Get`, `Get Next`, `Get Table`, `Walk`, and `Graph` commands – and view resulting data. This data can help you to resolve problems on a device.
- Perform immediate diagnosis on network devices that are displaying faulty behavior.

Restriction: You can use the **SNMP MIB Browser** to display MIB information only. You cannot use the **SNMP MIB Browser** to modify MIB information.

Accessing MIB data

Access MIB variables for network devices in order to diagnose problems on network devices.

About this task

The following topics describe how to access MIB data.

Accessing the SNMP MIB Browser

Access the **SNMP MIB Browser** to retrieve MIB variable values for network devices and diagnose problems on those devices.

Procedure

1. Click the **Incident** icon and select **Network Availability** > **SNMP MIB Browser**.
2. In the **SNMP MIB Browser** issue an SNMP MIB query for a device.

Related tasks

Issuing an SNMP MIB query
Issue a MIB query to retrieve MIB variables from network devices and subsequently diagnose problems on those devices.

Launching the SNMP MIB Browser from an event list

Launch the **SNMP MIB Browser** from an event list in order to diagnose problems on network devices associated with selected events.

Before you begin

To perform this procedure, you must be in the **Event Viewer**.

Procedure

1. In the event list select the event of interest.

   To select multiple events, press Ctrl while you click. To select contiguous events, select the first event in a continuous list and then press Shift while you click the last event in the continuous list.
2. Right-click anywhere in the event list and choose **Browse SNMP MIB Data**.

   After a few moments the **SNMP MIB Browser** opens in one or more separate browser windows. Each **SNMP MIB Browser** appears preloaded with the IP address of the device associated with the selected event.

What to do next

You can now issue an SNMP MIB query for this device.

Related tasks

Issuing an SNMP MIB query

Issue a MIB query to retrieve MIB variables from network devices and subsequently diagnose problems on those devices.

Launching the SNMP MIB Browser from the Hop View or Network Views

Launch the **SNMP MIB Browser** from the **Network Hop View** or **Network Views** in order to diagnose problems on selected network devices.

Procedure

1. From the **Network Hop View** or **Network Views** network map, select the device from which to retrieve MIB data.

   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **Browse SNMP MIB Data**.

   The **SNMP MIB Browser** opens in one or more separate browser windows. Each **SNMP MIB Browser** appears preloaded with the IP address of the selected event.

What to do next

You can issue an SNMP MIB query for this device.

Related tasks

Issuing an SNMP MIB query

Issue a MIB query to retrieve MIB variables from network devices and subsequently diagnose problems on those devices.

Launching the SNMP MIB Browser from the Structure Browser

Launch the **SNMP MIB Browser** from the **Structure Browser** to diagnose problems for a device.

About this task

The **Structure Browser** has two display modes: tree and table. The tree mode can be accessed by right-clicking a device and selecting **Show Device Structure**; the tree is also available as a widget. The table mode is shown underneath the Hop View in a default installation. The table is only available from a widget.

Procedure

1. Navigate to the **Structure Browser**.
2. From either the tree or the table, proceed as follows.
   - From the tree, select an entity that has SNMP data associated with it and click **Tools** > **Browse SNMP MIB Data**.
   - From the table, click **Show Interfaces** or **Show Device Connectivity** and then select a row and right-click to select **Tools** > **Browse SNMP MIB Data**.

   After a few moments, the **SNMP MIB Browser** window opens preloaded with the IP address of the selected device.

What to do next

You can now issue an SNMP MIB query for the device.

Related tasks

Issuing an SNMP MIB query

Issue a MIB query to retrieve MIB variables from network devices and subsequently diagnose problems on those devices.

Issuing an SNMP MIB query

Issue a MIB query to retrieve MIB variables from network devices and subsequently diagnose problems on those devices.

Before you begin

To perform this procedure, you must be in the **SNMP MIB Browser**.

Procedure

1. Navigate to the part of the MIB tree that contains the MIB object that you wish to query and select the desired MIB object. Specify the MIB object that you wish to query. You can do this in one of the following ways:

   The **OID** field displays the MIB object identifier that corresponds to the MIB object you selected.

   Tip: Standard MIB variables can be found at the MIB tree path `iso/org/dod/internet/mgmt/mib-2`. Vendor-specific MIB variables can be found at the MIB tree path `iso/org/dod/internet/private/enterprises`.
2. Type the IP address or hostname of the target device in the **Host** field.

   If you launched the **SNMP MIB Browser** from the **Event Viewer**, from a network map, or from the **Structure Browser**, then the **Host** field is automatically filled in when the **SNMP MIB Browser** starts.
3. Select the query to issue from the **Method** drop-down list.

   The options available within this menu are:

   Get
   Use this query to obtain a single (scalar) values; for example, sysUpTime

   Get Next
   Use this query to obtain the next single (scalar) value in an array.

   Walk
   Use this query to obtain array data; for example, system.

   Get Table
   Use this query to obtain table data.

   Graph
   Use this query to start the Graph Properties window and specify the information (content and scope) to be displayed in the MIB graph.

   The choice of SNMP query is constrained by the type of MIB object you selected..

   For example, you cannot perform a Get query on a MIB variable of type table. If you try to issue a query on a node that does not accept that query, the **SNMP MIB Browser** responds with a warning.
4. Deselect the **Ignore filtering** checkbox if you want to limit the interfaces that the **SNMP MIB Browser** queries by applying any interface filters that are configured. By default, the **Ignore filtering** option is selected, and the **SNMP MIB Browser** has access to all interfaces, regardless of any interface filters. Interface filters only apply to SNMP walks and SNMP table requests. The **Ignore filtering** checkbox is only active when the **Walk** or **Get Table** option is selected in the **Method** list.
5. Click **Go**.

   The results of the query appear in the **SNMP Query Results** area.

   Note: If the SNMP query yields no results, the reason may be one of the following:

   - The MIB object you selected does not exist on the host.
   - The SNMP Helper, the device that the **SNMP MIB Browser** uses to query the host, is unable to access the host.

6. To refresh MIB object data to see how data has changed since the last time a query was issued, click the **Go** button.

SNMP queries available from the SNMP MIB Browser

Use this information to understand the SNMP queries that you can issue using the **SNMP MIB Browser**.

You can use the **SNMP MIB Browser** to issue SNMP queries, as described in the following table. The examples shown in the table can all be found within the **MIB tree** at the following path: `iso/org/dod/internet/mgmt/mib-2`.

*Table 44. SNMP Queries Available from the **SNMP MIB Browser***

SNMP Query	Description	Node	Example

`Get`	Performs a single instance lookup. It obtains a MIB object together with an instance of this MIB object. For example, if you perform a `Get` query on the `sysDescr` MIB object, then you obtain data for an instance of this single MIB object, `sysDescr.0`.	Single MIB objects only	`sysDescr`
			`sysUpTime`
			`sysLocation`

`Get Next` `Walk`	Obtains all instances of a MIB object. This query only works with MIB objects that are sequential. For example, if you issue a `Get Next` query on `ifDescr`, which is a column object in the table `ifTable`, then this query returns the value for all instances of `ifDescr` in the table, that is, `ifDescr.1` and `ifDescr.2`. Note that the `Get Next` and `Walk` queries both perform the same operation.	Single MIB objects	`sysDescr`
		Tables	`ifTable` `ipRouteTable`
		Single MIB objects that represent columns in a table	`ifDescr`
		Branch nodes that contain only single MIB objects	`icmp`
		Branch nodes that contain only tables	`at`
		Branch nodes that contain single MIB objects and tables	`system` `interfaces`
`Get Table`	Obtains a MIB table, which is a grouping of MIB objects. For example, the `interfaces` table contains information for all interfaces on a network device.	Tables	`ifTable` `ipRouteTable`
`Graph`	Displays a real-time graph of a MIB variable for the selected device.	Numerical single MIB objects only	`memory usage`

Graphing MIB variables

You can display a real-time graph of MIB variables for a device and use the graph for fault analysis and resolution of network problems.

Configuring MIB graph properties and preferences

You use SNMP MIB Graph to define the information and the scope of the information that is displayed in the MIB graph.

About this task

You first define graph properties, before expanding the Preferences area to define your display preferences.

Procedure

1. In the Properties section, accept the default values or provide new values for the fields:

   Domain
   Specifies the device domain from a list of domains that are currently supported by Network Manager.

   Host
   Specifies the device hostname or IP address. The host field supports either hostname, or an IPv4/IPv6 address. This field can be passed in from the **Event Viewer**, Network View, Network Hop View, structure browser, or MIB Browser.

   Poll data
   Contains a list of up to two poll definitions or MIB OIDs that have been added. The **Add** button becomes inoperable once two polls have been added.

   MIB OID
   Specifies the use of a MIB OID. The default value is selected. When selected, the MIB OID text field and **Browse** button are enabled for input.

   Poll Definition
   Specifies the use of a poll definition. The default value is unselected. When selected, the **Poll Definition** dropdown and the **New** button are enabled.

   Polling interval (seconds)
   Provides the polling interval to be used for sending requests to the device to retrieve the desired values.

2. In the Preferences section, accept the default values or provide new values for the fields:

   Title
   Specifies the title of the graph. The default value is *Hostname – MIBOID/PollDef name*.

   Graph refresh interval (seconds)
   Specifies the period between device queries. The default value is 15 seconds.

   Default selected rows
   Specifies whether the lowest or highest values will be graphed/selected by default.

   Column
   Specifies which column will be graphed/selected by default. The choices are average, current, maximum, and minimum. The default is current.

   Override SNMP Community String (SNMP v1 and v2 only)
   Optionally allows you to override the community string currently being used by the polling engine. The default value is unselected. When the checkbox is selected, the Community string field is enabled.

   Community String
   Optionally specifies the community string to be used in the device query. The default value is blank and disabled. This field supports overriding SNMP v1 and v2 community strings only.

Working with the MIB graph

A graph can display data for up to two MIB OIDS or poll definitions against the same host. You can take several actions when viewing a MIB graph.

Before you begin

A MIB graph must be configured before you can view it. .

About this task

You can view MIB graphs in the SNMP MIB Graph widget accessed from Network Availability, or launch it in context from another interface. If launched in context, SNMP MIB Graph is displayed in a separate browser window.

Procedure

1. Open SNMP MIB Graph.
   - Place the mouse cursor over a line to display summary graph data.
   - Toggle to the table view to view detailed graph data.
2. Use the graph toolbar in the following way:

   Graph/Table
   Switches graph area between graph view and table view.
3. Use the main toolbar in the following way:

   Configure
   Switches to Edit mode.

   Copy graph configuration
   Launches a new browser window with a copy of the current graphs configuration to allow the user to use all the current settings, but perhaps alter the device.

   Legend/Line
   Switches the legend area to the table view to allow manual line selection.

   Auto-line
   Switches the lines to be displayed between the following options:
   - User select (displays the Line Selection table)
   - Highest average
   - Lowest average
   - Highest current
   - Lowest current
   - Highest maximum
   - Lowest maximum
   - Highest minimum
   - Lowest minimum

   Apply
   Applies changes to line selection.
4. If you have selected User Select in the previous step, use the line selection table to manually select the lines to be displayed in the graph.

Chapter 19. Supporting problem resolution

Support problem resolution by helping network engineers work on devices.

About this task

The following topics describe how you can support problem resolution.

Creating polls

Create a poll if existing monitoring of network devices does not meet your requirements. You can configure ping, link state, and threshold polls directly from the network map.

Procedure

1. In the **Network Hop View** or **Network Views** network map select the device to poll.
   To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **Create a Poll Policy**.
   The **Poll Configuration Wizard** appears with the selected devices preloaded.

What to do next

You can configure a poll for the selected devices using the **Poll Configuration Wizard**.

Making devices available for maintenance

Make devices available for maintenance so that network engineers can work on known device problems.

About this task

The following topics describe how to put devices and their components into and out of unmanaged state.

Unmanaging devices and components

Place a device or its components into unmanaged state so that engineers can work on the device to resolve a problem.

About this task

The following topics describe how to place a device or its components into unmanaged state.

Placing devices into unmanaged state

Place a device into unmanaged state so that engineers can work on the device to resolve a problem.

About this task

Placing a device into unmanaged state deactivates Network Manager polling and event correlation for this device.

Note: The event list still displays events for this device generated due to polling by other network manager software, such as Tivoli Netcool/OMNIbus. You can configure the event list to filter out or to tag these events.

Procedure

1. In the **Network Hop View** or **Network Views** network map select the device to place into unmanaged state.

To select multiple devices, press Ctrl.

2. Right-click one of the selected devices and choose **Unmanage**.

A wrench icon  appears next to the selected devices indicating that the device is now in unmanaged state.

Placing device components into unmanaged state

Place device components, including interfaces, into unmanaged state so that engineers can work on the device and its components to resolve a problem.

About this task

Placing device components into unmanaged state deactivates Network Manager polling and event correlation for the components.

Note: The event list still displays events for the components generated due to polling by other Network Manager software, such as Tivoli Netcool/OMNIbus. You can configure the event list to filter out or to tag these events.

Complete these steps from the **Structure Browser**.

The **Structure Browser** has two display modes: tree and table. The tree mode can be accessed by right-clicking a device and selecting **Show Device Structure**; the tree is also available as a widget. The table mode is shown underneath the Hop View in a default installation. The table is only available from a widget.

Procedure

1. From the **Structure Browser**, identify a device with components that you want to change from managed state to unmanaged state and proceed as follows.
   - From the tree, double-click the device.
   - From the table, click **Show interfaces** or **Show device connectivity**.
2. Identify the managed device components that you want to change to unmanaged and click **Tools** > **Unmanage**.

Results

A wrench icon  appears next to the selected components indicating that these components are now in unmanaged state. Polling and event correlation stops for these components.

The Unmanage node tool

If a device is unavailable or defective, use the **`UnmanageNode.pl`** command to set a device to an unmanaged state by using the command-line interface.

If you set a device to unmanaged, Network Manager polling is suspended for the unmanaged node. In the **Event Viewer**, all alerts are tagged to indicate they are from an unmanaged device, and are not used for root cause analysis.

You can also unmanage individual devices or groups of devices from the topology map views. There is also an option to set individual components of a device to unmanaged state using the Structure Browser.

Note: After unmanaging a device, the poller does not stop the polling. You must restart the poller to complete ongoing process. Once the poller is started, it reads the new values for any device to add the devices to monitor instance table. If the device is unmanaged, then that device has to be removed from monitored instance table so that no further events are generated on that device.

Usage

This command is located in NCHOME/precision/bin.

The following syntax shows how the **UnmanageNode.pl** command works:

```
ncp_perl UnmanageNode.pl -domain DomainName -user username -pwd password -file
FileName -verbose host
```

The following table describes the command-line options for **UnmanageNode.pl**.

Table 45. UnmanageNode.pl command-line options

Command-line option	Description
`-domain` *DomainName*	Mandatory; the name of the domain where the node to be unmanaged resides.
`-user` *username*	Mandatory; the name of the NCIM database user.
`-pwd` *password*	Mandatory; the password for the NCIM database user.
`-file` *FileName*	Optional; file containing the list of nodes to be unmanaged. Add one IP address or host name per line in the file. **Note:** You must provide the names of the nodes either in a file or by entering them in the command line, as described in *host* below.
`-verbose`	Optional; provides more information on the screen.
`-host`	Optional; the name of the node to be unmanaged. You can add any number of nodes this way, separated by spaces. The information entered for a node can be either the IP address or the fully qualified host name. If you do not provide a host name, then the `-file` option must be used.

Examples

The following examples show how to use the **UnmanageNode.pl** command.

```
./ncp_perl UnmanageNode.pl -domain NCOMS -user root -pwd fruit -verbose -file
mynodes.txt
```

```
./ncp_perl UnmanageNode.pl -domain NCOMS -user root -pwd fruit -verbose
neptune.ibm.com 192.168.0.6
```

Taking devices and components out of unmanaged state

Place a device or any of its components back into managed state once the device problem has been resolved and you wish to receive events for this device once again.

About this task

The following topics describe how to take devices and components out of unmanaged state.

Taking devices out of unmanaged state

Place a device back into managed state once the device problem has been resolved and you wish to receive events for this device once again.

Procedure

1. In the **Network Hop View** or **Network Views** network map identify the unmanaged device.

   A wrench icon  next to the device indicates that it is unmanaged.
2. Check that the device responds to a ping command. Right-click the device and choose **Ping from this host**.

   If the ping test is successful, then go to the next step. If the device fails the ping test, then the device might require further investigation.
3. Right-click the device and choose **Manage**.

   The wrench icon disappears indicating that the device is now managed. Polling and event correlation now resume for this device.

What to do next

If the device was updated during the resolution of the problem, you should discover the device again to refresh the device information in the network topology.

Changing device components from unmanaged to managed state

Change device components, including interface, back to managed state if the problem was resolved and you want to receive events for the device components.

About this task

The **Structure Browser** has two display modes: tree and table. The tree mode can be accessed by right-clicking a device and selecting **Show Device Structure**; the tree is also available as a widget. The table mode is shown underneath the Hop View in a default installation. The table is only available from a widget.

Procedure

1. From either the tree or the table, identify a device with unmanaged components.

   These devices have a half-wrench icon  beside them.
2. From either the tree or the table, proceed as follows.
   - From the tree, double-click the device.
   - From the table, click **Show Interfaces** or **Show Connectivity**.
3. Identify the unmanaged device components and click **Tools** > **Manage**.

Results

The components are now managed and the wrench icons are removed. Polling and event correlation resumes for these components.

The Manage node tool

Use the **`ManageNode.pl`** to set the status of an unmanaged device back to the managed status by using the command-line interface.

This is useful when a device is in unmanaged state and you want to set it to managed state again to receive alerts that are not tagged unmanaged and are used for root cause analysis.

Usage

This command is located in NCHOME/precision/bin.

The following syntax shows how the **ManageNode.pl** command works:

```
ncp_perl ManageNode.pl -domain DomainName -user username -pwd password -file
FileName -verbose host
```

The following table describes the command-line options for **ManageNode.pl**.

Table 46. ManageNode.pl command-line options

Command-line options	Description
`-domain` *DomainName*	Mandatory; the name of the domain where the unmanaged node resides.
`-user` *username*	Mandatory; the name of the database user.
`-pwd` *password*	Mandatory; the password for the database user.
`-file` *FileName*	Optional; file containing the list of nodes to be set to managed state. Add one IP address or host name per line in the file. **Note:** You must provide the names of the nodes either in a file or by entering them in the command line, as described in *host* below.
`-verbose`	Optional; provides more information on the screen.
host	Optional; the name of the node to be set to managed state. You can add any number of nodes this way, separated by spaces. The information entered for a node can be either the IP address or the fully qualified host name. If you do not provide a host name, then the `-file` option must be used.

Examples

The following examples show how to use the **ManageNode.pl** command.

```
./ncp_perl ManageNode.pl -domain NCOMS -user root -pwd fruit -verbose -file
mynodes.txt
```

```
./ncp_perl ManageNode.pl -domain NCOMS -user root -pwd fruit -verbose
neptune.ibm.com 192.168.0.6
```

Adding and removing devices

You can add network devices to your network topology and remove network devices from your network topology by using the command-line interface.

Use the following Perl scripts to add and remove devices:

- Use the **AddNode.pl** command to add devices to the network topology.
- Use the **RemoveNode.pl** command to remove devices from the network topology.

For more information on the **AddNode.pl** and **RemoveNode.pl** Perl scripts, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Chapter 20. Reporting on devices

You can run reports on network devices to check the health of devices, summarize network and device data, or troubleshoot problems.

About this task

As a network operator, you can run reports from the GUI in several ways. Access to reports and report groups is controlled by the administrator. Your administrator can also create and customize reports. Ensure that at a minimum a reader is installed on your computer for the file format to which you output reports. For example, to output reports in `.pdf` format, install a PDF reader.

From Network Manager V4.2, reports no longer need to be filtered by date. Reports use the data from Apache Storm, which is already aggregated by time period. Where available, you can drill down into a smaller time period, for example, from one week to daily by using the drill-down report..

Note: Network Manager 4.2 supports reports in only PDF and HTML formats.

Tip: If your network is large and complex, detailed reports can potentially contain very large amounts of data. Reports that are hundreds of thousands of lines long can be more difficult to use, and can cause the reporting components to run out of memory. Ensure that your reports are optimized to return the data that is useful to you.

Running reports from the Reports window

You can run reports directly from the **Reports** window.

About this task

To run a report, complete the following steps.

Procedure

1. Click the **Reporting** icon and select **Common Reporting**. Within the widget, select **Network Manager**. A list of folders display. These folders contain all Cognos reports for your access.

   Note: On Linux on IBM z Systems, the option is called **Cognos Reporting**. If you are running reports using the remote Cognos Analytics 3.1 server, the reporting page might have a different name.
2. Click on a report set to see a list of available reports.
3. Click a report name to generate a report in HTML format.

   You can also use the **Actions** icons to customize or perform other actions on the report. For more information about the options available in the **Reports** window, click the help icon in the **Reports** window toolbar.

Running reports from a network map

You can run reports from any Network Manager topology display.

About this task

To run a report from a network map, complete the following steps.

Procedure

1. Navigate to the one of the following GUIs: **Network Views**, **Network Hop View**, **Path Views GUI**, or **Structure Browser**.
2. Right-click a device and click **Reports**.

All reports that are available to run on that device type are displayed.

3. Click the report that you want to run.
4. Enter any parameters required for the report.

Notices

This information applies to the PDF documentation set for IBM Tivoli Network Manager IP Edition.

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069
Australia

IBM Corporation
896471/H128B
76 Upper Ground
London
SE1 9PZ
United Kingdom

IBM Corporation
JBF1/SOM1 294
Route 100
Somers, NY, 10589-0100
United States of America

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

The terms in Table 47 on page 429 are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Table 47. IBM trademarks

AIX	Informix®	PR/SM
BNT	iSeries	System p
ClearQuest®	Lotus®	System z®
Cognos®	Lotus	Tivoli
Db2	Netcool	WebSphere®
Db2 Universal Database	NetView®	z/OS®
developerWorks®	OMEGAMON®	z/VM®
DS8000	Passport Advantage	zSeries
Enterprise Storage Server®	PowerPC	
IBM	PowerVM®	

Adobe, Acrobat, Portable Document Format (PDF), PostScript, and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering may collect IP addresses, user names and passwords for the purpose of performing network discovery. Failure to enable the collection of this information would likely eliminate important functionality provided by this Software Offering. You as customer should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details, and the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/privacy.

Part Number:

Printed in the Republic of Ireland

(1P) P/N:

2021-4213-01