

Network Manager IP Edition
Version 3 Release 9

Network Troubleshooting Guide



Network Manager IP Edition
Version 3 Release 9

Network Troubleshooting Guide



Note

Before using this information and the product it supports, read the information in “Notices” on page 103.

This edition applies to version 3.9 of IBM Tivoli Network Manager IP Edition (product number 5724-S45) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2006, 2013.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication	v
Intended audience	v
What this publication contains	v
Publications	vi
Accessibility	ix
Tivoli technical training	ix
Support information	x
Conventions used in this publication	x

Chapter 1. About network troubleshooting 1

About network views and the Network Hop View	1
Network Hop View	1
Network views	2
Network domains	3
Device connectivity	3
Network map and tree icons and symbols	4
Default network view nodes	6
About events	7
Default event status icons	8
About the Structure Browser	9

Chapter 2. Finding network devices . . . 13

Searching for devices using the Network Hop View	13
Using the basic search	13
Using the advanced search	14
Browsing the network using the Network Views	16
Searching for devices within a view	16
Finding Cisco devices in the current view	17
Finding Ethernet interfaces in the current view	17
Searching for a network view	17
Visualizing devices in tabular layout	18
Switching to tabular layout	19
Filtering devices in tabular layout	21

Chapter 3. Identifying network problems. 23

Identifying problems using network views	23
Using the Network Health View	23
Monitoring subnets	24
Monitoring device classes	24
Monitoring links	25
Monitoring Border Gateway Protocol (BGP) networks	26
Monitoring Open Shortest Path First (OSPF) routing domains	26
Monitoring multicast groups and routes	27
Monitoring MPLS Traffic Engineered tunnels	28
Monitoring VPLS VPNs	28
Identifying problems using event lists	28

Chapter 4. Diagnosing network problems. 31

Investigating faulty devices	31
--	----

Displaying related events	31
Displaying a Network Hop View related to a network view	32
Displaying network views related to a Network Hop View	33
Investigating events	33
Displaying related topology views	33
Investigating root cause	35
Investigating service-affected events	37
Retrieving related MIB information	38
View the structure of the network device related to an event	39
Investigating network connections	39
Showing device connectivity	39
Tracing the route to devices	40
Visualizing a network path	45
Pinging devices and subnets	49
Retrieving Cisco and Juniper route information	55
Setting up login credentials	59
Retrieving device information	60
Logging into a device	60
Querying domain registration information	60
Retrieving protocol information from Cisco and Juniper devices	63
Investigating the health of device components	70
Viewing the structure of a network device	71
Identifying faulty components from the Structure Browser tree	73
Identifying faulty components from the Structure Browser table	74
Searching the node text in the Structure Browser tree	76
Switching between tree and table mode in the Structure Browser	77
Showing events for a device or component	78
Customizing Structure Browser preferences	78
Showing device connectivity	79
Retrieving MIB information	80
About the SNMP MIB Browser	80
Accessing MIB data	81
Issuing an SNMP MIB query	82
Graphing MIB variables	84
About MIB graphing	84
Graphing MIBs	85

Chapter 5. Supporting problem resolution 89

Creating polls	89
Making devices available for maintenance	89
Unmanaging devices and components	89
Taking devices and components out of unmanaged state	91
Discovering devices again	94
The Add node tool	94
The Remove node tool	95

Chapter 6. Reporting on devices.	97
Running reports from the Reports window	97
Running reports from a network map	97
Appendix. Network Manager glossary	99

Notices	103
Trademarks	105
Index	107

About this publication

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 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 Systems Director.

The *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide* describes how to use Network Manager IP Edition to troubleshoot network problems.

Intended audience

This publication is intended for network operators who are responsible for identifying or resolving network problems using IBM Tivoli Network Manager IP Edition.

IBM Tivoli Network Manager IP Edition works in conjunction with IBM Tivoli Netcool/OMNIBus; this publication assumes that you understand how IBM Tivoli Netcool/OMNIBus works. For more information on IBM Tivoli Netcool/OMNIBus, see the publications described in “Publications” on page vi.

What this publication contains

This publication contains the following sections:

- Chapter 1, “About network troubleshooting,” on page 1
Describes the network troubleshooting tools available in Network Manager.
- Chapter 2, “Finding network devices,” on page 13
Describes how to search for a specific device using its IP address or host name, or browse for a device in the network views.
- Chapter 3, “Identifying network problems,” on page 23
Describes how to use Network Manager to identify network problems.
- Chapter 4, “Diagnosing network problems,” on page 31
Describes how to use the network troubleshooting tools available in Network Manager to diagnose problems with the network.
- Chapter 5, “Supporting problem resolution,” on page 89
Describes how to support network problem resolution.
- Chapter 6, “Reporting on devices,” on page 97
Describes how to run reports on network devices to check the health of devices, summarize network and device data, visualize Return On Investment and Green initiatives, and troubleshoot problems.

Publications

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

Your Network Manager library

The following documents are available in the Network Manager library:

- *IBM Tivoli Network Manager IP Edition Release Notes*, GI11-9354-00
Gives important and late-breaking information about IBM Tivoli Network Manager IP Edition. This publication is for deployers and administrators, and should be read first.
- *IBM Tivoli Network Manager Getting Started Guide*, GI11-9353-00
Describes how to set up IBM Tivoli Network Manager IP Edition after you have installed the product. This guide describes how to start the product, make sure it is running correctly, and discover the network. Getting a good network discovery is central to using Network Manager IP Edition successfully. This guide describes how to configure and monitor a first discovery, verify the results of the discovery, configure a production discovery, and how to keep the network topology up to date. Once you have an up-to-date network topology, this guide describes how to make the network topology available to Network Operators, and how to monitor the network. The essential tasks are covered in this short guide, with references to the more detailed, optional, or advanced tasks and reference material in the rest of the documentation set.
- *IBM Tivoli Network Manager IP Edition Product Overview*, GC27-2759-00
Gives an overview of IBM Tivoli Network Manager IP Edition. It describes the product architecture, components and functionality. This publication is for anyone interested in IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*, SC27-2760-00
Describes how to install IBM Tivoli Network Manager IP Edition. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Administration Guide*, SC27-2761-00
Describes administration tasks for IBM Tivoli Network Manager IP Edition, such as how to administer processes, query databases and start and stop the product. This publication is for administrators who are responsible for the maintenance and availability of IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Discovery Guide*, SC27-2762-00
Describes how to use IBM Tivoli Network Manager IP Edition to discover your network. This publication is for administrators who are responsible for configuring and running network discovery.
- *IBM Tivoli Network Manager IP Edition Event Management Guide*, SC27-2763-00
Describes how to use IBM Tivoli Network Manager IP Edition to poll network devices, to configure the enrichment of events from network devices, and to manage plug-ins to the Tivoli Netcool/OMNIBus Event Gateway, including configuration of the RCA plug-in for root-cause analysis purposes. This publication is for administrators who are responsible for configuring and running network polling, event enrichment, root-cause analysis, and Event Gateway plug-ins.

- *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide, GC27-2765-00*
Describes how to use IBM Tivoli Network Manager IP Edition to troubleshoot network problems identified by the product. This publication is for network operators who are responsible for identifying or resolving network problems.
- *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide, SC27-2764-00*
Describes how to configure the IBM Tivoli Network Manager IP Edition network visualization tools to give your network operators a customized working environment. This publication is for product administrators or team leaders who are responsible for facilitating the work of network operators.
- *IBM Tivoli Network Manager IP Edition Management Database Reference, SC27-2767-00*
Describes the schemas of the component databases in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the component databases directly.
- *IBM Tivoli Network Manager IP Edition Topology Database Reference, SC27-2766-00*
Describes the schemas of the database used for storing topology data in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the topology database directly.
- *IBM Tivoli Network Manager IP Edition Language Reference, SC27-2768-00*
Describes the system languages used by IBM Tivoli Network Manager IP Edition, such as the Stitcher language, and the Object Query Language. This publication is for advanced users who need to customize the operation of IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Perl API Guide, SC27-2769-00*
Describes the Perl modules that allow developers to write custom applications that interact with the IBM Tivoli Network Manager IP Edition. Examples of custom applications that developers can write include Polling and Discovery Agents. This publication is for advanced Perl developers who need to write such custom applications.
- *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide, SC27-2770-00*
Provides information about installing and using IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. This publication is for system administrators who install and use IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition to monitor and manage IBM Tivoli Network Manager IP Edition resources.

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, SC23-9680*
Includes installation and upgrade procedures for Tivoli Netcool/OMNIBus, 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, SC23-9683*
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, SC23-9681*

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, SC23-9684*
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 SC23-9682*
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 Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at:

<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp>

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 Tivoli publications online at the following Web site:

<http://www.elink.ibm.link.ibm.com/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 Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:
<http://www.elink.ibm.link.ibm.com/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

The following list includes the major accessibility features in Network Manager:

- The console-based installer supports keyboard-only operation.
- The console-based installer supports screen reader use.
- 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:
 - Web pages do not contain anything that flashes more than two times in any one second period.

The Network Manager Information Center, and its related publications, are accessibility-enabled. The accessibility features of the information center are described in Accessibility and keyboard shortcuts in the information center.

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 -**.

IBM® and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Tivoli® technical training

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

<http://www.ibm.com/software/tivoli/education>

Support information

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 <http://www.ibm.com/software/support/probsub.html> 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 <http://www.ibm.com/software/support/isa>

Conventions used in this publication

This publication uses several conventions for special terms and actions and operating system-dependent commands and paths.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations:**)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point* line)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This publication uses environment variables without platform-specific prefixes and suffixes, unless the command applies only to specific platforms. For example, the directory where the Network Manager core components are installed is represented as NCHOME.

When using the Windows command line, preface and suffix environment variables with the percentage sign %, and replace each forward slash (/) with a backslash (\) in directory paths. For example, on Windows systems, NCHOME is %NCHOME%.

On UNIX systems, preface environment variables with the dollar sign \$. For example, on UNIX, NCHOME is \$NCHOME.

The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to \$TMPDIR in UNIX environments. If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Chapter 1. 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 **Active Event List (AEL)**. The AEL provides lists of events on network devices and can be filtered to show events from selected devices only.

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.

About network views and the Network Hop View

There are two types of topology view: the Network Hop View and network views. Use these views to visualize the network and as a starting point for network troubleshooting.

Network Hop View

Use the Network Hop View 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 Hop Views 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.

Network views

Network Views show hierarchically organized views of a discovered network. Use the Network Views to view the results of a discovery and to troubleshoot network problems.

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 devices within the network view. Click on the icon to open an AEL 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 IP Edition 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.

Related tasks:

“Searching for a network view” on page 17

If you have many network views, you can search through the network view tree to find the view you want.

Network domains

A network domain is a collection of network entities to be discovered and managed. A single Network Manager IP Edition 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: Only alphanumeric characters and the underscore (_) character may be used for domain names. Any other characters, for example the hyphen (-) are forbidden.

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.

The following sections explain and illustrate the different views.

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 Layer 3 to show all routers and connections between them, or Layer 2 for data link connections.

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 table describes 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 1. Icons used in network maps









Icon	Name	Description
	Router icon	Represents a device that is designated as a router.
	Switch icon	Represents a device that is designated as a switch.
	End node icon	Represents end-node devices, including Windows, Linux, and Solaris workstations and printers.
	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.
	Subnet icon	Represents a subnet
	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.

Table 1. Icons used in network maps (continued)

Icon	Name	Description
[4]	Number of connections indicator	This indicates either of the following: <ul style="list-style-type: none"> 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.
	Completely unmanaged device	The entire device, including all its interfaces, is unmanaged.
	Partially unmanaged device	Only certain components of this device are unmanaged.

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 2. 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.

You might see only some of the default network views. 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 views 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. The network view nodes available by default in the network view tree are listed in the following table.

Table 3. Default network view nodes

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.
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 Routers	All devices with layer 3 connectivity, that is, all devices that Network Manager has classed as routers in the ncm.entityClass database table.
All Switches	All devices with layer 2 connectivity, that is, all devices that Network Manager has classed as switches in the ncm.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.

Table 3. Default network view nodes (continued)

Network view node	Description of devices contained in this network views node
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.
Global VLANs	All the Virtual Local Area Networks (VLANs) in the network domain.
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).
NAT Address Spaces	Devices grouped by membership of Network Address Translation (NAT) address spaces.
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.
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.
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.

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 **Active Event List (AEL)**. You can also view events in the Lightweight Event List (LEL) and in the Table View. From the **AEL**, 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 AEL, with a count value indicating how many times the event occurred.

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 4. Default event status icons











Default icon in the Network Views	Severity or meaning	Color in the Active Event List
	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 might be an error.	Not applicable
	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

Table 4. Default event status icons (continued)

Default icon in the Network Views	Severity or meaning	Color in the Active Event List
	This icon appears next to devices that contain unmanaged components.	Not applicable

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 portlet 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 portlet, for example, underneath the Hop View in a default installation.

Tree mode

In tree mode, the Structure Browser 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 **Active Event List (AEL)** 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 **Active Event List (AEL)** 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 portlet preferences or by clicking on the Hop View to load device information immediately. The first time the portlet 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” on page 76

You can search for a value within the nodes in the Structure Browser tree.

“Identifying faulty components from the Structure Browser tree” on page 73

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” on page 74

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 2. Finding network devices

Search for a specific device using its IP address or host name, or browse for a device in the network views.

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


Search for a seed device in the Network Hop View to display that device and those devices connected to it.

The Network Hop View 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.

Using the basic search

In the Network Hop View, use the basic search to find a device by IP address or device name.

1. Click **Network Availability > Network Hop View**.
2. Select a network domain from the **Domain** list.
3. Click **Search for Seed Device**  to specify the device to search for.
4. 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.

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 can also use the percent character (%) or the asterisk (*) as wildcards.

Device Name

Specify the name of the device. You can specify all of the name, or only the first part of the name. You can also use the percent character (%) or the asterisk (*) as wildcards. Device names are not case-sensitive. If you specify both an IP address and a device name, the IP address takes precedence.

5. Click **Find**. The **Results** list box displays the devices resulting from your search, as a listing of IP addresses or entity names.
6. 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.

Tip: If you know the entity ID of the device, you can also type it into the **Seed** field. Do not type device IP addresses or hostnames into the **Seed** field.

7. 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.
8. Specify how to display connectivity:

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 **Layer 3** to show all routers and connections between them, or **Layer 2** for data link connections.

PIM Shows all devices that belong to Protocol Independent Multicast (PIM) groups.

IPMRoute

Shows all devices that belong to Internet Protocol Multicast (IPM) routes.

9. Click **Apply Changes** . The topology you selected is displayed in the network map. Faulty devices are displayed with an associated event icon.

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.

To perform an advanced search for a device, complete the following steps:

1. Click **Network Availability > Network Hop View**.
2. Select a network domain from the **Domain** list.

3. Click **Search for Seed Device**  to specify the device to search for.
4. 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.

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.

5. Click **Find**. The **Results** list box displays the devices resulting from your search, as a listing of IP addresses or entity names.
6. 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.

Tip: If you know the entity ID of the device, you can also type it into the **Seed** field. Do not type device IP addresses or hostnames into the **Seed** field.

7. 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.
8. Specify how to display connectivity:

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 **Layer 3** to show all routers and connections between them, or **Layer 2** for data link 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.



9. Click **Apply Changes** . The topology you selected is displayed in the network map. Faulty devices are displayed with an associated event icon.

Browsing the network using the Network Views

Browse the network using network views in order to visualize the network based on geographical or other groupings. For example, you can browse subnets or device classes.

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.

1. Click **Availability > Network Availability > Network Views**.
2. In the **Network Views** tree on the left of the portlet, 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.

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.


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.


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.

To search for a particular network view name, complete the following steps.

1. From the Network Views, 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 front 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

Switch to tabular layout of your topology maps using the **Network Health View** and **Network Views**. Displaying topology maps in tabular layout enables filtering and sorting of topology data.

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 symmetrical 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 symmetrical or orthogonal.
- When switching between tabular layout and other layouts, device selection is not preserved.
- The tabular layout cannot be printed or saved as an image. To print the view, choose a different layout, such as symmetrical or orthogonal.

Switching to tabular layout

You can display topology maps using tabular layout.

In order to display a topology map using tabular layout, you must be in the **Network Health View** or **Network Views**.

Note: You cannot display a topology map in tabular layout using the Network Hop View.

1. Click **Availability > Network Availability > Network Health View** to open the **Network Health View** or **Availability > Network Availability > Network Views** to open the **Network Views**.
2. Navigate the Network View Tree to find a network view of interest.
3. 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.



Save

Saves the view or view container.

Filter Filter the contents of the table by entering a string in the **Filter** field and pressing the Return key.

For example, to find all rows that contain the string "snmp", type snmp. The search is case insensitive. For columns containing icons, such as the **Maximum Severity** column, the search string is compared against the tooltip value for the relevant cell. For example, if you enter a filter value of 3, then the filter returns any rows containing nodes that have an associated Minor severity, because the Minor severity icons has a tooltip that reads Severity 3.

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 regular expressions in the **Filter**.

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 symmetrical 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.

You can perform the following actions on the table that lists the network view nodes. Any settings made are valid for this session only.

Restriction: Sort operations performed on the IP Address field treat IPv6 addresses as bigger than IPv4 addresses. Within each IP version, the sorting is performed based on byte representations of the IP addresses.

Sort Column

Click the column header to sort that column in descending order. Click the column a second time to sort the column in ascending order. Further clicks toggle the column between descending and ascending order. The meaning of ascending and descending order varies according to the type of data in the column:

Alphabetical data

Ascending order orders the data from a to z. Descending order orders the data from z to a.

Numerical data

Ascending order orders the data from lowest to highest. Descending order orders the data from highest to lowest.

Icon Ascending order orders the icons from the highest to lowest value associated with the icon. Descending order orders the icons from the lowest to highest value associated with the icon. The values associated with each icon are listed below.

Resize a column

Click and drag the vertical line separator to the right of the column heading.

Move a column

Click a column header and drag it to the right or the left of adjacent columns.

The table that lists the network view nodes contains that the following columns.

Display Name

Human-readable name to be displayed adjacent to this entity in a topology map and in the Network Views tabular layout.

IP Address

The IP address through which this entity was discovered and will be monitored.

Class Name

The name of a class of devices.

Class Type

The type of device or type of class.

Managed State

Takes one of the following values:

- **Managed:** if the row represents a device container, such as Cisco, then all devices in the container are in managed status. If the row represents a device then the device is in managed status.
- **Unmanaged.** if the row represents a device container, such as Cisco, then all devices in the container are in unmanaged status. If the row represents a device then the device is in unmanaged status.
- **Partially Managed:** if the row represents a device container, such as Cisco, then one or more, but not all, of the devices in the container is in unmanaged status. If the row represents a device, then one or more components in the device is in unmanaged status.

Maximum Severity

Displays an event status icon showing the severity of the device or the maximum severity of all devices if the row represents a device container, such as Cisco.

Note: If there are more than 2,000 devices in a single network view, then no event status information is displayed in the table.

Filtering devices in tabular layout

You can filter devices in a tabular layout of the topology map. For example, if you enter a search string of 3, the table might display rows containing devices with IP addresses such as 172.3.102.10 and with class names like 3Com.

This task assumes that you are already in the **Network Health View** or **Network Views** and that you are displaying a topology map in tabular layout.

1. In the **Filter** field, type a filter string and press Enter. Here are some examples of filter strings:

- To display all devices that have associated Critical events , type **critical**.

Note: By default, the **Maximum Severity** column displays an icon related to the severity. A tooltip associated with the icon displays the severity string associated with the icon. Use the text displayed in the icon tooltip to filter on the **Maximum Severity** value.

- To display all Cisco devices, type **cisco**. This shows all devices where the **Class Name** column contains the string "Cisco".

The **Filter** field does not support wildcard characters such as *. It also does not support regular expressions. If the table is refreshed, for example due to an update in **Maximum Severity** of one or more devices displayed in the table, then the filter you specified is reapplied before the filtered table is displayed.

2. To remove the filter, empty the **Filter** field and press Enter.

Chapter 3. Identifying network problems

You can identify network problems in two ways: using network views or using event lists.

Identifying problems using network views

Use network views to view the results of a discovery or to troubleshoot network problems.

Before you can work with network views the administrator must complete the following tasks:

- The first network discovery must have successfully completed.
- The administrator must configure network views for you, either by dynamically generating network views or by creating custom network views.

You can use different types of network view to monitor different types of devices or device technologies.

1. Click **Network Availability > Network Views**.
2. In the **Network Views** tree on the left of the portlet, 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” on page 31

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.

Using the Network Health View

Use the Network Health View to display events on a device.

1. Click **Availability > Network Availability > Network Health View**. The **Network Health View** page appears with the Network Views portlet above and the **Active Event List (AEL)** portlet below.

Note: When you first open the **Network Health View** page, the **AEL** portlet displays all events in the ObjectServer.

2. Display a network view of interest in the Network Views portlet.
3. Select a single device in the network map. The contents of the **AEL** portlet are filtered to display only the events that occurred on the selected device.

Restriction: The contents of the **AEL** portlet are not filtered in the following cases:

- Multiple devices are selected in the Network Views portlet.

- 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 AEL displays all events in the ObjectServer.

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.

To monitor subnets using the Network Views, proceed as follows:

1. Click **Availability > Network Availability > Network Views**.
2. In the navigation tree on the left of the portlet, 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.

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” on page 32

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.

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.

1. Click **Availability > Network Availability > Network Views**.
2. In the navigation tree on the left of the portlet, 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.

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” on page 31

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.

Your administrator can configure the display of the links as either colored, or colored with an associated severity icon. By default, link status is on.

The display of link status can be customized for each individual view.

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.
4. Right-click a link to open the right-click menu.

From the right-click menu, you can do any of the following tasks:

- Display the link events in the AEL. If you change the severity status of an event in the AEL, 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.

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.

To monitor BGP networks, proceed as follows.

1. Click **Availability > Network Availability > Network Views**.
2. In the navigation tree on the left of the portlet, 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” on page 64

Retrieve Border Gateway Protocol (BGP) information from devices in order to 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.

To monitor OSPF routing domains and OSPF areas, proceed as follows.

1. Click **Availability > Network Availability > Network Views**.
2. In the navigation tree on the left of the portlet, 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” on page 69

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.

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.

1. Click **Availability > Network Availability > Network Views**.
 - In the navigation tree on the left of the portlet, 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 portlet, 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 portlet, 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.

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.

1. Click **Availability > Network Availability > Network Views**.
2. In the navigation tree on the left of the portlet, 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.

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.

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.

1. Click **Availability > Network Availability > Network Views**.
2. In the navigation tree on the left of the portlet, 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.

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.

To monitor all network events, proceed as follows.

1. Click **Availability > Network Availability > Fault-Finding View**. The **Fault-Finding View** page appears with the **Active Event List (AEL)** portlet above and the Network Hop View portlet below.

Note: When you first open the **Fault-Finding View** page, the AEL portlet displays all events in the ObjectServer and the Network Hop View portlet is empty.

2. Select an event of interest in the AEL, or right-click an event and then click **Broadcast Topology Context**. The Network Hop View portlet now displays the network topology related to the selected event.

Restriction: Results vary if you select multiple events in the AEL.

- If all the selected events occurred on the same network device, then the Network Hop View portlet only displays the network topology related to that device.

- If the selected events occurred on different devices, then the Network Hop View portlet does not display any network topology .

Related tasks:

“Investigating events” on page 33

Use features of the **Active Event List (AEL)** to support network troubleshooting. You can use the AEL to show affected network devices, identify root-cause events, and identify events that have a major service impact.

Chapter 4. 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.

Related tasks:

“Investigating network connections” on page 39

Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

“Retrieving device information” on page 60

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” on page 70

Investigate the health of device components in order to isolate the fault within a network device.

“Retrieving MIB information” on page 80

Retrieve MIB variable information from network devices to diagnose network problems.

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.

To display events on a device:

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 **AEL** opens in a separate browser window containing the events on the selected device.

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” on page 33

Use features of the **Active Event List (AEL)** to support network troubleshooting. You can use the **AEL** 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.

To display events on devices in a subnet:

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 **AEL** appears in a separate browser window containing the events on the selected subnet.

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" on page 33

Use features of the **Active Event List (AEL)** to support network troubleshooting. You can use the **AEL** 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.

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 **AEL** 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.

To switch from a network view to a Network Hop View.

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.

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.

To switch from the Network Hop View to the Network Views:

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 **Active Event List (AEL)** to support network troubleshooting. You can use the **AEL** to show affected network devices, identify root-cause events, and identify events that have a major service impact.

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. An unmanaged device is usually marked Unmanaged because it is undergoing maintenance and may therefore generate unnecessary network events. Network Manager can filter out unmanaged events from the **AEL** in the following ways:

- Filtering out the unmanaged events so that they do not appear at all in the **AEL**.
- Configuring the **AEL** to display the NmosManagedStatus field. This field displays the value 1 (Operator unmanaged) or 2 (System unmanaged).

Check with your network administrator on how the system is configured to handle the presentation of unmanaged events in the **AEL**.

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 display a related Network Hop View, ensure that the event to investigate is selected in the **Active Event List (AEL)**.

To display the Network Hop View related to an event:

1. From an **AEL** 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.

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” on page 39

Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

“Retrieving device information” on page 60

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” on page 80

Retrieve MIB variable information from network devices to diagnose network problems.

“Investigating the health of device components” on page 70

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).

1. Select an event in the **Active Event List (AEL)**.
2. In the **AEL** 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.

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” on page 39

Investigate network connections, trace routes, and create paths in order to check connectivity within your network.

“Retrieving device information” on page 60

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” on page 80

Retrieve MIB variable information from network devices to diagnose network problems.

“Investigating the health of device components” on page 70

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.

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 **Active Event List (AEL)** to display this field.

For information on root-cause scenarios and examples, see the *IBM Tivoli Network Manager IP Edition Event Management 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 **Active Event List (AEL)** as symptom events. The system marks the non-symptom events as root cause events.

Root cause events are differentiated from symptom events in the **AEL** 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 **AEL**, 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 **AEL** showing all the events for that device.

Identifying root cause events

A single network problem may generate multiple events. You can use the **Active Event List (AEL)** to identify the root-cause event.

Before you issue the command to identify the root-cause event, ensure that at least one event is selected in the **AEL**.

To identify root-cause events:

1. From an **AEL** window, right-click an event and click **Show Root Cause**. An **AEL** opens in a separate browser window containing the root-cause event.
2. Use the features in the **AEL** to further investigate this event.

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” on page 33

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” on page 38

As part of network troubleshooting activity, you can retrieve MIB information for the device associated with a specified event in the **Active Event List (AEL)**.

“View the structure of the network device related to an event” on page 39

As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Active Event List (AEL)**.

Investigating symptom events

Starting from a root-cause event you can use the **Active Event List (AEL)** to identify the symptom events.

Before you issue the command to identify the symptom events, ensure that at least one event is selected in the **AEL**.

1. From an **AEL** window, right-click an event and click **Show Symptoms**. An **AEL** opens in a separate browser window containing symptom events.
2. Use the features in the **AEL** to further investigate these events.

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” on page 33

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” on page 38

As part of network troubleshooting activity, you can retrieve MIB information for the device associated with a specified event in the **Active Event List (AEL)**.

“View the structure of the network device related to an event” on page 39

As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Active Event List (AEL)**.

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 **Active Event List (AEL)** to quickly identify network service-affecting events.

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 **AEL**. The **Summary** field contains text indicating that the event is an SAE.

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 **AEL** 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.

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.

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” on page 38

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 identifying the contributing events, first identify the relevant SAE.

To identify contributing events:

1. From an **Active Event List (AEL)** window, right-click an SAE and click **Show SAE Related Events**. An AEL opens in a separate browser window containing the events that contributed to the SAE.
2. Use the features in the AEL to further investigate these events.
3. Optional: To identify contributing services, click **Show SAE Related Services**.

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” on page 33

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 **Active Event List (AEL)**.

“View the structure of the network device related to an event” on page 39

As part of network troubleshooting activity, you can view the structure of a device associated with a specified event in the **Active Event List (AEL)**.

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 **Active Event List (AEL)**.

To retrieve MIB information related to an event:

1. Select an event in the AEL.
2. From an AEL 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” on page 82

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 **Active Event List (AEL)**.

Before you issue the command to drill into the affected device, ensure that the event to investigate is selected in the Active Event List.

1. Select an event in the **AEL**.
2. From an **AEL** 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” on page 73

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.

1. From the Network Hop View or Network Views 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 IP Edition server, or perform a remote traceroute from any Cisco or Juniper network

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.

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 IP Edition to check network paths.

To perform this procedure, you must be in the Network Views or in the Network Hop View.

1. From the Network Hop View or Network Views network map, 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.

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.

Restriction: Network Manager servers running on Windows can only specify a limited number of traceroute parameters. In the steps below, the parameters that are available on UNIX only and are not available on Windows are marked with a UNIX flag.

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.

UNIX

Send

Specify the number of packets at each hop. The default value is 3.

UNIX

Packet Size

Specify the size in bytes of each packet to send to the specified targets. The default value is 40.

UNIX

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.

UNIX

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.

UNIX

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.

UNIX

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.

UNIX

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.

UNIX

Use: Parallel Probing

Specify whether or tool should use parallel probing to increase the speed of the traceroute. This option is selected by default.

UNIX**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.

UNIX**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.

The following topics describe how to perform remote traceroute operations.

Related tasks:

“Setting up login credentials” on page 59

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.

If you want to automatically login into Cisco or Juniper devices, you must first configure login credentials.

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.

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.
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.

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.
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 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.

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 `$ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file and changing the values for the following view attributes:

- `topoviz.pathview.accesslevel`
- `topoviz.pathview.accessid`

1. Click **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', 'itmadmin', 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 IPv4 Network Path window, where you can create a new path view.

Note: IP path views only.

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 IPv4 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.

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.

Save as Image 

Saves the view or view 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 an overview of the current view on a new page.

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 symmetrical 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.

Note: If the path was not successfully traced, then you get a path trace error, indicating the reason that the path could not be traced. Path trace errors include the following:

- 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.
- Input parameters specified in the Trace an IPv4 Path window are invalid.
- An IP address in the path did not respond to ping verification.
- Time to trace the path exceeds one of the path trace timeouts.
- A communication error occurred while the path trace was trying to communicate with the Topology manager, ncp_model, or with the NCIM topology database.

Possible reasons for these errors include the following:

- SNMP access for at least one of the devices along the path has not been correctly configured.
- This device does not make the necessary SNMP MIB routing information available.
- This device is not running an SNMP agent.
- Path trace timeouts are too short.

You can take one or more of the following actions to resolve these errors:

- Click **View Path Trace Details** for detailed log information on the error.
- Check, and 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.
- Increase the length of the path trace timeouts.
- Correct the parameters specified in the Trace an IPv4 Path window and retrace the path.
- Check that the Topology manager, ncp_model, is running and that the NCIM topology database is accessible.

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 IP Edition server, or remote ping from any Cisco or Juniper network device.

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.

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.

The following topics describe how to ping devices and subnets from the Network Manager Server.

Pinging devices:

Ping one or more devices in the network map from the Network Manager IP Edition server to check connectivity to that device.

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.

It is also possible to perform a custom ping by customizing the ping settings.

Related tasks:

“Performing a custom device ping” on page 50

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.

Restriction: Network Manager servers running on Windows can only specify a limited number of ping parameters. In the steps below, the parameters that are available on UNIX only and are not available on Windows are marked with a UNIX flag.

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.

UNIX

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.

UNIX

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.

UNIX

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): UNIX

Ping one or more subnets in the network map from the Network Manager server to check connectivity to that subnet.

Restriction: This task is only available if your Network Manager server is running on UNIX.

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.

The following topics describe how to perform remote ping operations.

Related tasks:

“Setting up login credentials” on page 59

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.

If you want to automatically login into Cisco or Juniper devices, you must first configure login credentials.

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.

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.
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.

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.
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.

The following topics describe how to retrieve routing information from Cisco and Juniper devices.

Related tasks:

“Setting up login credentials” on page 59

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.

If you want to automatically log into Cisco or Juniper devices, you must first configure login credentials.

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.

If you want to automatically login into Cisco or Juniper devices, you must first configure login credentials.

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.

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.
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.

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:

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.

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” on page 52

Perform remote ping operations from Cisco and Juniper devices to troubleshoot device availability and latency issues.

“Performing remote traceroute operations” on page 42

Perform remote traceroute operations from Cisco and Juniper devices to troubleshoot device availability and latency issues.

“Retrieving Cisco and Juniper route information” on page 55

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.

The following topics describe how to retrieve device information.

Logging into a device

Use Telnet to log into a network device to troubleshoot a device. This command is not available on Windows 2008 and Windows Vista operating systems.

Restriction: This command is not available on Windows 2008 and Windows Vista operating systems. This is because the Telnet client is not installed by default on those operating systems.

1. From the Network Hop View or Network Views network map, select the device to log into. To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and choose **Telnet**. This launches a command prompt, issues a Telnet command to the local machine and displays the progress of the Telnet login in the command prompt.

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.

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.

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.

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,

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.

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.

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.

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.

By default, this operation retrieves DNS address (A) records only.

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.

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.

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.

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.

You can only launch this command on Cisco and Juniper devices.

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.

- 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 to troubleshoot BGP-related network issues.

You can only launch this command on Cisco and Juniper devices.

- From the Network Hop View or Network Views network map, select the device to query. To select multiple devices, press Ctrl.
- 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...

- 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.

You can only launch this command on Cisco and Juniper devices.

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.

To perform this procedure, you must be in the Network Views or in the Network Hop View.

You can only launch this command on Cisco devices.

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.

To perform this procedure, you must be in the Network Views or in the Network Hop View.

You can only launch this command on Cisco and Juniper devices.

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...
Juniper	Choose the menu option WebTools > Juniper Tools...> Information Tools...> View MPLS Information...

The Cisco or Juniper Information Tool window appears.

- 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.

- 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.

You can only launch this command on Cisco and Juniper devices.

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.

You can only launch this command on Cisco and Juniper devices.

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.

Investigating the health of device components

Investigate the health of device components in order to isolate the fault within a network device.

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.

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.

When you launch the Network Hop View, the Structure Browser opens in a portlet below the Network Hop View. The Structure Browser opens in either tree or table mode, depending how it has been configured.

1. Click **Availability > Network Availability > Hop View**. The Network Hop View page appears with the Network Hop View portlet above and the Structure Browser portlet below.

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 IP Edition Network Visualization Setup 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” on page 78

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” on page 77

If the Structure Browser is displayed as a portlet, you can choose to display the Structure Browser in tree mode or table mode.

“Identifying faulty components from the Structure Browser tree” on page 73

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” on page 74

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” on page 76

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.

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 portlet.

Opening the Structure Browser from the event list

Launch the Structure Browser from an **Active Event List (AEL)** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

To perform this procedure, you must be in the **Active Event List (AEL)**.

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 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.

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" on page 78

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" on page 74

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" on page 77

If the Structure Browser is displayed as a portlet, you can choose to display the Structure Browser in tree mode or table mode.

"Searching the node text in the Structure Browser tree" on page 76

You can search for a value within the nodes in the Structure Browser tree.

"Identifying faulty components from the Structure Browser tree" on page 73

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" on page 78

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.

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 portlet, it can be configured to display in either tree mode or table mode.

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 AEL 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 Hop View

Starts the Network Hop View in a separate window and displays the network topology, with the device containing the selected component highlighted.

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.

Rediscover Nodes

Rediscover one or more devices including the currently-selected device.

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.

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.

Related concepts:

“About the Structure Browser” on page 9

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” on page 71

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” on page 77

If the Structure Browser is displayed as a portlet, you can choose to display the Structure Browser in tree mode or table mode.

“Searching the node text in the Structure Browser tree” on page 76

You can search for a value within the nodes in the Structure Browser tree.

“Showing events for a device or component” on page 78

Show events for a device or component from within the Structure Browser to isolate the fault within a network device.

“Creating polls” on page 89

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.

“Discovering devices again” on page 94

You can discover a particular device or set of devices again if you think that they have changed, and you do not want to wait for the next full discovery.

“Retrieving MIB information” on page 80

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.

The Structure Browser has two modes: tree and table. When the Structure Browser is displayed as a portlet, it can be configured to display in either tree mode or table mode. Complete these steps in table mode.



1. Select the faulty entity in the Hop View.
2. In the Structure Browser table below the Hop View portlet, 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.

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 **AEL** 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 Hop View

Starts the Network Hop View in a separate window and displays the network topology, with the device containing the selected component highlighted.

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.

Rediscover Nodes

Rediscovered one or more devices including the currently-selected device.

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.

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.

Related concepts:

“About the Structure Browser” on page 9

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” on page 71

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” on page 72

Launch the Structure Browser from an **Active Event List (AEL)** 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.

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:

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” on page 9

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” on page 71

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” on page 72

Launch the Structure Browser from an **Active Event List (AEL)** 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” on page 73


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 portlet, you can choose to display the Structure Browser in tree mode or table mode.

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 portlet, for example, underneath the Hop View in a default installation.

To change the display mode of a Structure Browser portlet, complete the following steps.

1. From the Structure Browser portlet, 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” on page 71

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” on page 72

Launch the Structure Browser from an **Active Event List (AEL)** 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” on page 73

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.

1. Open the Structure Browser in either tree or table mode.
2. Select a faulty device or component.
3. Click **Tools > Show Events**.

An AEL appears in a separate browser window containing the events on the selected device or component.

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.

The configuration files are located in the ITNMHOME/profiles/TIPProfile/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.

1. From the command line, navigate to the ITNMHOME/profiles/TIPProfile/etc/tnm directory.
2. Back up and edit the ITNMHOME/profiles/TIPProfile/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 portlet. The default mode determines how data is displayed when the Structure Browser is opened as a portlet. The two options are tree or table. The default mode can be overridden by a user's portlet preferences. Note: The Structure Browser table is only available when the Structure Browser is opened as a portlet. 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.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.table.connectivity.width. localColumnName	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.

Structure Browser property	Description
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.tree.image.x	Specifies the managed status icon to display in the tree and the table.

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 ITNMHOME/profiles/TIPProfile/etc/tnm/structurebrowser.properties file from the ITNMHOME/profiles/TIPProfile/etc/tnm/default/structurebrowser.properties file.

3. Save and close the file.
4. Back up and edit the ITNMHOME/profiles/TIPProfile/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” on page 71
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” on page 72
Launch the Structure Browser from an **Active Event List (AEL)** in order to view the internal structure of the device associated with the event and investigate the health of the device components.

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.

1. From the Network Hop View or Network Views 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.

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.

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.

1. Click **Availability > 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” on page 82

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.

To perform this procedure, you must be in the **Active Event List (AEL)**.

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.

You can now issue an SNMP MIB query for this device.

Related tasks:

“Issuing an SNMP MIB query” on page 82

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.

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.

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.

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 portlet. The table mode is shown underneath the Hop View in a default installation. The table is only available from a portlet.

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.

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.

To perform this procedure, you must be in the SNMP MIB Browser.

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 **AEL**, 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. 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.
5. 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 5. 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

Table 5. *SNMP Queries Available from the SNMP MIB Browser (continued)*

SNMP Query	Description	Node	Example
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.

About MIB graphing

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.

For MIB graphing to display information for a device, that device needs to have been discovered and information on that device needs to be contained within the NCIM database. The SNMP MIB Graph portlet can be invoked from the following views:

Network Availability

Click **SNMP MIB Graph**.

MIB Browser

Select an OID, and request to graph the variable. Displays the MIB graph using the specified host and OID, with default values for the remaining configuration parameters.

Active Event List

Select an event, and launch the MIB graph from the context menu.

Any network view displaying a resource

Select a device, and launch the MIB graph from the context menu.

Note: When SNMP MIB Graph is launched in context from another interface, it is displayed in a separate browser window. In addition, it will attempt to display stored historical data for the selected device. You can change this by editing the default MIB Graph settings.

Graphing MIBs

Use the SNMP MIB Graphs window to graph a MIB variable for fault analysis and resolution of network problems.

You can launch the MIB Graph Properties window from several locations.

If launched from the Active Event List, Topology, structure browser or Dashboard views, the MIB Graph Properties window receives only the hostname of the resource to be polled. If it is launched from the MIB Browser, then an OID is also passed in.

The MIB Graph Properties window ensures that the OID to graph is a valid value; for example, not a text field.

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.

You first define graph properties, before expanding the Preferences area to define your display preferences.

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 AEL, 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.

A MIB graph must be configured before you can view it. .

You can view MIB graphs in the SNMP MIB Graph portlet 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.

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.

Period Allows changing graph from real time to a specific historical period.

Start date

Changes the start of the historical period by date and time.

Apply Applies changes to period and start date.

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 5. Supporting problem resolution

Support problem resolution by helping network engineers work on devices.

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.

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.

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.

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.

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.

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.

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.

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 portlet. The table mode is shown underneath the Hop View in a default installation. The table is only available from a portlet.

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**.



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.

If the device or its components was updated during the resolution of the problem, rediscover the device to refresh the device information in the network topology.

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 Active Event List, 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.

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 6. *UnmanageNode.pl* command-line options

Command-line option	Description
-domain <i>DomainName</i>	Mandatory; the name of the domain where the node to be unmanaged resides.
-user <i>username</i>	Mandatory; the name of the NCIM database user.
-pwd <i>password</i>	Mandatory; the password for the NCIM database user.
-file <i>FileName</i>	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 <i>host</i> 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.

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.

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.

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.

Related tasks:


“Discovering devices again” on page 94

You can discover a particular device or set of devices again if you think that they have changed, and you do not want to wait for the next full discovery.

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.

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 portlet. The table mode is shown underneath the Hop View in a default installation. The table is only available from a portlet.

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**.

The components are now managed and the wrench icons are removed. Polling and event correlation resumes for these components.

If the device or its components was updated during the resolution of the problem, rediscover the device to refresh the device information in the network topology.

Related tasks:

“Discovering devices again” on page 94

You can discover a particular device or set of devices again if you think that they have changed, and you do not want to wait for the next full discovery.

The Manage node tool

Use the **ManageNode.p1** 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 7. *ManageNode.pl* command-line options

Command-line options	Description
-domain <i>DomainName</i>	Mandatory; the name of the domain where the unmanaged node resides.
-user <i>username</i>	Mandatory; the name of the database user.
-pwd <i>password</i>	Mandatory; the password for the database user.
-file <i>FileName</i>	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 <i>host</i> below.
-verbose	Optional; provides more information on the screen.
<i>host</i>	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
```

Discovering devices again

You can discover a particular device or set of devices again if you think that they have changed, and you do not want to wait for the next full discovery.

Discovering a device can take several hours. Before issuing this command, ensure that discovery has been correctly configured by the network administrator.

1. In the Network Hop View or Network Views network map select the device to discover again. To select multiple devices, press Ctrl.
2. Right-click one of the selected devices and click **Rediscover Node(s)**.
3. In the Partial Discovery window make any desired changes to the partial discovery settings.
4. Optional: Add extra seeds and scope zones.

Restriction: Change discovery settings only if you are a network administrator and you are familiar with the network.

5. Click **Go** to launch the discovery.

The Add node tool

Use the **AddNode.pl** command to add network devices to your network topology by using the command-line interface. When you add a device, a partial discovery is triggered to add the device to the network topology.

Full topology connectivity is not displayed for the device until after the next full discovery is completed.

Usage

This command is located in NCHOME/precision/bin.

UNIX Before running this script, ensure that you have set up the UNIX environment.

The following syntax shows how the **AddNode.pl** command works:

```
ncp_perl AddNode.pl -domain DomainName -latency MessageLatency -debug  
DebugLevel -file FileName -verbose host
```

The following table describes the command-line options for **AddNode.pl**.

Table 8. AddNode.pl command-line options

Command-line options	Description
-domain <i>DomainName</i>	Mandatory; the name of the domain you want to add the node to.
-latency <i>MessageLatency</i>	Optional; the maximum time in milliseconds to wait between attempts to send a message. This is needed for busy networks.
-debug <i>DebugLevel</i>	Optional; the level of detail the debugging output provides. Values are 1 to 4, where 4 represents the most detailed output.

Table 8. *AddNode.pl* command-line options (continued)

Command-line options	Description
<code>-file FileName</code>	Optional; file containing the list of nodes to be added to the network topology. 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 <i>host</i> below.
<code>-verbose</code>	Optional; provides more information on the screen.
<i>host</i>	Optional; the name of the node to be added. 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 host name. If you do not provide a host name, then the <code>-file</code> option must be used.

Examples

The following examples show how to use the **AddNode.pl** command.

```
./ncp_perl AddNode.pl -domain NCOMS -file mynodes.txt
./ncp_perl AddNode.pl -domain ABCD -verbose 192.168.0.6 neptune.ibm.com
```

The Remove node tool

Use the **RemoveNode.pl** tool to remove devices from your network topology by using the command-line interface.

The **RemoveNode.pl** command sets the device to unmanaged state and marks the device to be removed during the next full discovery. This is useful when you have removed a device from the network, and you want to remove it from your network topology as soon as possible, instead of waiting for 3 full discovery cycles. The tool marks the nodes and all associated objects for deletion. The next full discovery removes the nodes and all objects from the databases.

Usage

This command is located in `NCHOME/precision/bin`.

UNIX Before running this script, ensure that you have set up the UNIX environment.

The following syntax shows how the **RemoveNode.pl** command works.

Note: The node must also be removed manually from any Discovery File Finder seed files.

```
ncp_perl RemoveNode.pl -domain DomainName -latency MessageLatency -debug
DebugLevel -user username -pwd password -file FileName -verbose -force host
```

The following table describes the command-line options for **RemoveNode.pl**.

Table 9. RemoveNode.pl command-line options

Command-line options	Description
-domain <i>DomainName</i>	Mandatory; the name of the domain you want to add the node to.
-latency <i>MessageLatency</i>	Optional; the maximum time in milliseconds to wait between attempts to send a message. This is needed for busy networks.
-debug <i>DebugLevel</i>	Optional; the level of detail the debugging output provides. Values are 1 to 4, where 4 represents the most detailed output.
-user <i>username</i>	Mandatory; the name of the database user.
-pwd <i>password</i>	Mandatory; the password for the database user.
-file <i>FileName</i>	Optional; file containing the list of nodes to be removed from the network topology. 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 <i>host</i> below.
-verbose	Optional; provides more information on the screen.
-force	Optional; when used, you are not prompted to confirm the removing of a node.
<i>host</i>	Optional; the name of the node to be removed. 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 **RemoveNode.pl** command.

```
./ncp_perl RemoveNode.pl -domain NCOMS -user root -pwd fruit -file
mynodes.txt
```

```
./ncp_perl RemoveNode.pl -domain ABCD -user root -pwd fruit -verbose
neptune.ibm.com 192.168.0.6
```

Chapter 6. Reporting on devices

You can run reports on network devices to check the health of devices, summarize network and device data, or troubleshoot problems.

Access to reports and report groups is controlled by the administrator. Your administrator can also create and customize reports.

As a network operator, you can run reports from the GUI in several ways.

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.

To run a report, complete the following steps.

1. Log in to the Tivoli Integrated Portal and click **Reporting > Common Reporting > Network Manager**.
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.

To run a report from a network map, complete the following steps.

1. Log in to the Tivoli Integrated Portal and navigate to a Network View, Hop View, Path View, 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.

Appendix. Network Manager glossary

Use this information to understand terminology relevant to the Network Manager product.

The following list provides explanations for Network Manager terminology.

AOC files

Files used by the Active Object Class manager, `ncp_class` to classify network devices following a discovery. Device classification is defined in AOC files by using a set of filters on the object ID and other device MIB parameters.

active object class (AOC)

An element in the predefined hierarchical topology of network devices used by the Active Object Class manager, `ncp_class`, to classify discovered devices following a discovery.

agent See, discovery agent.

class hierarchy

Predefined hierarchical topology of network devices used by the Active Object Class manager, `ncp_class`, to classify discovered devices following a discovery.

configuration files

Each Network Manager process has one or more configuration files used to control process behaviour by setting values in the process databases. Configuration files can also be made domain-specific.

discovery agent

Piece of code that runs during a discovery and retrieves detailed information from discovered devices.

Discovery Configuration GUI

GUI used to configure discovery parameters.

Discovery engine (`ncp_disco`)

Network Manager process that performs network discovery.

discovery phase

A network discovery is divided into four phases: Interrogating devices, Resolving addresses, Downloading connections, and Correlating connectivity.

discovery seed

One or more devices from which the discovery starts.

discovery scope

The boundaries of a discovery, expressed as one or more subnets and netmasks.

Discovery Status GUI

GUI used to launch and monitor a running discovery.

discovery stitcher

Piece of code used during the discovery process. There are various discovery stitchers, and they can be grouped into two types: data collection stitchers, which transfer data between databases during the data collection

phases of a discovery, and data processing stitchers, which build the network topology during the data processing phase.

domain

See, network domain.

entity

A topology database concept. All devices and device components discovered by Network Manager are entities. Also device collections such as VPNs and VLANs, as well as pieces of topology that form a complex connection, are entities.

event enrichment

The process of adding topology information to the event.

Event Gateway (ncp_g_event)

Network Manager process that performs event enrichment.

Event Gateway stitcher

Stitchers that perform topology lookup as part of the event enrichment process.

failover

In your Network Manager environment, a failover architecture can be used to configure your system for high availability, minimizing the impact of computer or network failure.

Failover plug-in

Receives Network Manager health check events from the Event Gateway and passes these events to the Virtual Domain process, which decides whether or not to initiate failover based on the event.

Fault Finding View

Composite GUI view consisting of an **Active Event List (AEL)** portlet above and a Network Hop View portlet below. Use the Fault Finding View to monitor network events.

full discovery

A discovery run with a large scope, intended to discover all of the network devices that you want to manage. Full discoveries are usually just called discoveries, unless they are being contrasted with partial discoveries. See also, partial discovery.

message broker

Component that manages communication between Network Manager processes. The message broker used by Network Manager is called Really Small Message Broker. To ensure correct operation of Network Manager, Really Small Message Broker must be running at all times.

NCIM database

Relational database that stores topology data, as well as administrative data such as data associated with poll policies and definitions, and performance data from devices.

ncp_disco

See, Discovery engine.

ncp_g_event

See, Event Gateway.

ncp_model

See, Topology manager.

nep_poller

See, Polling engine.

network domain

A collection of network entities to be discovered and managed. A single Network Manager installation can manage multiple network domains.

Network Health View

Composite GUI view consisting of a Network Views portlet above and an **Active Event List (AEL)** portlet below. Use the Network Health View to display events on network devices.

Network Hop View

Network visualization GUI. Use the Network Hop View 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. Formerly known as the Hop View.

Network Polling GUI

Administrator GUI. Enables definition of poll policies and poll definitions.

Network Views

Network visualization GUI that shows hierarchically organized views of a discovered network. Use the Network Views to view the results of a discovery and to troubleshoot network problems.

OQL databases

Network Manager processes store configuration, management and operational information in OQL databases.

OQL language

Version of the Structured Query Language (SQL) that has been designed for use in Network Manager. Network Manager processes create and interact with their databases using OQL.

partial discovery

A subsequent rediscovery of a section of the previously discovered network. The section of the network is usually defined using a discovery scope consisting of either an address range, a single device, or a group of devices. A partial discovery relies on the results of the last full discovery, and can only be run if the Discovery engine, `nep_disco`, has not been stopped since the last full discovery. See also, full discovery.

Path Views

Network visualization GUI that displays 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.

performance data

Performance data can be gathered using performance reports. These reports allow you to view any historical performance data that has been collected by the monitoring system for diagnostic purposes.

Polling engine (nep_poller)

Network Manager process that polls target devices and interfaces. The Polling engine also collects performance data from polled devices.

poll definition

Defines how to poll a network device or interface and further filter the target devices or interfaces.

poll policy

Defines which devices to poll. Also defines other attributes of a poll such as poll frequency.

Probe for Tivoli Netcool/OMNIBus (nco_p_ncpmonitor)

Acquires and processes the events that are generated by Network Manager polls and processes, and forwards these events to the ObjectServer.

RCA plug-in

Based on data in the event and based on the discovered topology, attempts to identify events that are caused by or cause other events using rules coded in RCA stitchers.

RCA stitcher

Stitchers that process a trigger event as it passes through the RCA plug-in.

root-cause analysis (RCA)

The process of determining the root cause of one or more device alerts.

SNMP MIB Browser

GUI that retrieves MIB variable information from network devices to support diagnosis of network problems.

SNMP MIB Grapher

GUI that displays a real-time graph of MIB variables for a device and uses the graph for fault analysis and resolution of network problems.

stitcher

Code used in the following processes: discovery, event enrichment, and root-cause analysis. See also, discovery stitcher, Event Gateway stitcher, and RCA stitcher.

Structure Browser

GUI that enables you to investigate the health of device components in order to isolate faults within a network device.

Topology Manager (ncp_model)

Stores the topology data following a discovery and sends the topology data to the NCIM topology database where it can be queried using SQL.

WebTools

Specialized data retrieval tools that retrieve data from network devices and can be launched from the network visualization GUIs, Network Views and Network Hop View, or by specifying a URL in a web browser.

Notices

This information applies to the PDF documentation set for IBM Tivoli Network Manager IP Edition 3.9.

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 10 are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Table 10. IBM trademarks

AIX	iSeries	RDN
ClearQuest	Lotus	SecureWay
Cognos	Netcool	solidDB
Current	NetView	System z
DB2	Notes	Tivoli
developerWorks	OMEGAMON	WebSphere
Enterprise Storage Server	PowerVM	z/OS
IBM	PR/SM	z/VM
Informix	pSeries	zSeries

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.

Index

A

- accessibility ix
- add node tool 94
- AddNode.pl 94
- Advanced Ping Tool 49
- alerts
 - see events 7

B

- BGP
 - monitoring BGP networks 26
 - retrieving information 64
- browsing
 - the network 16

C

- Cisco devices
 - finding in Hop View 17
 - finding in Network Views 17
- Cisco Information Tool
 - running 63, 64, 65, 66, 67, 69, 70
- Cisco route information
 - retrieving 55
- components
 - faulty 70, 73, 74
 - unmanaging 90
 - visualizing 72
- connectivity
 - about 3
 - IP Subnets 3
 - Layer 2 3
 - Layer 3 4
 - showing 39, 79
- conventions, typeface x
- creating
 - polls from Network Hop View or Network Views 89
- custom DNS lookup
 - issuing 62
- custom Internet registry database query
 - issuing 61
- Customizing Structure Browser 78

D

- default network view nodes 6
- device
 - icons 4
 - related events 31
 - related to event 39
- device components
 - changing to managed state 92
- device connectivity
 - showing 39, 79
- device structure
 - visualizing 72

- devices
 - browsing the network 16
 - connectivity 3
 - custom ping 50
 - discovering again 94
 - faulty components 70, 73, 74
 - finding 13
 - logging into 60
 - monitoring 24
 - performing traceroute to 40
 - pinging 49
 - searching for 13
 - seed 1
 - showing connectivity 39, 79
 - taking out of unmanaged state 91
 - unmanaged 33
 - unmanaging 89
 - viewing device structure 71
 - visualizing components 72
 - visualizing in tabular layout 18
- devices with high-speed interfaces
 - finding in Hop View 17
 - finding in Network Views 17
- discovery
 - starting from the Hop View 94
 - starting from the Network Views 94
- displaying
 - events on device 31
 - events on subnet 32
 - network hop view related to event 33
 - network hop view related to network view 32
 - network views related to event 34
 - network views related to network hop view 33
- DNS lookups
 - about 62
 - custom 62
 - issuing 62
- domains
 - see network domains 3

E

- education
 - see Tivoli technical training ix
- environment variables, notation x
- event correlation 35
- event lists
 - launching SNMP MIB Browser 81
 - launching Structure Browser 72
 - using to identify network problems 28
- event status icons 8
- events
 - about 7
 - contributing to SAEs 38
 - investigating 33
 - on a device 31
 - on a subnet 32

- events (*continued*)
 - related network hop view 33
 - related network views 34
 - root-cause 36
 - service-affected 37
 - symptom 35, 36
 - unmanaged 33

F

- fault analysis
 - graphing MIBs 85
- finding
 - devices in Hop View 17
 - devices in Network Views 17
- finding devices
 - methods for 13

G

- glossary 99
- graphing MIBs 84
 - for fault analysis 85
 - for resolution of network problems 85

H

- Hop View
 - about 1, 13
 - finding devices 17
 - launching SNMP MIB Browser 81

I

- icons
 - event status 8
 - for devices 4
- identifying
 - faulty components 70, 73, 74
 - network problems 23
 - network problems using event lists 28
 - network problems using network views 23
 - root-cause events 36
 - SAEs 37
 - symptom events 36
- interface administrative status 63
- interface operational status 63
- Internet registry database query
 - issuing 60
- investigating
 - events 33
 - network routes 39
 - SAEs 37
- IP Subnets connectivity 3
- ISIS information
 - retrieving 65

- issuing
 - custom DNS lookup 62
 - custom Internet registry database query 61
 - DNS lookups 62
 - Internet registry database query 60

J

- Juniper Information Tool
 - running 63, 64, 65, 66, 67, 69, 70
- Juniper route information
 - retrieving 57

L

- launching
 - SNMP MIB Browser from event list 81
 - SNMP MIB Browser from Hop View 81
 - SNMP MIB Browser from Network Views 81
 - SNMP MIB Browser from Structure Browser 82
 - Structure Browser from event 72
- Layer 2 connectivity 3
- Layer 3 connectivity 4
- logging into
 - devices 60
- login credentials
 - setting up 59

M

- mainNodeDetails table 13
- maintenance mode
 - see unmanaged state 89
- managed state 89
- management information base
 - see MIB 82
- ManageNode.pl 92
- manuals vi
- MBGP information
 - retrieving 66
- MIB Browser
 - see SNMP MIB Browser 80, 81
- MIB graph
 - working with the MIB graph 86
- MIB Graph Properties window 85
- MIB graphing
 - about 84
- MIB tree
 - ifDescr column object 83
 - ifRouteTable table 83
 - ifTable table 83
 - interfaces branch node 83
 - sysDescr scalar object 83
 - sysLocation scalar object 83
 - system branch node 83
 - sysUpTime scalar object 83
- MIBs
 - about 80, 83
 - graphing 84

- MIBs (*continued*)
 - graphing with the Graph Properties window
 - for fault analysis 85
 - for resolution of network problems 85
 - navigating 82
 - retrieving data 82
- monitoring
 - BGP networks 26
 - devices 24
- MPLS
 - TE
 - monitoring tunnels 28
- MPLS information
 - retrieving 67
- multicast
 - monitoring groups 27
 - monitoring routes 27

N

- navigating
 - MIBs 82
- NCOMS 2, 3
- network
 - browsing 16
 - network domains 2, 3
 - network hop view
 - related to event 33
 - related to network view 32
 - Network Manager glossary 99
 - network maps
 - finding devices in 16
 - network problems
 - diagnosing 31
 - identifying 23
 - identifying using event lists 28
 - identifying using network views 23
 - troubleshooting 31
 - network routes
 - investigating 39
 - network view nodes
 - default 6
 - network views
 - displaying events on 32
 - related to event 34
 - related to network hop view 33
 - searching 17
 - using to identify network problems 23
 - visualizing in tabular layout 18
- Network Views 2
 - about 16
 - finding devices 17
 - launching SNMP MIB Browser 81
- nodes
 - network view tree 6

O

- object identifier (OID) 82
- online publications vi
- ordering publications vi
- OSPF information
 - retrieving 69

P

- pinging
 - devices 49
 - from local client 49
 - from Network Manager server 49
 - remote 52
 - subnets 51
- pivot device
 - see seed device 1
- polls
 - creation from Network Hop View or Network Views 89
- Portlet views
 - Structure Browser 78
- publications vi

R

- remote ping
 - about 52
 - from Cisco devices 52
 - from Juniper devices 52
 - within label-switched path (LSP) 53
 - within virtual private network (VPN) 54
- remote traceroute
 - about 42
 - from Cisco devices 42
 - from Juniper devices 42
 - within label-switched path (LSP) 43
 - within virtual private network (VPN) 44
- remove node tool 90, 92, 95
- RemoveNode.pl 95
- reports
 - running 97
- resolving network problems
 - graphing MIBs 84, 85
- retrieving
 - BGP information 64
 - Cisco route information 55
 - interface administrative and operational status 63
 - ISIS information 65
 - Juniper route information 57
 - MBGP information 66
 - MIB data 82
 - MIB information 80
 - MPLS information 67
 - OSPF information 69
 - route information 55
 - VPLS information 70
 - VRF route information 58
- root-cause analysis 35
- root-cause events
 - identifying 36
- route information
 - about 55
 - retrieving 55
- router icon 4

S

- SAEs
 - contributing events 38
 - identifying 37

- SAEs (*continued*)
 - investigating 37
- searching
 - for devices 13
 - node text in Structure Browser 76
- seed device 1, 13
- service-affected events
 - see SAEs 38
- setting up
 - login credentials 59
- Show events
 - Structure Browser 78
- showing
 - device connectivity 39, 79
- SNMP MIB Browser
 - about 80
 - launching 81
 - launching from event list 81
 - launching from Hop View 81
 - launching from Network Views 81
 - launching from Structure Browser 82
 - queries 83
 - using 82
- SNMP queries
 - Get Next query 83
 - Get query 83
 - Get Table query 83
 - Walk query 83
- Structure Browser 72
 - about 9, 71
 - customizing 78
 - launching from event list 72
 - launching SNMP MIB Browser 82
 - searching node text 76
 - Show events 78
- subnet
 - related events 32
- subnet icon 4
- subnets
 - pinging 51
- support information x
- switch icon 4
- symptom events 35
 - identifying 36

T

- table view 18
- tabular layout 18
- Telnet login credentials 59
- Tivoli software information center vi
- Tivoli technical training ix
- tools
 - AddNode.pl 94
 - ManageNode.pl 92
 - RemoveNode.pl 95
 - topology management 90, 92, 94, 95
 - UnmanageNode.pl 90
- topology management tools
 - add node 94
 - remove node 90, 92, 95
- topology maps
 - visualizing in tabular layout 18
- traceroute
 - about 40
 - custom 40
 - from server 40

- traceroute (*continued*)
 - remote 42
 - to devices 40
- training, Tivoli technical ix
- troubleshooting
 - network 1
 - network problems 31
- typeface conventions x

U

- unmanaged devices 33
- unmanaged events 33
- unmanaged state 89
- UnmanageNode.pl 90
- unmanaging
 - components 90
 - devices 89
- using
 - SNMP MIB Browser 82

V

- variables, notation for x
- viewing
 - components 73, 74
 - device structure 71
 - structure of device related to event 39
- visualizing
 - device components 72
 - device structure 72
- VPLS information
 - retrieving 70
- VRF route information
 - retrieving 58

W

- WebTools
 - multiple login details 59



Printed in the Republic of Ireland

GC27-2765-02

