Copyright Notice

Copyright © 2001 by Tivoli Systems, an IBM Company, including this documentation and all software. All rights reserved. May only be used pursuant to a Tivoli Systems Software License Agreement or Addendum for Tivoli Products to IBM Customer or License Agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of Tivoli Systems. Tivoli Systems grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the Tivoli Systems copyright notice. No other rights under copyright are granted without prior written permission of Tivoli Systems. The document is not intended for production and is furnished “as is” without warranty of any kind. All warranties on this document are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Note to U.S. Government Users–Documentation related to restricted rights–Use, duplication, or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corporation.

Trademarks

The following product names are trademarks of Tivoli Systems or IBM Corporation: IBM, NetView, and, Tivoli.

Java and Hot Java are trademarks of Sun Microsystems, Inc.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Notice

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to Tivoli Systems’ or IBM’s valid intellectual property or other legally protectable right, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user.

Tivoli Systems or IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to: IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York, 10504-1785, USA.
## Contents

### Preface

Who Should Read This Guide .......................................................... vii
Prerequisite and Related Documents .............................................. vii
What This Guide Contains .............................................................. vii
Typeface Conventions ...................................................................... vii
Terminology ..................................................................................... viii
Online Information .......................................................................... viii
Accessibility Information ................................................................. viii
  Keyboard Access ........................................................................... viii
Contacting Tivoli Support ............................................................... viii

### Chapter 1. Introducing the Web Console

Before You Begin .............................................................................. 1
Getting Started ................................................................................ 1
  Defining Users .............................................................................. 2
  Web Server ................................................................................... 2
  Starting the Web Console ............................................................. 2
  Logging On to the Web Console .................................................... 2
Using the Web Console Desktop ....................................................... 2
  Using Menus ................................................................................ 3
  Using Toolbars ............................................................................ 7
  Accessing Online Information .................................................... 8
  Working with Tables .................................................................... 8
  Understanding the Web Server Communication Status Lights ....... 9
Learning about Objects ................................................................... 9
  Understanding Object Properties ................................................ 10
  Understanding Capability Fields ................................................ 10
  Managing and Unmanaging Objects ............................................ 10
  Acknowledging and Unacknowledging Objects ......................... 10

### Chapter 2. Using Submap Explorer

Understanding the Submap Explorer ................................................. 11
  Submap Explorer Menu Bar .......................................................... 11
  Submap Explorer Tool Bar ........................................................... 12
  Submap Explorer Toolbar Drop-down Lists .................................. 13
  Learning about Symbols ................................................................ 14
  Understanding Maps and Submaps ............................................... 17
Using the Zoom Function ................................................................. 18
Using the Find Function ................................................................. 18
  Using Wild Cards ....................................................................... 19
Understanding Context ................................................................... 19
Using Filters .................................................................................. 20

### Chapter 3. Working with MIBs

Understanding MIBs ....................................................................... 21
  MIBs Supported by the Tivoli NetView Program ......................... 21
  MIB Naming Conventions ........................................................... 22
Using the Web Console MIB Browser (SNMP V1/V2) ....................... 23
  Read and Write Community Names ............................................ 23
  SNMP Version .............................................................................. 23
  SNMP Walk ............................................................................... 24
  Real-time Graph ........................................................................ 24
  Setting MIB Variable Values ....................................................... 24
Index ........................................ 53
Preface

This document provides a foundation for understanding and operating the Tivoli® NetView Web Console. This product is referred to as the Web Console in this document.

This document explains the functions of the Web Console and how to use the Web Console to monitor a network.

Who Should Read This Guide

This document is intended for network operators and administrators.

Prerequisite and Related Documents

The following is a list of Tivoli NetView for Windows® related publications:
Tivoli NetView for Windows User’s Guide
Tivoli NetView for UNIX User’s Guide

What This Guide Contains

This book contains the following information:

- “Chapter 1. Introducing the Web Console” on page 1
  Provides information about starting the Web Console and using the Web Console desktop.
- “Chapter 2. Using Submap Explorer” on page 11
  Provides information about using the Submap Explorer.
- “Chapter 3. Working with MIBs” on page 21
  Provides information about MIBs.
- “Chapter 4. Monitoring Network Configuration” on page 27
  Provides information about a network’s configuration.
- “Chapter 5. Diagnosing Network Problems” on page 33
  Provides information about diagnosing network problems.
- “Chapter 6. Working with Events and Event Filters” on page 43
  Provides information about using the Event Browser.
- “Chapter 7. Configuration and Security” on page 47
  Provides administration and configuration information for system administrators.

Typeface Conventions

This guide uses several typeface conventions for special terms and actions. These conventions have the following meaning:

Bold
Lowercase and mixed-case commands, command options, and flags that appear within text appear like this, in bold type.

Graphical user interface elements (except for titles of windows and dialogs) and names of keys also appear like this, in bold type.

Italic
Variables, values you must provide, new terms, and words and phrases that are emphasized appear like this, in italic type.
Monospace  Commands, command options, and flags that appear on a separate line, code examples, output, and message text appear like this, in monospace type.

Names of files and directories, text strings you must type, when they appear within text, names of Java methods and classes, and HTML and XML tags also appear like this, in monospace type.

---

**Terminology**

For a list of Tivoli NetView terms and definitions, refer to:  

**User**  Means either an operator or administrator. For tasks that must be performed by a user that has an administrator or SuperUser role defined, the term *administrator* is used. For example, all of the tasks described in [Chapter 7. Configuration and Security on page 47](#) must be performed by an administrator.

**NetView**  Means either Tivoli NetView for UNIX or Tivoli NetView for Windows.

---

**Online Information**

Online help is not available for the Web Console.

The Release Notes and online books are available in HTML and PDF versions. Click Help → Books On-line to access the Release Notes and library.

In addition, you can access online documents at this Web address:  
http://www.tivoli.com/support/

A user name and password are required.

---

**Accessibility Information**

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in this product enable users to:

- Operate specific or equivalent features using only the keyboard.
- Keyboard Navigation of the User Interface.

**Keyboard Access**

Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

---

**Contacting Tivoli Support**

If you have a problem with any Tivoli product, you can contact Tivoli Customer Support. See the *Tivoli Customer Support Handbook* at the following Web address:

http://www.tivoli.com/support/handbook/

The handbook provides information about how to contact Tivoli Customer Support, depending on the severity of your problem, and the following information:
• Registration and eligibility
• Telephone numbers and e-mail addresses, depending on the country you are in
• What information you should gather before contacting support
Chapter 1. Introducing the Web Console

The Tivoli NetView Web Console provides a flexible, customizable environment for users that need access to network status and configuration information.

The Web Console provides a dynamic web interface that enables you to:

- View maps and events
- Run network diagnostic tools
- Work with management information base (MIB) objects

See the following for more information about the tasks you can perform using the Web Console:

- "Chapter 1. Introducing the Web Console"
- "Chapter 2. Using Submap Explorer" on page 11
- "Chapter 3. Working with MIBs" on page 21
- "Chapter 4. Monitoring Network Configuration" on page 27
- "Chapter 5. Diagnosing Network Problems" on page 33
- "Chapter 6. Working with Events and Event Filters" on page 43
- "Chapter 7. Configuration and Security" on page 47

Before You Begin

The term user is used to mean either an operator or administrator. See "Terminology" on page viii for more information.

Note that all of the Web Console functions and views are described in this book. However, the following can be restricted depending on the role and scope specified for your user ID:

View
Some views or objects in views might not be displayed.

Function
Some functions might not be enabled.

Event Browser
Some events might not be displayed.

This chapter provides the following information:

- "Getting Started"
- "Using the Web Console Desktop" on page 2
- "Learning about Objects" on page 9

Getting Started

This section describes the tasks that must be performed before you can use the Web Console:

- Define users using the Web Console security function
- Start the optional netviewd daemon. Refer to the Release Notes for more information.
- Start the Web Console
- Log on to the Web Console
Defining Users

Users must be defined before they can log on to the Web Console. The following information defines a user:
- User ID
- Password
- Role
- Scope

See "Web Console Security" on page 47 for more information.

Web Server

The Web Console communicates with the Web Server. See "Configuration and Security" on page 47 for information about configuring and starting the Web Server.

Starting the Web Console

Use one of the following methods to start the Web Console:

Table 1. Web Console Start Methods.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Start Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>Enter <a href="http://hostname:8080/netview/NetViewApplet">http://hostname:8080/netview/NetViewApplet</a></td>
</tr>
<tr>
<td>Windows server</td>
<td>Click Start + Programs + Tivoli NetView + NetView Web Console</td>
</tr>
<tr>
<td>Windows client</td>
<td>Click Start + Programs + Tivoli NetView Web Console + NetView Web Console</td>
</tr>
<tr>
<td>Windows command line</td>
<td>Enter \usr\ov\bin\nvwc.bat hostname</td>
</tr>
<tr>
<td>UNIX® server</td>
<td>Enter /usr/OV/bin/nvwc.sh hostname</td>
</tr>
<tr>
<td>UNIX client</td>
<td>Enter /usr/OV/bin/nvwebclient</td>
</tr>
</tbody>
</table>

Logging On to the Web Console

Use the following procedure to log on to the Web Console:
- Enter your user ID and password.
- Enter the host name of the Web Server that you want to connect to.
- Enter the port number of the Web Server that you want to connect to. The default is 8080.
- Click OK.

The NetView welcome screen is displayed. If you do not want the welcome screen displayed again, select the Do not show this again check box.

Using the Web Console Desktop

The Web Console desktop is displayed when you have successfully logged on to NetView.

The Web Console can display multiple windows, but you can interact with only one window at a time. The window you interact with is known as the active window.
Windows are identified by title bars located at the top of the window border. Menu choices are listed in menu bars located under the title bar.

The Web Console uses standard window-handling features. For example, you can change the size and location of a Web Console window on your screen.

The Tivoli NetView program displays a logical representation of your network through dynamic topology maps that contain hierarchies of submaps. The submaps include graphical representations of your network at several levels. These levels include root, internet, network, segment, and node. To access submaps that are lower in the map hierarchy, you double-click on symbols that explode into lower submaps.

### Using Menus

Tivoli NetView tasks can be started from menu bar, context menus, or toolbars. Each Tivoli NetView application and user-added application selected from menu bar items runs in its own separate window.

Menus contain items that enable you to access and perform the operations of the Tivoli NetView program. If a menu item is unavailable, that choice is disabled because one of the following conditions exists:

- An object is not selected.
- The selected objects have capabilities that are incompatible with the menu item.
- The number of items selected is not within a range of minimum and maximum number of selections set for that menu item.

### Using the Desktop Menu Bar

The desktop menu bar provides menus for accessing and controlling network management functions and tools.

The following menus and associated submenus provide context-sensitive functions:

- **Object**
- **Monitor**
- **Test**

See "[Understanding Context](#)" on page 13 for more information.

**Notes:**

1. Not all menu selections are available for all objects.
2. The information that is provided about an object depends on:
   - The type of the object, for example, information that is displayed for a node is different from the information provided for a router.
   - The function that the objects support, for example, if an object is not running SNMP, you can perform functions that are available from the Test menu, but you cannot perform any of the SNMP-related diagnostics like those available from the Monitor menu.

The following desktop menu descriptions are provided:

- "[File Menu](#)" on page 4
- "[Object Menu](#)" on page 4
- "[Monitor Menu](#)" on page 5
- "[Test Menu](#)" on page 6
- "[Tools Menu](#)" on page 6
File Menu: The File menu provides the following functions:

Open
Select Open to open a Submap Explorer window.

Close
Select Close to close the active window.

Exit
Select Exit to stop the Web Console.

Object Menu: The Object menu provides the following functions:

Manage
Select Manage to change an unmanaged object to managed. See "Managing and Unmanaging Objects" on page 10 for more information.

Unmanage
Select Unmanage to change a managed object to unmanaged. See "Acknowledging and Unacknowledging Objects" on page 10 for more information.

Acknowledge
Select Acknowledge to stop the Tivoli NetView program from continuously notifying you of a known problem.

Unacknowledge
Select Unacknowledge to start or resume monitoring by the Tivoli NetView program.

Object Properties
Select Object Properties to display information about objects. The following information is provided:

Category
Information Provided

General
- Object name
- Vendor
- SNMP Agent
- SNMP Supported
- SNMP Proxied
- IP Address
- Alias
- Subnet Mask
- Physical Address (LLA)
- Interface Type
- Hostname
- IP Status
- Description
- Interface Speed
- True IP Address
- ISDN Backup
- HSRP
- MPLS
- SNMP Address
- Location
- Object ID
- Contact

Events
- Time
- Severity
- Description

**Other**
- Interface
- Status
- IP Address
- Network Mask
- Link Address
- Interface Type

**MIB Browser**
Select **MIB Browser** to display MIB information for an object. See "Understanding MIBs" on page 21 for more information.

**Home Page**
Select **Home Page** to view the home web page of the selected node.

**Management Page**

**Monitor Menu:** The Monitor menu provides the following functions:

**Network**
Select **Network** to monitor the following:
- Address
- Interfaces
- Routing Table
- ARP Cache
- IP Services
- TCP Connections

**System**
Select **System** to monitor the following:
- General
- CPUs
- Processes
- Memory
- Printers
- Devices
- Storage
- Partitions
- File Systems

**LAN Manager**
Select **LAN Manager** to monitor the following:
- Shared Files
- Server Statistics
- Workstation Statistics
- Services
- Printer Queues

**Other**
Select **Other** to monitor the following:
- Interfaces
- System

**MPLS**
Select **MPLS** to monitor the following:
- MPLS Node View
- MPLS Interface View

**Switch Management**
Select **Switch Management** to monitor the following:
- Port View
• Switch Status
• MAC View
• Inactive Ports

**Test Menu:** The Test menu provides the following functions:

**Connectivity**
- Select **Connectivity** to test TCP/IP and SNMP protocols.

**Ping**
- Select **Ping** to test the number of packets sent and lost, and to verify connectivity at the IP level.

**Demand Poll**
- Select **Demand Poll** to query the values of `ifAdminStatus` and `ifOperStatus` for each interface of a node.

**Locate Route**
- Select **Locate Route** to locate specific IP routes between two selected nodes.

**QuickTest**
- Select **QuickTest** to poll all managed interfaces and determine the complete status of the node.

**QuickTest Critical**
- Select **QuickTest Critical** to poll interfaces that are currently marked as down.

**Tools Menu:** The Tools menu provides the following functions:

**Diagnostics**
- Select **Diagnostics** to open a Diagnostics window. The following menu items are available for use with the specified object:
  - **Test** All test menu choices are available.
  - **Network**
    - All Monitor → Network menu choices are available.
  - **System**
    - All Monitor → Other menu choices are available.

**Object Properties**
- Select **Object Properties** to display the object properties for the specified object. See “[Object Menu](#)” on page 4 for a list of properties that are provided.

**Note:** Not all menu selections are available for all objects.

**Event Browser**
- Select **Event Browser** to start the Event Browser function.

**MIB Browser**
- Select **MIB Browser** to start the MIB Browser function.

**Server Status**
- Select **Server Status** to query the status of the daemons on the NetView server. The following information is provided for each daemon:
  - Daemon Name
  - Behavior
  - State
  - Last Message
  - Exit Status

**Window Menu:** Select **Window** to work with open windows. The following options are available:
- Cascade
- Tile Horizontally
- Tile Vertically
Context Menus

Context menus are pop-up menus that are provided for performing operations on individual objects and submaps. The context menus provide a subset of operations that are available from the menu bar.

Context menus are available for Submap Explorer and the Event Browser.

**Submap Explorer:** To access the Submap Explorer context menus, right-click the object.

The following context menu options are available:

- Open
- Manage
- Unmanage
- Acknowledge
- Unacknowledge
- Object Properties
- Management Page
- Ping
- Show in

**Event Browser:** The Event Browser enables you to display event details. To display the event details, right-click the event and then click Details.

The following information is provided:

- Time
- Node
- Enterprise
- Generic
- Specific
- Severity
- Category
- Source
- Description

Using Toolbars

Toolbars provide shortcuts to menu items for commonly used commands. The toolbars provide convenient access to applications and tools you regularly use. For example, from the toolbar, you can open a new application, check SNMP and interface traffic, and print the contents of a particular window.

Each icon in the Tivoli NetView toolbars represents a menu item, an available tool, an application, or a status. These tools and applications allow you to perform tasks on selected objects in a submap or on all the information in a submap. Click on an icon to perform an action or to start that tool or application. If an icon is unavailable, it cannot be selected.

The Tivoli NetView program provides the Submap Explorer toolbar and the Status Filter toolbar.
Submap Explorer Toolbar
The Submap Explorer toolbar icons represent a menu item or function. See "Submap Explorer Tool Bar" on page 12 for more information.

Status Filter Toolbar
The Status Filter toolbar displays or hides the nodes in the submap based on their status. For example, click on the Unknown Status icon to hide all nodes with unknown status.

Accessing Online Information
To access the Web Console User’s Guide, click Help → Books On-line from the main menu.

Working with Tables
The Tivoli NetView program displays information in tables. For example, the Event Browser and all views except the Topology View are presented in table format.

Using Table Filters
Use the filter function to reduce or refine the list of objects that is displayed in tables. For example, use filters with table views or with the Event Browser.

Use the following procedure to create a filter:
• Click the right-arrow button.
• Click Show Filter Row.
• Click the filter row under the field that you want to filter. An Edit Filter - Description dialogue box is displayed.
• Enter the filter text.
• Click the down-arrow on the Contains button and select either Contains or Starts with.
• Select the Match case check box if you want the filter to be case sensitive.
• Click OK. The filter is automatically applied.

Table Usage Notes
• To sort the information in a table, click the up arrow to sort the data in that column in ascending order. Click the down- arrow to sort the data in descending order. Once the information has been sorted, only the chosen arrow is displayed.
• To resize a column, move the mouse cursor over the column head separators. When the mouse cursor changes, drag the cursor to the left or right to widen or narrow the column.
• To rearrange the order of the columns, click the heading of the column that you want to move and drag it to the position you want drop it. The columns are automatically rearranged.
• When a filter is created, a box is created below each table column heading. A line is drawn in the box under the column that is being sorted, indicating that the column is being filtered. To suspend a filter, click the line. The line is broken and the filter is temporarily suspended. To apply the filter again, click the broken line.
• To clear a filter, use the procedure for creating a filter, but clear the text field. The filter is removed when you click OK. To clear all filters, click the right- arrow button and click Clear All Filters.
• The row at the bottom of the table lists the following:
  • The total number of items
  • The number of items displayed
  • The number of items selected
Note: The difference between the total number of items and the total number displayed is the number of items being filtered.

Understanding the Web Server Communication Status Lights

The Web Console communication status lights provide a visual indication of the communication status between the Web Console and Web Server. There are two lights: a green light on the left and a red light on the right. The lights have the following meaning:

<table>
<thead>
<tr>
<th>Light</th>
<th>Communication Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady green</td>
<td>The communication path is ready. No communication is occurring.</td>
</tr>
<tr>
<td>Blinking green</td>
<td>Communication between the Web Console and Web Server is occurring.</td>
</tr>
<tr>
<td>Steady red</td>
<td>The communication path is not ready (disconnected).</td>
</tr>
<tr>
<td>Blinking red</td>
<td>The Web Console is trying to reconnect.</td>
</tr>
</tbody>
</table>

Web Server Communication Status Light Usage Notes

- The light blinks only when meaningful events are returned. Blinking is suppressed for event-related polling activity made by the Submap Explorer and Event Browser, to limit unnecessary blinking.
- After communication is lost, the red light blinks every time it attempts to reestablish communications with the Web Server. If the attempt is unsuccessful, it waits 5 seconds before it makes another attempt. Each attempt takes between 5 and 60 seconds. If the red light blinks every 5 seconds, it means that the Web Console is reaching the web server, but it cannot connect to the port that is specified. If the red light blinks every 60 seconds, it means that you cannot connect to the Web Server host, which means there is a network problem.
- When communication is lost and then reestablished, the Web Console determines if the Web Server has been stopped and restarted. If it has been stopped and restarted, a dialogue is displayed to indicate that you must restart the Web Console. Note that closing the dialog stops the Web Console. If the Web Server has not been stopped and restarted, you can continue working with the current Web Console.
- If the Web Console has not communicated with the Web Server for one hour, a dialogue is displayed to indicate that you must restart the Web Console. Note that closing the dialog stops the Web Console. See "Customizing the Web Console Inactive Interval" on page 52 for the procedure to change the interval.

Learning about Objects

An object is an internal representation of a logical or physical entity or resource that exists somewhere in a computer network. An object is made up of a set of fields that specify all the properties of the object. Examples of resources represented by objects include:

- A computer node
- A software process on a computer
- An IP network
Understanding Object Properties

The properties of each object are contained in fields that make up the object. Each field contains information about the object, such as:

- The object name
- The object IP address
- Whether the object supports SNMP
- The type of hardware the object represents
- The status of the object

The entries in these fields define the object and are called object properties. You can display object properties using one of the following methods:

- Click the object in a submap and then click **Object** → **Object Properties**.
- Click the object in a submap and then click **Tools** → **Object Properties** and then click **Get Object from Map**.
- Click **Tools** → **Object Properties** and then type the object name and click **Refresh**.

Understanding Capability Fields

An important type of object property is the *capability field*. A capability field is a Boolean field, which can take the values True and False, and indicates whether the object has a certain characteristic or capability. Capability fields are displayed as boxes. A box with a check mark indicates that the object supports that capability.

Capability fields govern the actions that you can take when working with an object. When you select an object from a submap, the capability fields of that object help determine which menu options are enabled.

Managing and Unmanaging Objects

An object can be managed or unmanaged by clicking an object and then clicking **Object** → **Manage** or **Object** → **Unmanage**. A managed object is monitored by the Tivoli NetView program for topology, status, and configuration changes. The symbol for a managed object reports status change by changing to the color that represents the status.

If an object is not being managed, the symbol for the object does not report the status because it is not known.

Acknowledging and Unacknowledging Objects

If you know that an object has stopped functioning, but you do not want the Tivoli NetView program to notify you continuously about this problem, you can acknowledge it. Acknowledge and unacknowledge an object by clicking an object and then clicking **Object** → **Acknowledge** or **Object** → **Unacknowledge**.

When you acknowledge the object, the object changes to the color set for acknowledged symbols and remains in the acknowledged state until you either select the object and unacknowledge it or until the status of the node changes. Unacknowledging an object causes the Tivoli NetView program to resume normal processing for that object.
Chapter 2. Using Submap Explorer

Use Submap Explorer to work with submaps. The submap window provides a graphical representation of a portion of your network.

This chapter provides the following information:
- “Understanding the Submap Explorer”
- “Using the Zoom Function” on page 18
- “Using the Find Function” on page 18
- “Understanding Context” on page 19
- “Using Filters” on page 20

Understanding the Submap Explorer

To open a Submap Explorer window, click File → Open. A map is opened and the root submap for the map is displayed.

The title of the first window is Submap Explorer. The title of the each additional window is Submap Explorer followed by a number. For example, the title of the second Submap Explorer window that is opened is Submap Explorer 2. More than one Submap Explorer window can be displayed at a time, but only one can be active at a time.

The left side of a Submap Explorer window is a tree view of the submap and is used to navigate the submap hierarchy. Each submap is represented by its parent object. Double-clicking an object or clicking the ▶ symbol next to an object expands it to display the next level. Then, an object at the next level can be expanded and so on. In this way, the entire hierarchy can be navigated. Double-clicking or clicking the – symbol collapses an expanded object. Selecting an object displays the contents of its submap in the right-hand side of the Submap Explorer. The context menus are available for objects in the list or tree view by right clicking the object.

The right side of a Submap Explorer window is a view displaying the contents of the submap selected in the tree view. The view that is displayed is controlled by the view drop-down list on the tool bar. See View Drop-down List on page 13 for more information.

Use the toolbar to work with views. See Submap Explorer Tool Bar on page 12 for more information.

The width of each column can be resized by dragging the column separators. The list can be sorted by the contents of a column by clicking on the column header.

Submap Explorer Menu Bar

The Submap Explorer menu bar provides menus for working with submaps. Note that menu selections with icons beside them indicate sections that are available from the Submap Explorer toolbar.

The following submap menu descriptions are provided:
- [Table 2 on page 12]
- [Table 3 on page 12]
Note: Not all selections are available for all views.

Table 2. File Menu

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td>Closes the Submap Explorer Window</td>
</tr>
</tbody>
</table>

Table 3. Edit Menu

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide Selected</td>
<td>Hides all selected objects</td>
</tr>
<tr>
<td>Hide Unselected</td>
<td>Hides all unselected objects</td>
</tr>
<tr>
<td>Select All</td>
<td>Selects all objects that are currently displayed.</td>
</tr>
<tr>
<td>Deselect All</td>
<td>Deselects all objects that are displayed</td>
</tr>
<tr>
<td>Invert Selection</td>
<td>Changes all selected objects to unselected and changes unselected objects to selected.</td>
</tr>
<tr>
<td>Find</td>
<td>Displays the Find function row. See &quot;Using the Find Function&quot; on page 18 for more information.</td>
</tr>
</tbody>
</table>

Table 4. Submap Menu

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Opens the child submap</td>
</tr>
<tr>
<td>Refresh Data</td>
<td>Refreshes the data displayed for the selected object.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Rearranges the displayed nodes by the attribute selected.</td>
</tr>
</tbody>
</table>

Table 5. View Menu

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent</td>
<td>Displays the parent submap.</td>
</tr>
<tr>
<td>Icon size</td>
<td>Changes the icon size from small to large and vice versa.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Starts the zoom function. See &quot;Using the Zoom Function&quot; on page 18 for more information.</td>
</tr>
</tbody>
</table>

Submap Explorer Tool Bar

The toolbar is comprised of drop-down lists and icons. See "Submap Explorer Toolbar Drop-down Lists" on page 13 for more information.

Pause the pointer over the icons to display the name of the function that the icon provides. Table 6 provides a description of the icons.

Table 6. Toolbar Icons

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>Starts the Find function. See &quot;Using the Find Function&quot; on page 18 for more information.</td>
</tr>
<tr>
<td>Parent</td>
<td>Displays the parent submap.</td>
</tr>
<tr>
<td>Large Icons</td>
<td>Switches to large icons, which shows more detail in the icons.</td>
</tr>
</tbody>
</table>
Table 6. Toolbar Icons (continued)

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Icons</td>
<td>Switches to small icons, which enables more objects to be displayed at one</td>
</tr>
<tr>
<td></td>
<td>time without scrolling.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Starts the zoom function. See <a href="#">Using the Zoom Function</a> on page 18 for</td>
</tr>
<tr>
<td></td>
<td>more information.</td>
</tr>
<tr>
<td>Invert Selected</td>
<td>Changes all selected objects to unselected and changes unselected objects</td>
</tr>
<tr>
<td></td>
<td>to selected.</td>
</tr>
<tr>
<td>Hide Selected</td>
<td>Hides all selected objects</td>
</tr>
<tr>
<td>Hide Unselected</td>
<td>Hides all unselected objects</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the current view</td>
</tr>
</tbody>
</table>

Submap Explorer Toolbar Drop-down Lists

The Submap Explorer toolbar provides two drop-down lists:

- View
- Property Tip (See [Property Tip Drop-down List](#) on page 14 for more information)

**View Drop-down List**

Use the view drop-down list to display the list of views that are available. Click a view to display it.

Table 7 provides a description of the view drop-down lists:

Table 7. Submap Explorer Views

<table>
<thead>
<tr>
<th>View</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>A graphical depiction of objects and connections</td>
</tr>
<tr>
<td>System Configuration</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• Vendor</td>
</tr>
<tr>
<td></td>
<td>• Contact</td>
</tr>
<tr>
<td></td>
<td>• Agent</td>
</tr>
<tr>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• SNMP Address</td>
</tr>
<tr>
<td></td>
<td>• MPLS</td>
</tr>
<tr>
<td>IP Address</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Subnet Mask</td>
</tr>
<tr>
<td></td>
<td>• MAC Address</td>
</tr>
<tr>
<td>Interface</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• MAC Address</td>
</tr>
<tr>
<td></td>
<td>• Subnet Mask</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
<tr>
<td></td>
<td>• Speed</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• HSRP</td>
</tr>
<tr>
<td></td>
<td>• Alias</td>
</tr>
<tr>
<td></td>
<td>• ISDN Backup</td>
</tr>
</tbody>
</table>
### Table 7. Submap Explorer Views (continued)

<table>
<thead>
<tr>
<th>View</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• Home Web Page</td>
</tr>
<tr>
<td></td>
<td>• Management Page</td>
</tr>
<tr>
<td></td>
<td>• Vendor</td>
</tr>
<tr>
<td>IP Configuration</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• Forward</td>
</tr>
<tr>
<td></td>
<td>• TTL</td>
</tr>
<tr>
<td></td>
<td>• IP Reasm Time</td>
</tr>
<tr>
<td>TCP Connections</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• Max Conns</td>
</tr>
<tr>
<td></td>
<td>• Est Cons</td>
</tr>
<tr>
<td></td>
<td>• Estab Resets</td>
</tr>
<tr>
<td></td>
<td>• Attempt Fails</td>
</tr>
<tr>
<td></td>
<td>• Passive Opens</td>
</tr>
<tr>
<td>TCP Configuration</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• Retran Algorithm</td>
</tr>
<tr>
<td></td>
<td>• Min Retrans Timeout</td>
</tr>
<tr>
<td></td>
<td>• Max Retrans Timeout</td>
</tr>
<tr>
<td>SNMP</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• SNMP Queries</td>
</tr>
<tr>
<td></td>
<td>• Bad Community Names</td>
</tr>
<tr>
<td></td>
<td>• Traps Sent</td>
</tr>
<tr>
<td></td>
<td>• Authentication Failure Traps</td>
</tr>
<tr>
<td>Default Route</td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• IP Routes</td>
</tr>
</tbody>
</table>

### Property Tip Drop-down List
A property tip is brief information that is displayed when you pause the cursor over a symbol in the submap. The Web Console provides the following property tips that enable you to quickly access various types of information about an object:

- Object Name
- IP Address
- MAC Address
- Subnet Mask
- System Object ID
- System Location
- System Description
- System Contact
- Vendor
- SNMP Agent
- SNMP Supported
- SNMP Proxied
- None

### Learning about Symbols
A symbol is the icon used on a submap to represent an object in your network. Different symbol types are used to depict different kinds of network objects. For example, a square-shaped symbol type is used to show all computers (PCs, workstations, mainframes, and so forth), and a diamond-shaped symbol type is used to show all connectors (like bridges, gateways and repeaters).
In some cases, a single object can be represented by several different symbols. For example, the IP Map application determines the status of a node object based on the operational status of IP interfaces installed on the node. If all of a node’s IP interfaces are down, the IP Map application reflects the node’s status as critical. From the perspective of the IP Map application, the node is nonfunctional. However, another application might consider the same node to be running, because that application monitors a different protocol with fully functional interfaces. This is an example where you might want to create different symbols to represent different states of the one object.

A symbol has several properties that define how the symbol is used in the Tivoli NetView program. The following sections describe symbol properties.

**Symbol Type**
The symbol type is represented by the outer shape of the symbol, and the symbol subtype is represented by the graphic shown within the shape. For example, the symbol used for a personal computer has a square outer shape and a personal computer icon for its graphic.

**Symbol Behavior**
Symbol behavior defines what happens when you double-click on the symbol or when you click on it and press Enter on the keyboard.

**Explodable Symbols**
When you double-click on an explodable symbol (or click and press Enter), a child submap is opened. An explodable symbol is a symbol that opens to display a lower level of the submap hierarchy.

**Web Manageable Symbols**
Some network objects can use Web-based home pages for configuration and monitoring. To enable web-based home pages, modify the file `\usr\ov\conf\oid_to_type` at the NetView Server; identify the sysObjectIds of the devices that support Web-based management and add the W flag to those lines as per the instructions in the heading of the file. The management home page for a node is assumed to be http://hostname. To use a different URL, modify the ManagementURL field in the Other page of the Object Properties dialog.

**Symbol Label**
Each symbol has a label that describes the object represented by the symbol. The label is displayed below the symbol.

**Symbol Status**
When the Tivoli NetView program displays symbols on a submap, the color of each symbol indicates the status of the object or connection that the symbol represents. For example, an object whose symbol is displayed with a green background is functioning normally. A red background means the object or connection is in critical condition. Table 8 on page 16 shows the default colors used to display status for both icon symbols and connection symbols.

The Tivoli NetView program uses a predetermined set of rules that determine the status to display for each symbol on a submap. See Status Propagation on page 16 for more information.
Table 8. Default Symbol Status Colors

<table>
<thead>
<tr>
<th>Status</th>
<th>Status Meaning</th>
<th>Default Icon Color</th>
<th>Default Connection Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>Status cannot be determined.</td>
<td>Blue</td>
<td>Black</td>
</tr>
<tr>
<td>Normal</td>
<td>Normal operational state</td>
<td>Green</td>
<td>Black</td>
</tr>
<tr>
<td>Marginal</td>
<td>Impaired, but still functional</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Critical</td>
<td>Not functioning</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Unmanaged</td>
<td>Not being monitored. The user has marked this symbol.</td>
<td>Wheat</td>
<td>Black</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Not currently reachable from the management station</td>
<td>White</td>
<td>Black</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Not being monitored. The user has marked this symbol.</td>
<td>Dark Green</td>
<td>Black</td>
</tr>
<tr>
<td>User1</td>
<td>A node is down for reconfiguration. This status is cleared when the node again becomes operational.</td>
<td>Pink</td>
<td>Black</td>
</tr>
<tr>
<td>User2</td>
<td>Indicates a failure that cannot be reset by netmon polling. If User2 is associated with a netmon status trap, the netmon status will override User2.</td>
<td>Violet</td>
<td>Black</td>
</tr>
</tbody>
</table>

**Status Propagation**

The Tivoli NetView program sets the symbol colors on a submap based on the status of objects on its child submaps. This process is called *status propagation*.

**Status Propagation for Nodes With Multiple Interfaces:** Red, green, and yellow are the NetView default colors for status. If a node, such as a router, has multiple interfaces and one interface is down (critical), then the node is red inside the subnet and segment where the critical interface resides. The node is green in all other subnets and segments where the node’s interfaces are up (normal). The node is yellow (marginal) at the IP Internet level, where the compound status of the node is displayed.

**Default Status Rule:** You can use the default status rule for determining status propagation. See Table 9 for more information.

Table 9. Tivoli NetView Default Status Rule

<table>
<thead>
<tr>
<th>Object Status</th>
<th>Condition of Symbols in the Child Submap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>All symbols are normal, acknowledged, or User1.</td>
</tr>
<tr>
<td>Critical</td>
<td>At least one symbol is critical or User2, and no symbols are normal.</td>
</tr>
<tr>
<td>Marginal</td>
<td>Any of the following:</td>
</tr>
<tr>
<td></td>
<td>• All symbols are marginal.</td>
</tr>
<tr>
<td></td>
<td>• Some symbols are normal and some symbols are marginal.</td>
</tr>
<tr>
<td></td>
<td>• Some symbols are normal, some symbols are marginal, and some symbols are critical.</td>
</tr>
<tr>
<td>Unknown</td>
<td>No symbols with a status of normal, critical, marginal, or unmanaged.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Child symbols remain the status they were before the symbol changed to unreachable.</td>
</tr>
</tbody>
</table>
Understanding Maps and Submaps

The Web Console and Web Console Security use the default map. Depending on the role and scope that is defined for your user ID, you can display all of the default map or a portion of it.

The network administrator can create multiple maps within a single NetView program. Each user should open either the default map, or the map indicated by the network administrator.

The NetView program divides a map into submaps based on the TCP/IP network topology. Custom submaps (sometimes called locations) can be created, which display a customized view of the network. Note that the submap hierarchy is defined on the NetView server.

Understanding the Submap Hierarchy

When a map is created, a hierarchy of submaps is created that displays your network in increasing detail. From the internet symbol on the root submap, you can open and display the highest-level internet submap. The following submap hierarchies are created:

- Internet submap
- Network submaps
- Segment submaps
- Node submaps

Using the Internet Submap: The internet submap shows the logical partitioning of IP networks and subnetworks connected by gateways on the graphical map.

Using Network Submaps: The network submap represents the physical topology of a network at the level of network segments. The IP Map application can discover and display objects such as IP-addressable segments, gateways (routers), bridges, and the connections between them on the network submap.

Note: If you are using IP subnetting, network implies subnet.

A network submap can contain segment symbols in the network class and symbols in the connector class.

Using Segment Submaps: A segment submap represents the physical topology of a segment of your network at the level of nodes and connectors. It displays the computers and connectors that comprise a segment on your network.

In IP networks, a segment is a group of data communication objects, with varying degrees of intelligence, that are interconnected through a common transmission medium. Nodes belonging to the same segment typically use a common physical medium to communicate with each other (for example, Ethernet, token ring, telephone lines, or satellite links).

The IP Map application can discover and display the following segment topologies:

- **Bus** Represents nodes attached to a single linear cable that transmits data (for example, Ethernet or IEEE 802.3)

- **Token ring** Represents nodes attached to an SNMP, IP-addressable token ring central wiring MAU through twisted pair wiring, which conforms to the IEEE 802.5 standard
Star  Represents all nodes attached to an SNMP central multiport repeater (a hub)

FDDI ring  Represents nodes attached to an SNMP, IP-addressable Fiber Optic Data Distribution Interface (FDDI)

Using Node Submaps:  The node submap displays symbols that represent the components of a node in a row and column layout. The IP Map application places interfaces on the node submap. When an interface object is added to a node submap, the IP Map application places a connection symbol that represents the interface object in higher-level submaps. In addition, if the nvsniffer program determines that the node contains services, the Collmap application places services on the node submap.

The default propagation of object status within node submaps to the associated nodes in the IP topology is based on both the IP interface objects as well as the service objects. You can, however, customize this propagation in certain ways. Use Edit → Properties/Map→ tab→ page/MapApplication/Properties at the NetView server to specify such things as:

• Whether services should contribute to IP status
• Whether a node should be displayed with the same status in all submaps (by not associating a particular IP interface object with the particular segment on which the node appears). Use Exclusively Set the Status for Nodes at the NetView server to change this.

Using the Zoom Function

Use the zoom function to magnify portions of a Submap Explorer view. Use either of the following methods to start the zoom function:

• Click View → Zoom from the Submap Explorer menu, or click the zoom icon on the Submap Explorer toolbar.
• Place the cursor over the portion of the view that you want to magnify
• To stop the zoom function, click View → Zoom on the Submap Explorer toolbar.

Using the Find Function

Use the find function to find an object, such as a node, network, or interface card. Use the following procedure to find an object:

• Click the Find toolbar button or click Edit → Find from the main toolbar. The find toolbar is displayed.
• Define your search criteria. Click the down-arrow button for each search criteria to see a list of options:
  – Type of find
  – Search by
  – Wildcard (See "Using Wild Cards" on page 19 for more information.)

See Table 10 on page 19 for a description of the search definition options.
• Type your search text.
• Click the Find button.

The search results are displayed in the search results table. The following information is displayed for each object, if applicable:

• Label
• Submap
• Object Name

The following search definition options are available:

<table>
<thead>
<tr>
<th>Find Type</th>
<th>Find By</th>
<th>Find Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find</td>
<td>Find</td>
<td>Displays a list of submaps in which the object is found. Double-click the submap that you want to display.</td>
</tr>
<tr>
<td></td>
<td>QuickFind</td>
<td>Displays the submap immediately if the object is found in only one submap.</td>
</tr>
<tr>
<td>Search By</td>
<td>Object Name</td>
<td>Searches for the object by name.</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td>Searches for the object by hostname.</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Searches for the object by IP address.</td>
</tr>
<tr>
<td>Wildcard</td>
<td>Exactly</td>
<td>The search text is matched exactly.</td>
</tr>
<tr>
<td></td>
<td>Using Wildcards</td>
<td>Use asterisk ( * ) wildcards in the search text.</td>
</tr>
<tr>
<td></td>
<td>Using a Regular Expression</td>
<td>Searches for specific strings from a set of character strings.</td>
</tr>
</tbody>
</table>

Using Wild Cards

Wildcards enable you to substitute one character for either another character or a string of characters. The Wildcard drop-down list provides the following options:

Exactly

Searches for an exact match of the string. Use this option if you know the exact characters that are to appear in the string. For example:

• **pluto.ma.dev.tivoli.com** searches for this hostname.
• **146.84.242** searches for this object name.
• **146.84.242.21** searches for this IP Address.

Using Wildcard

Wildcards are enabled. Use an asterisk (*) as a wildcard anywhere in the search text.

Using a Regular Expression

Regular expressions provide a way to search for specific strings from a set of character strings. For example, `^[a-z][0-9]+\.ma\.dev\.tivoli\.com$` searches for all hostnames that start with 0 or more letters, followed by 1 or more numbers, and end with `ma.dev.tivoli.com`. This would match `nvnt42.ma.dev.tivoli.com`, but would not match `pluto.ma.dev.tivoli.com`.

Refer to *Tivoli NetView for UNIX Administrator’s Guide* for more information.

Understanding Context

Context provides a convenient way to select an object in a view and perform an operation with that object. Menu selections preceded by a diamond (⋄) are used exclusively with context. The following menus and associated submenus are used exclusively with context:

• Object
• Monitor
• Test

For example, use the following procedure to unmanage an object:
• Click the object in a view that you want to unmanage.
• Click **Object → Unmanage** from the main menu.
• The color of the symbol changes to the color defined for unmanage.

**Note:** Not all operations are supported for all objects. You cannot perform operations on an object for which the diamond (◇) is unavailable.

The **Tools** menu provides another way to use context. When you click either **Diagnostics** or **Object Properties**, you can click the **Get Object From Map** button. This inserts the name or IP address of the selected object into the text box.

---

**Using Filters**

Use the table filter function to reduce or refine the list of objects that is displayed in a table. Filters can be applied to all views except tree views. See ["Using Table Filters" on page 8](#) for more information.
Chapter 3. Working with MIBs

The Tivoli NetView program helps you manage network performance by providing several ways to track and collect performance information for objects on the network. You can use performance information in any of the following ways:

- Monitoring the network for signs of potential problems
- Resolving network problems

The performance data collected by the Tivoli NetView program is based on the values of MIB objects. The Web Console displays MIB object values in a table format.

This chapter provides the following information:

- "Understanding MIBs"
- "Using the Web Console MIB Browser (SNMP V1/V2)" on page 23
- "Web Console MIB Loader (SNMP V1/V2)" on page 25

Understanding MIBs

The physical and logical characteristics of network objects make up a collection of information called the MIB. The MIB is not an actual database residing somewhere on the network. The individual pieces of information, called MIB objects, reside on the agent system, where they can be accessed and changed by the agent at the manager's request. This is how the Tivoli NetView program manages network objects.

MIB objects and network objects are not the same. Network objects represent devices and groups of devices that reside on a network. MIB objects are individual pieces of information that, taken as a whole, describe a network object.

MIBs Supported by the Tivoli NetView Program

The Tivoli NetView program supports the following types of MIBs:

- Standard MIB: all devices that support SNMP are also required to support a standard set of common managed object definitions, of which a MIB is composed. The standard MIB object definitions, MIB-I and MIB-II, enable you to monitor and control SNMP managed devices. Agents contain the intelligence required to access these MIB values.

- Enterprise-specific MIB: SNMP permits vendors to define MIB extensions, or enterprise-specific MIBs, specifically for controlling their products. These enterprise-specific MIBs must follow certain definition standards, just as other MIBs must, to ensure that the information they contain can be accessed and modified by agents.

The Tivoli NetView program provides the ability to load enterprise-specific MIBs from a MIB description file. By loading a MIB description file containing enterprise-specific MIBs on a manager station, you can monitor and control vendor devices.

- Generic topology MIB: the Tivoli NetView program provides a generic MIB definition that enables you to manage network elements that communicate by using a protocol other than SNMP. For a list of protocols defined by the Tivoli NetView program, refer to the Tivoli NetView for UNIX Programmer's Guide.
MIB Naming Conventions

MIB objects are logically organized in a hierarchy within a tree structure. Each MIB object has a name derived from its location in the tree structure. This name, called an object ID, is created by tracing the path from the top of the tree structure, or the root, to the bottom, the object itself. Each place where the path branches is called a node. A node can have both a parent and children. If a node has no children, it is called a leaf node. A leaf node is the actual MIB object. Only leaf nodes return MIB values from agents. Figure 1 shows a MIB tree structure.

A full MIB object ID contains all nodes, starting at the root, and including the leaf node. The nodes are concatenated and separated by period marks, in a format known as dotted decimal notation. For example, the mib-2 subtree is .iso.org.dod.internet.mgmt.mib-2, which is concisely written as .1.3.6.1.2.1.

The standard MIB-I and MIB-II definitions are registered in the mib-2(1) subtree. The mib-2(1) subtree is primarily used to manage TCP/IP-based networks through the SNMP protocol.

Enterprise-specific MIBs are registered off the private(4) branch in the subtree enterprises(1). Each enterprise is assigned a number. Digital is assigned the enterprise number 36; so all Digital enterprise-specific objects have the dotted decimal notation starting with .1.3.6.1.4.1.36, corresponding to the tree structure .iso.org.dod.internet.private.enterprises.digital. IBM® is assigned the enterprise number 2, so all IBM enterprise-specific objects have the dotted decimal notation starting with .1.3.6.1.4.1.2, corresponding to the tree structure .iso.org.dod.internet.private.enterprises.IBM.
Using the Web Console MIB Browser (SNMP V1/V2)

Use the MIB Browser to query MIB values for both standard and enterprise-specific MIB objects.

You can also use the MIB Browser to graph MIB objects and their specific instances. Some MIB objects can occur several times per network object, each time with a different value. Each such occurrence of the MIB object is called an instance.

The MIB object iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr, for example, has as many instances as its associated network object has interfaces, as shown in the following example:

1: SE0 DESVA-Class Ethernet Device.
2: LO0 Loopback Port.

However, the system MIB object iso.org.dod.internet.mgmt.mib-2.system.sysContact has only one instance per network object, because generally there is only one person designated as the system contact. This is MIB instance 0, as shown in the following example:

sysContact.0: J. J. Yukio 555-1234

The MIB Browser window provides a tree view in the left pane and information about the selected node in the right pane. In the tree view, branch nodes are represented by folder icons and leaf nodes are represented by a page icon. A branch node is the color white until it is selected. It changes to a darker color when selected, indicating that it is expanding or retrieving data. When expansion or data retrieval is complete, it changes to a very dark color, indicating that it has completed its task. The color of the node depends on the color preferences you have set on your computer.

The Web Console MIB Browser provides the following:
- Read and write community name fields
- SNMP version options
- SNMP walk function
- Real-time graphing function
- Set MIB variable value function

Read and Write Community Names

By default, the MIB Browser uses the community names configured in the SNMP Options (Windows) or SNMP Configuration (UNIX) located in the native console Options menu. To use a community name other than the default, clear the Use Default check box and enter the read or write community name that you want to use.

SNMP Version

The MIB Browser SNMP Version menu provides two options: Version 1 and Version 2. For all features except walk, if a table or object contains any SNMPv2-only objects (counter 64), the MIB browser automatically uses SNMPv2. However, SNMPv2 is not automatically selected for the walk function. Click Version 2 from the SNMP Version menu to perform walks on SNMPv2 tables or objects.
SNMP Walk

You can use the walk function to walk a MIB tree. Use the following procedure to walk a MIB:

- Click or type a name or IP address in the Name or IP Address drop-down list.
- Click the MIB object. The Walk button is enabled.
- Click Version 2 from the SNMP Version drop-down list if you want to walk an SNMPv2 MIB. See “SNMP Version” on page 23 for more information.
- If you want to use a read community name other that the default, clear the Use Default check box that is located under the Read Community Name drop-down box and either select the read community name from the drop-down list or type the read community name.
- Click Walk to begin walking the MIB
- Click Stop at any time to end the walk.

Real-time Graph

The graph function provides a real-time graph of a MIB variable. Use the following procedure to graph a MIB variable:

- Click or type a name or IP address in the Name or IP Address drop-down list.
- Click the MIB object. The Graph button is enabled.
- If you want to use a read community name other that the default, clear the Use Default check box that is located under the Read Community Name drop-down box and either select the read community name from the drop-down list or type the read community name.
- Click Graph to begin real-time graphing
- Click Stop at any time to end the graphing.

When a valid is entered and a relevant MIB object is selected, the Graph button becomes enabled. of the MIB results.

Setting MIB Variable Values

You can change the value of a MIB using the Web Console MIB Browser. Use the following procedure to set a MIB variable value:

- Click or type a name or IP address in the Name or IP Address drop-down list.
- Click the MIB object you want to work with. The Apply button is enabled.
- If you want to use a read community name other that the default, clear the Use Default check box that is located under the Read Community Name drop-down box and either select the read community name from the drop-down list or type the read community name.
- If you want to use a write community name other that the default, clear the Use Default check box that is located under the Write Community Name drop-down box and either select the write community name from the drop-down list or type the write community name.
- Change the MIB variable value in the Value text box
- Click Apply to set the MIB variable.
Web Console MIB Loader (SNMP V1/V2)

Use the simple network management protocol (SNMP) Web Console MIB Loader to load and unload MIBs for the Web Console MIB Browser. The MIB loader is part of the native console. To start the MIB loader, click **Tools → Web Console MIB Loader** for both Windows and UNIX. The MIB Loader window displays a list of the loaded MIBs.

**Loading MIBs**

Use the following procedure to load a MIB:

- Click **Load**.
- Either click **Look In** and find the files to load into the drop-down list, or type the path and filenames in the **File Name** field.
- Click **Load**. A Loading MIBs window is displayed and a progress bar shows file processing status. The **Messages** pane provides informational messages and parsing errors.
- Click **OK** to commit the changes.

**Unloading MIBs**

Use the following procedure to unload a MIB:

- Select the MIB from the list of loaded MIBs.
- Click **Unload**. An Unloading MIBs window is displayed and a progress bar shows the file processing status.
- The Messages window displays informational messages. Click **OK** when prompted to commit the changes if parsing encountered no errors.
Chapter 4. Monitoring Network Configuration

There are many reasons to keep track of the configuration of objects on your network. The following provides configuration information you might need:

- The IP and non-IP addresses for a node or nodes
- The types of interfaces a node supports, and the status of each
- How a node is connected to the network
- Whether two nodes show the same address for a third node
- Whether a particular service has been installed on a remote node

This chapter provides the following information:

- "Chapter 4. Monitoring Network Configuration"
- "Displaying Addresses for Remote SNMP Nodes"
- "Displaying Configured Interfaces"
- "Displaying Routing Table Information" on page 28
- "Displaying ARP Cache Information" on page 28
- "Displaying Configured IP Services" on page 28
- "Displaying TCP Information" on page 28
- "Monitoring I ANS" on page 29
- "Monitoring MPLS Network Status" on page 30
- "Retrieving MIB Configuration Information" on page 30
- "Displaying MIB Interface Information" on page 31
- "Displaying MIB System Information" on page 31
- "Managing Network Devices through the Web" on page 31

Displaying Addresses for Remote SNMP Nodes

To display IP and non-IP addresses associated with a remote SNMP node, select a node on a submap, then click Monitor → Network → Addresses from the menu bar to collect information that you might otherwise have to obtain by looking at numerous configuration files. The following information is provided about each interface this object has with the network:

- The name of the interface
- The IP address of the interface
- The network mask
- The network address
- The link address if any

Displaying Configured Interfaces

Click Monitor → Network → Interfaces from the main menu to display information about interfaces on remote SNMP nodes. This information can help you resolve performance problems, because it provides statistics on incoming and outgoing SNMP node traffic and associated errors. It can also help you resolve connectivity problems because it lists the status of interfaces.

The following information is provided:

- The MIB instance of the interface on the selected node.
- The name of the interface.
- The type of interface, for example, loopback, Ethernet, FDDI.
- The maximum transmission unit (MTU) size. This is the largest packet size that can be sent unfragmented.
- The status of the interface, which can be up, down, or testing. If the status is testing, no operation packets can be passed through the interface.
- The total number of input packets and the number of erroneous input packets received.
- The total number of output packets and the number of erroneous output packets sent.

For hubs and bridges, each entry in the MIB table corresponds to a port on the hub or bridge.

**Displaying Routing Table Information**

To display routing table information for selected remote SNMP nodes, click Monitor → Network → Routing Table from the menu bar. The following information is provided to help you resolve connectivity problems.

- The default destination, which is a route used by the system when it cannot find a specific route
- The name of the next gateway between the selected node and the destination
- The following types of connection:
  - Direct, a directly connected local area network (LAN)
  - Remote, through a remote gateway
  - Other
- The name of the interface that is used to reach the destination

**Displaying ARP Cache Information**

The Address Resolution Protocol (ARP) cache is helpful in resolving connectivity problems, because it can tell you whether two nodes have a different link address than a third node.

To display this information for selected remote SNMP nodes, click Monitor → Network → ARP Cache from the menu bar. The following information is displayed:

- The name or IP address of the destination node
- The link address associated with the destination node
- The interface name of the selected node that is used to access the destination node

**Displaying Configured IP Services**

You might need to know the IP services a node is configured to support. For example, a user might be having trouble accessing a particular service on a remote SNMP node. Click Monitor → Network → IP Services to display the following information:

- The service protocol.
- The port to which the service is bound.
- The service for which the node is listening, such as SNMP or Telnet. If this field is blank, the service is unknown.
Displaying TCP Information

Click **Monitor → Network → TCP Connections** to obtain the following information:
- The local address
- The remote address
- The state of the connection

Determining System Information

Use the System menu to display information about the nodes in your network.

**Note:** To display system information, the object must be running an SNMP agent that supports the host resource MIB.

Click **Monitor → System** to display the following information:

<table>
<thead>
<tr>
<th>Selection</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Displays general MIB information about the node, such as how long the system has been running and how many users are working on the system</td>
</tr>
<tr>
<td>CPUs</td>
<td>Identifies the object’s CPU and its one minute load average</td>
</tr>
<tr>
<td>Processes</td>
<td>Displays process information, such as the process parameters and status</td>
</tr>
<tr>
<td>Memory</td>
<td>Displays information about the memory on the object</td>
</tr>
<tr>
<td>Printers</td>
<td>Displays information about the printers on the object</td>
</tr>
<tr>
<td>Devices</td>
<td>Displays information about devices on the object</td>
</tr>
<tr>
<td>Storage</td>
<td>Displays information about storage devices on the object</td>
</tr>
<tr>
<td>Partitions</td>
<td>Displays disk partition information</td>
</tr>
<tr>
<td>File Systems</td>
<td>Displays file system information about the object</td>
</tr>
</tbody>
</table>

Monitoring LANs

Use the **LAN Manager** menu to display information about the LAN Manager nodes in your network. Click **Monitor → LAN Manager** to display the following information:

<table>
<thead>
<tr>
<th>Selection</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Files</td>
<td>Display information about shared files on the node. Shared files are files that the LAN Manager node has made available to other nodes in the network.</td>
</tr>
<tr>
<td>Server Statistics</td>
<td>Displays information about the node’s performance as a LAN Manager server.</td>
</tr>
<tr>
<td>Workstation Statistics</td>
<td>Displays information about the node’s performance as a LAN Manager workstation.</td>
</tr>
<tr>
<td>Services</td>
<td>Displays the services available on the node.</td>
</tr>
<tr>
<td>Print Queues</td>
<td>Displays information about the print queues that the LAN manager node has defined for sharing on the network.</td>
</tr>
</tbody>
</table>
Monitoring MPLS Network Status

A router that supports Multiprotocol label switching (MPLS) is called a *Label Switching Router* (LSR). Use the MPLS function to monitor the MPLS layer of LSR backbone networks. Two views of MPLS information are provided:

- An MPLS node view, which displays information for the interface that the segment comes in on.
- An MPLS interface view, which displays information for the segments that enter the LSR on the interface that is selected.

Click **Monitor → MPLS → MPLS Node View** to display the following information:

<table>
<thead>
<tr>
<th>Column Label</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>InSeg ifIndex</td>
<td>The interface that the segment comes in on</td>
</tr>
<tr>
<td>InSeg Label</td>
<td>The incoming label</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Used with Admin Status to provide the cross-connection status</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Used with Oper Status to provide the cross-connection status</td>
</tr>
<tr>
<td>OutSeg ifIndex</td>
<td>The outgoing interface</td>
</tr>
<tr>
<td>OutSeg Label</td>
<td>The outgoing label</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The address of the next hop</td>
</tr>
</tbody>
</table>

Click **Monitor → MPLS → MPLS Interface View** to display the following information:

<table>
<thead>
<tr>
<th>Row Label</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper Status</td>
<td>Used with Admin Status to provide the cross-connection status.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Used with Oper Status to provide the cross-connection status.</td>
</tr>
<tr>
<td>OutSeg ifIndex</td>
<td>The outgoing interface</td>
</tr>
<tr>
<td>OutSeg Label</td>
<td>The outgoing label</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The address of the next hop</td>
</tr>
</tbody>
</table>

Retrieving MIB Configuration Information

Certain MIB variables store information that provides a summary of the configuration of a selected network node or nodes. Use the procedures in this section to enable you to conveniently retrieve the values of frequently accessed MIB variables.
Displaying MIB Interface Information

To display the current values of a network object’s interface MIB variables, select a symbol on the submap, then click Monitor → Other → Interfaces from the menu bar. Table 13 provides more information.

Table 13. MIB Interface Information

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>MIB Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Description</td>
<td>ifDescr</td>
<td>The manufacturer, product, and version of the hardware interface</td>
</tr>
<tr>
<td>Type</td>
<td>ifType</td>
<td>Type of interface</td>
</tr>
<tr>
<td>MTU</td>
<td>ifMtu</td>
<td>Size of largest datagram that can be sent or received over this interface, specified in octets</td>
</tr>
<tr>
<td>Speed</td>
<td>ifSpeed</td>
<td>Estimated current bandwidth of the interface, in bits per second (bps)</td>
</tr>
<tr>
<td>Physical Address</td>
<td>ifPhysAddress</td>
<td>Address of the protocol layer at the protocol layer immediately below the network layer in the protocol stack, in octets.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>ifAdminStatus</td>
<td>Desired state of the interface (up, down, or testing)</td>
</tr>
<tr>
<td>Operational State</td>
<td>ifOperStatus</td>
<td>Current operational state of the interface</td>
</tr>
</tbody>
</table>

Displaying MIB System Information

To display the current values of a network object’s system MIB variables, select a symbol on the submap, then click Monitor → Other → System from the menu bar. The information in Table 14 is displayed:

Table 14. MIB System Information

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>MIB Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Description</td>
<td>sysDescr</td>
<td>Name and version of the hardware, software operating system, and networking software</td>
</tr>
<tr>
<td>Object ID</td>
<td>sysObjectID</td>
<td>Node that is being managed</td>
</tr>
<tr>
<td>Up Time</td>
<td>sysUpTime</td>
<td>Time, in hundredths of a second, since the network management portion of a system was last initialized</td>
</tr>
<tr>
<td>Contact</td>
<td>sysContact</td>
<td>Contact person for this managed node, and how to contact that person</td>
</tr>
<tr>
<td>Name</td>
<td>sysName</td>
<td>Administrative name (fully qualified domain name) assigned to this node</td>
</tr>
<tr>
<td>Location</td>
<td>sysLocation</td>
<td>Physical location of the node</td>
</tr>
</tbody>
</table>

Managing Network Devices through the Web

Certain network devices can be managed through World Wide Web pages. You can configure NetView to access the management pages directly from the NetView submap. Select the device symbol, then either click Object → Management Page, or right-click the object and then click Management Page. The default Web browser is started with the default home page on that device.
Chapter 5. Diagnosing Network Problems

The Tivoli NetView program enables you to perform fault management tasks to locate and resolve problems that occur in networks managed by the Tivoli NetView program.

You can use the Web Console to continuously monitor routine monitoring of the networks managed by the Tivoli NetView program. Monitoring a network’s behavior gives you an historical record of its performance, which can be helpful if you need to re-create a particular network configuration after discovering a widespread problem. You can also monitor the network’s real-time performance to track developing trends and lessen the risk of major problems.

This chapter provides the following information:
- "Gathering Information about Your Network"
- "Diagnosing Network Connectivity Problems" on page 34
- "Diagnosing Network Performance Problems" on page 38
- "Diagnosing Network Service Problems" on page 40

Gathering Information about Your Network

The Tivoli NetView program enables you to gather and save information about your network that can help you track and resolve problems. This section describes some ways to gather network information.

Polling the Network

Generally, agents in the network are regularly polled to update the status of the Tivoli NetView objects. The information obtained by this regular polling is used to update the topology map.

To collect status information between scheduled polling intervals, select the node or nodes whose status you want to know, then click **Test → Demand Poll** from the menu bar. If a node suddenly goes down or if you suspect problems with network traffic to or from the node, a demand poll can help you pinpoint the problem area.

Regardless of whether polling is conducted at regular intervals or on demand, the polled data includes the following information:
- Object status
- Network topology changes, including new nodes
- Configuration changes
- Surpassed thresholds that indicate a set limit was reached or exceeded

Viewing Network Events

Use the Event Browser to check for events that are problems or could become problems. The Tivoli NetView program records network events and creates the following event categories shown in **Table 15**.

<table>
<thead>
<tr>
<th>Events Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold Events</td>
<td>A threshold was exceeded.</td>
</tr>
<tr>
<td>Network Topology Events</td>
<td>An object or an interface was added or deleted by an application.</td>
</tr>
</tbody>
</table>
Table 15. Network Events (continued)

<table>
<thead>
<tr>
<th>Events Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Events</td>
<td>An inconsistent or unexpected behavior occurred.</td>
</tr>
<tr>
<td>Status Events</td>
<td>An object or an interface status changed to up or down, because the object or interface started or stopped responding to ICMP echo requests.</td>
</tr>
<tr>
<td>Node Configuration Events</td>
<td>A node’s configuration changed.</td>
</tr>
<tr>
<td>Application Alert Events</td>
<td>A Tivoli NetView application generated an alarm or alert.</td>
</tr>
</tbody>
</table>

To view the events in each category:
- Click **Tools → Event Browser** from the main menu bar.
- Click **Filter → Set** from the Event Browser menu bar.
- Click **Other**
- Click the **Events with Categories** check box.
- Click the categories that you want to display
- Click **Apply → OK**
- Click

**Displaying Node Information**
Click **Monitor → Network → Addresses** to retrieve and display specific information in a Diagnostics window about a selected node, including TCP/IP and physical (link) addresses. Once the diagnostics window is open, you can retrieve and display the following information by clicking an object in the tree view:
- Interface
- Routing Table
- ARP Cache
- IP Services
- TCP Connection

See "Gathering Connectivity Information" on page 38 for more information.

**Diagnosing Network Connectivity Problems**

A network connectivity problem exists when a user cannot contact a system on the local network or on another network.

**Testing Connectivity**

Use the following functions to test your network’s connectivity:
- Click **Test → Connectivity** to test the TCP/IP and SNMP protocols. This selection polls the device at the TCP/IP and SNMP layers to verify that it is connected to the management system.
- Click **Test → Ping** to determine the number of packets sent and lost, and the round-trip times between the manager and a remote node. This command verifies connectivity at the IP level.
- Examine patterns in the status colors to determine connectivity problems. For example, if a connector and all objects on one side of it are down (indicated by the color red), the connector is probably the source of the problem.
QuickTest is an enhanced ping tool that polls all managed interfaces and quickly determines the complete status of the node. QuickTest displays the ifAdminStatus and ifOperStatus of each interface for nodes that use SNMP to poll for status. For all other nodes, QuickTest displays the ping result for each interface. If the status of an interface has changed, the map is updated and an event sent.

To use QuickTest, click either Test → QuickTest or Test → QuickTest Critical. You must have one or more nodes selected to access the QuickTest menus. The Test → QuickTest Critical menu item only polls interfaces that are currently marked as down. The Test → QuickTest menu item polls all interfaces, regardless of their current status.

Locating Routes between Nodes

To keep certain parts of the network running, you might need to locate an alternate route between two nodes so all traffic between them can bypass another route that is having problems. To locate specific IP routes between two selected nodes:

- In Submap Explorer, click on the object you want to locate the route from.
- Click Test → Locate Route from the menu bar.
- In Submap Explorer, click on the object you want to locate the route to.
- Click Get Object From Map → Refresh

Both nodes and all IP-addressable objects and connections between them are displayed. The source node and node address and the intervening gateways and gateway addresses are also displayed if applicable.

Gathering Connectivity Information

Gather and analyze the following information to help diagnose connectivity problems:

- Click Monitor → Network → Routing Table to obtain gateway routing table information for a remote SNMP node.
- Click Monitor → Network → ARP Cache to obtain address translation table information for a remote SNMP node.
- Click Monitor → Network → Addresses to determine IP and link addresses for a remote SNMP node.
- Click Monitor → Network → IP Services to determine network services available on a remote SNMP node.
- Click Monitor → Network → Interfaces to obtain interface information.
- Click Monitor → Network → TCP Connections to obtain address and state information.

Checking Connectivity within the Same Network

Use the following procedure when a user is having problems connecting from one system to another system within the same network.

Prerequisites:

- To connect to a node through Telnet, the remote node must have TCP Services running.
- To use the ARP Cache operation, the selected node must support SNMP.
In Figure 2, a user is unable to connect from System A to System B on the same network.

![Figure 2. Connectivity within the Same Network](image)

1. Look at the status color of System B on the map. If it is red, System B is down. If it is not red, go to Step 2.
2. Check to see if System A and System B are operational.
3. Click Test → Ping to send a ping from the management system to System A and System B.
   If the ping to either system fails, check to see if the system is down.
   If the ping to both systems is successful, go to Step 4.
4. Determine if there is a hostname-to-IP address mapping problem.
   From the command line, use Telnet to login to System A. After you have logged in, ping System B. If the ping fails, go to Step 5.
   If the ping works, you might have a hostname-to-IP address mapping problem.
   To verify and fix the problem, do the following:
   a. Look in the hosts file for the hostname of System B, as defined to System A.
      If System A is a UNIX workstation, the hosts file is /etc/hosts.
      If System A is a Windows workstation, the hosts file is \%windir%\system32\drivers\etc\hosts, where %windir% is the release directory for the release of Windows that is running on the management system.
   b. Telnet to System B, and then ping System A. Look in the System B host's file for the hostname of System B. It should be the same as System B's name in the System A host's file.
5. Determine whether there is an IP-address-to-link-address mapping problem.
   a. On the map, select the management system and System A.
   b. Click Monitor → Network → ARP Cache to view the ARP cache tables of the management system and System A.
   c. Locate the IP address of System B in both tables and compare the link address for System B.
      If System A's link address for System B is not the same as the management system's link address for System B, change System B's link address on System A.
      If the link addresses are the same, you might not have a connectivity problem, but rather a performance or network service problem. For more information, see "Diagnosing Network Performance Problems" on page 38 and "Diagnosing Network Service Problems" on page 40.
Checking Connectivity across Networks

Use the following procedure when a user is having connectivity problems from a system on one network to a system on a different network.

Prerequisites:

To use the Locate Route command:

- All nodes along the route, except the destination node, must be running SNMP.
- All gateways between the selected nodes must have their community names correctly set.

In Figure 3, a user is trying to connect from System B on Network 1 to System C on Network 2. The path between the two networks includes two gateways, G1 and G2.

1. If System C’s status on the map is red, System C is down. If it is not red, go to Step 2.
2. Check connectivity to System C.
   - Click **Test → Ping** to send a ping from the management system to System C. If the ping is successful, go to Step 3. If the ping fails, take the following action:
     a. Send another ping from the management system to G2.
     b. If the second ping is successful, go to Step 3. If the second ping fails, G2 is down.
3. Check connectivity to System B.
   - Click **Test → Ping** to do a ping from the management system to System B. If the ping is successful, go to Step 4 on page 38. If the ping fails, take the following action:
     a. Send another ping from the management system to G1.
     b. If the second ping is successful, go to Step 4 on page 38. If the ping fails, G1 is down.
4. Find the route between the systems and all intermediate objects between them. On the map, select System B, then type the selection name for System C in the To text box. Click Test → Locate Route.

5. Look at the information in the dialog box to see if the path is correct. For example, if the route leads to G3 rather than G1 and G2, the routing table for System B is incorrect.

6. Look at the map to verify that all nodes along the correct path are operating. A node with a yellow or red status indicates that the node either has a problem or is not operating. If a node is yellow or red, diagnose the problem on that node.

7. If the route is correct and everything is operating along the path, the problem might not be related to connectivity, but rather to performance or network service. For more information, refer to "Diagnosing Network Performance Problems" and "Diagnosing Network Service Problems" on page 40.

---

**Diagnosing Network Performance Problems**

A network performance problem might be revealed by one of the following conditions:

- Users experience slow system response while running applications or during communications across the network. This could be caused by a traffic overload on the network or an unhealthy device, such as a gateway.

- Users experience a loss of data during transmission. A network or device might be overloaded, causing a timeout.

**Prerequisites:**

- The originating node can reach the destination node without losing a connection.
- Ensure that the community names for all gateways between the selected nodes are correct.
- To monitor interfaces or interface traffic on a selected node, the node must support SNMP.

In [Figure 4 on page 39], the user is experiencing unusually slow response time trying to communicate from System B on Network 1 to System C on Network 2. Suppose that, from the management system, the response time on Network 3, where System E resides, is normal. In this example:

- System A and System B are both on Network 1 (G1).
- System C is on Network 2 (G2).
- System E (which has relatively low usage) is on Network 3 (G3).
- Two gateways exist between System B and System C.
- The networks are Ethernet networks.
1. Click **Test → Locate Route** to find the route between System B and System C and all intermediate objects between them. In this example, the route is B to G1, G1 to G2, and G2 to System C.

2. Select System A and connect to it using Telnet. From System A, ping System C. Then select System B and connect to it using Telnet. From System B, send pings to Systems C, D, and E. Record the response times on these pings, and then diagnose the problem as follows:
   - If the response time from B to C, B to D, and A to C is slower than the response time from B to E, you have a network problem. Go to Step 3.
   - If the response time from B to C and A to C is slower than the response time from B to D and B to E, the central processing unit (CPU) for System C is overloaded. Select System C and log into it using Telnet. Then, run a local CPU monitoring utility to verify the CPU overload for System C. Next, reduce the CPU load for System C, for example, by stopping some processes or having users log off the system.
   - If the response time from B to C, B to E, and B to D is similar but slower than the response time from A to C, the CPU for System B is overloaded. Select System B and log into it using Telnet. Then run a local CPU monitoring utility to verify the CPU overload for System B. Next, reduce the CPU load for System B, for example, by stopping some processes or having users log off the system.

3. To locate the network problem, use Telnet and **Test → Ping** to do the following:
   - Log into System B and ping G1.
   - Log into System G1 and ping G2.
   - Log into System G2 and ping C.

   Record the response times on these pings, and then diagnose the problem as follows:
   - If the response time from B to G1 is faster than the response time from G1 to G2 and G2 to C, check the traffic on G2. Go to Step 4.
   - If the response time from G2 to C is faster than the response time from B to G1 and G1 to G2, check the traffic on G1. Go to Step 4.
   - If the response time from G1 to G2 is slower than the response time from B to G1 and G2 to C, the problem resides between G1 and G2. You might need to set up a different route, subnetwork, or gateway on your network.

4. Select the gateway with the problem. Click **Monitor → Network → Interfaces** to see trends of the interface traffic displayed in a table. Click **Monitor → Network → Interfaces** to see a snapshot of the interface data displayed in a table. If input and output data on interface traffic is abnormally high, you might have a routing problem.
problem, an overloaded interface, or an overloaded gateway. In this case, click **Test → Locate Route** to find alternate routes and reroute network traffic, accordingly.

**Monitoring Performance and Traffic**

If you suspect performance problems, you can monitor and graph certain statistics to help isolate problems. First, verify that the SNMP agent is running for the nodes you want to check. Then click **Monitor → Network → Interfaces** to observe traffic patterns on the nodes, peak values, and averages over given intervals:

To monitor performance and traffic on other vendor devices, or to monitor MIB variables other than MIB-2, use the MIB browser real-time graphing function by clicking **Tools → MIB Browser** from the main tool bar and **Tools → Graph** from the Event Browser tool bar. Status polling generates the heaviest amount of network traffic. You can monitor the traffic generated by the Tivoli NetView program by clicking **Monitor → Network → Interfaces**. Use this command several times and observe the differences in the number of packets sent and received.

**Gathering Performance Information**

Gather and analyze the following information to diagnose performance problems:

**Note:** The information that can be gathered for monitoring depends on the vendor MIBs.

- To detect changes in the status of interfaces, check the node color (indicating the status) and click **Object → Object Properties** to see the status of a specific interface.
- To check for errors in incoming and outgoing packets and errors for each connected interface for a remote SNMP node, click **Monitor → Network → Interfaces**.
- To determine the round-trip times between nodes, click **Test → Ping**.

**Diagnosing Network Service Problems**

In a network service problem, a user reaches System B from System A, but either the connection from System B is refused or the command that is executed from System A to System B is not accepted.

A network service problem might be revealed by one of the following conditions:

- After connecting to a remote system, the user receives an error that the remote system does not accept the command that was initiated. This could be a service problem related to security.
- After connecting to a remote system, the user receives an error that the command sent to the remote system was not recognized. For example, System B does not allow login for an `ftp` command from System A. This could mean the service is not installed or configured.

**Prerequisites:**

- To view the IP/TCP/SNMP protocols and services available on a selected node, the node must support SNMP.
- The originating node can reach the destination node without losing a connection.
- You must have privileges on the system you are trying to configure. For UNIX systems, you must have root authority. For Windows systems, you must be a member of the Administrators group.
In Figure 5, a user tries to use a network service, such as the `ftp` command, from System A to System B and receives an error message.

**Figure 5. Diagnosing Network Service Problems**

Perform the following steps to diagnose this network service problem:

1. Click **Test → Connectivity** on both System A and System B to ensure that they support the network protocols and that the protocols are working. If there are problems with the protocol, an error will appear in the message field.

2. If the nodes support SNMP, click **Monitor → Network → IP Services** to ensure that they support the service in question, such as FTP.

3. If the nodes provide the service, go to Step 5. If they do not provide the service, check the file system on the two systems to see if the software for the service, such as Telnet or FTP, is installed.

4. If the service is not installed, install the software on the system. If the service software is installed, configure the service on the system. Go to Step 6.

5. Check service security on System B. Ensure that the IP address of System A is set for allow access and not excluded by a deny access setting in the security files for the service in question.

6. Request the service again, from System A to System B, to verify that the problem is fixed.
Chapter 6. Working with Events and Event Filters

To help you manage a network effectively, the Tivoli NetView program must receive information about changes that affect objects in the network. Traps generated by agents that monitor network objects convey this information to the Tivoli NetView program. A trap is a message sent from an SNMP agent to an SNMP manager without a specific request from the SNMP manager.

Agents send traps to the SNMP manager to indicate that a particular condition exists on the agent system, such as the occurrence of an error. In addition, the SNMP manager generates traps when it detects status changes or other unusual conditions while polling network objects.

The Web Console provides the Event Browser for viewing traps, which are considered events by the Tivoli NetView program.

Large networks with many objects and agents can generate so many traps and events that you may want to create event filters. Event filters allow you to specify the kinds of events and traps you want to see in the Event Browser window. Filtering events enables you to keep your attention focused on only those events and traps that are important to you in managing your network.

This chapter provides the following information:
- "Understanding Events"
- "Displaying Events" on page 44
- "Graphing Events" on page 45
- "Filtering Events for Display" on page 45

Understanding Events

The Tivoli NetView program uses the following types of events:

**Map events**
Notifications issued when a user or application does something that affects the status of the current map or of the Tivoli NetView graphical interface. For example, if you add a connection between a workstation and a server on a submap, an event is generated and logged in the event log file. The contents of the submap change to include the added connection.

**Network events**
Messages sent by an agent to one or more managers to tell them an event has occurred that affects a network object. These events are not necessarily reflected in the map. For example, if an SNMP agent is not in your management region, but is configured to send traps to the manager, you receive events for that agent, even though the agent is not displayed on your map.

**Tivoli NetView**
Internal events are messages generated by Tivoli NetView applications.

When Events Are Generated

Events are generated when at least one of the following conditions occur:
- A threshold limit set through the Tools → MIB → Collect Data option on the native console was exceeded.
• The network topology changed; for example, an object or interface was added or deleted at the native console.
• An informational message or an error indicating inconsistent or unexpected behavior.
• An ICMP echo request detected that an object’s status changed or that an interface stopped.
• A node’s configuration changed.
• An SNMP trap was received from a managed node.

Information Displayed by Events

Events provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time that the trap occurred.</td>
</tr>
<tr>
<td>Node</td>
<td>The node that originated the trap.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>The network-management subsystem that generated the trap</td>
</tr>
<tr>
<td>Generic</td>
<td>If a generic trap is generated, the generic trap number is provided.</td>
</tr>
<tr>
<td>Specific</td>
<td>If a specific trap is generated, the specific trap number is provided.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity defined for the trap.</td>
</tr>
<tr>
<td>Category</td>
<td>The category assigned to the trap for the trap.</td>
</tr>
<tr>
<td>Source</td>
<td>The agent that generated the trap.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the trap.</td>
</tr>
</tbody>
</table>

Displaying Events

The Event Browser displays all the events you have filtered for display as they occur in your network. Some of these events are forwarded to the Tivoli NetView program from the attached network, and some are internal events generated by Tivoli NetView applications, such as the netmon daemon.

Starting the Event Browser

To start the Event Browser, click Tools → Event Browser from the main menu.

You can display events for all nodes or a selected node. As new events occur in the network, they are displayed in the Event Browser if they match the filter you select.

Customizing the Event Display

The Event Browser displays information in column format for an event. You can customize the display to show only the columns you need. For example, you can hide the columns you do not want displayed and resize the remaining columns for a better view of their information. Click View → Columns to hide or display columns.

To display all information for a specific event, either click the event and then click Event → Details, or right-click the event and then click the Details button. See "Information Displayed by Events" for a description of the information that is displayed.
Pausing the Event Display

As new events occur in the network, the Event Browser window is updated. The oldest event in the list is scrolled off the top of the list when a new event occurs, and the new event is added to the bottom of the list.

New events might occur before you have finished analyzing the existing events. To make sure the events you are working with are not scrolled, stop the display by clicking View → Pause Display.

Pausing the display only stops the event display, it has no impact on the events database. The Event Browser stores events in the events database and reads events from the database for display. When you resume the display, the Event Browser reads the events database and updates the display.

Graphing Events

You can graph events to display the ratio of events by severity. Click Tools → Graph to display the graph.

Filtering Events for Display

You can view or change filters by clicking Filter → Set. For example, you might not want to see an event every time a workstation is powered off for the day. Or, if several operators are monitoring the network, you might want to create different event filters for each system running the Tivoli NetView program, so each operator can concentrate on a specific type of network problem or a specific group of devices in the network.
Chapter 7. Configuration and Security

Use the information in this chapter to define users and configure the Web Console.

This chapter provides the following information:

- Web Console Security
- Web Console Security
- Working With Logs on page 50
- Customizing the Web Server on page 52

Web Console Security

The NetView program provides security using configuration files. Users, roles, and scope profiles are created using the Web Console Security window, and these profiles are used to validate Web Console access to the Web Server. Actions and views are regulated by roles and scoping, which are assigned to a user’s profile.

Use a combination of roles and scope to define the view that the user can display and the actions a user can perform within that view. Security is used to validate access to the following:

- Submap Explorer
- Object Properties
- Diagnostics
- Event Browser
- MIB Browser

Security Notes:

1. The roles and scope discussed in this section apply only to users accessing the NetView program through the Web Console.

2. Users with direct access to the NetView server and the conventional NetView client continue to have their access controlled by the existing NetView security mechanisms. Users with root access to the NetView server machine continue to have unlimited access to NetView capabilities and data.

3. You must control physical access to the NetView server machine (and provide a firewall if necessary) to protect your network. Some administrative tasks require physical and root access to the NetView server, because this is the appropriate way to control access to those functions.

4. The Security Console only defines users in the NetView realm. To view NetView or Jetty log files over HTTP, users must be defined in the NetView Admin and Jetty Admin security realms by editing the corresponding properties file. See Understanding Security Realms on page 50 for more information.

5. The Security Console is useful for configuring a small number of user accounts, but if you want to create or change a large number of accounts, you can write a script to modify file NetViewRealm.properties. See Understanding Security Realms on page 50 for more information.

Security must be defined on the security console. The UNIX security console must be started from the native console. The Windows security console can be started either from the native console or from the Windows program. Use the following procedures from the native console to start the security console on either Windows or UNIX:
Use the following procedures from the Windows program to start the security console:

- Click **Start → Program**
- Click **Tivoli NetView**
- Click **Administration**
- Click **Server Setup**. The Server Setup window is displayed.
- Click **Daemon** if the Daemon window is not displayed.
- Click the down- arrow and click **Web Server** from the pull-down list, double-click **webserver** in the daemons list.
- Click **Configure Web Console Security**.

### Defining Security Accounts

Use the following procedures to define:

- Roles
- Scope
- Users

**Note:** Roles and scope must be defined before users can be defined.

### Defining Roles

A user’s role constrains the actions that they are enabled to perform as follows:

- By the actions that are enabled at the Web Console.
- By a filtering mechanism at the Web Server that rejects unauthorized actions.

The following default roles are defined:

<table>
<thead>
<tr>
<th>Role</th>
<th>General Actions Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator and SuperUser</td>
<td>All actions are permitted.</td>
</tr>
<tr>
<td>Operator</td>
<td>All actions are permitted, except managing and unmanaging objects.</td>
</tr>
<tr>
<td>User</td>
<td>Permitted to use Submap Explorer, Object Properties, the Event Browser and the device’s Web home page.</td>
</tr>
</tbody>
</table>

Use the following procedure to define a role:

- Click **Roles**
- Click the **Add** icon, or click **Selected → Add**.
- Type the role name
- Type an optional description.
- Click **OK**.
Click the Allow Scoping in Event Browser check box if you want scoping enabled for the Event Browser.

Select the applicable actions and click Save.

Click File → Save. You are prompted to stop and restart the Web Server.

Click File to restart the Web Server if you didn’t restart it in the previous step.

Click File → Exit.

**Defining Scope**

Scope is used to limit the network topology that users can display. Scope is also used to limit the target objects that users can perform actions against. A scope is defined by a set of top level locations and networks. All logical objects (networks and segments) and physical devices (Routers, Nodes, Interfaces) within a scope’s set of root locations and networks are considered to be within the scope, and are available for viewing and performing actions against.

The default No scoping restrictions option means that users with this scope definition have unlimited access.

To enable scoping, the default map must be open either as the netviewd daemon or as the native console.

Scope is used by the Submap Explorer as follows:

- The only map enabled for viewing is the Default map.
- The Root submap contains only those networks and locations that are within scope. This submap uses a row and column layout style, which means that SmartSet submaps cannot be displayed.
- Node submaps do not display interfaces that are not in a user’s scope.
- The Find feature does not display any symbol matches that are not in a user’s scope.
- When you right-click an object, the Show in menu displayed does not contain any symbols that are not in a user’s scope.

For Diagnostic, Object Properties, and MIB Browser functions, if you type an object name, hostname, or IP address that is not in a user’s scope, the operation is not performed and a message is displayed.

The Event Browser does not display events that are not in a user’s scope if the Allow Scoping in Event Browser check box was checked when the user’s scope was defined.

Use the following procedure to define scope:

- Click Scope.
- Click Add.
- Type the user ID
- Click either Network or Location.
- Type a location or network.
- Click Add.
- Add other networks or locations that you want to include as part of this scope.
- Click File → Save. You are prompted to stop and restart the Web Server.
- Click File to restart the Web Server if you didn’t restart it in the previous step.
- Click File → Exit.
Defining Users
Use the following procedure to define users:
- Click **Add**.
- Type the user ID and password.
- Type the password again to confirm it.
- Click the down-arrow. Select the user’s role.
- Click **File → Save**. The Save dialogue is displayed.
- Click **No** if you want to either create or modify a role or scope for the user. Click **Yes** to restart the server.

Understanding Security Realms
A security realm is a Web Server security policy region. Table 17 provides information about the realm files:

<table>
<thead>
<tr>
<th>Realm</th>
<th>Properties File</th>
<th>URL Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetView</td>
<td>NetViewRealm.properties</td>
<td>/netview/*</td>
<td>Defines user security accounts for the Web Console</td>
</tr>
<tr>
<td>NetView Administration</td>
<td>NetViewAdminRealm.properties</td>
<td>/netviewlogs/*</td>
<td>Defines administrator security accounts that enable access to the NetView log files under /usr/OV/log</td>
</tr>
<tr>
<td>Jetty Administration</td>
<td>JettyAdminRealm.properties</td>
<td>/jetty/logs/*</td>
<td>Defines administrator security accounts that enable access to the Jetty log files under /usr/OV/www/log</td>
</tr>
</tbody>
</table>

Creating Security Realm User Accounts
Each time you enter a URL for a different realm, you must enter a username and password for an account in that realm. Use the following procedures to create and maintain the accounts.

**Creating NetView Realm Accounts:** Accounts in the NetView realm can be configured either by editing file NetViewRealm.properties, or by using the Web Security Console. See “Defining Security Accounts” on page 48 for information.

In addition to username, password, and role, the NetView realm file specifies each user’s scope. For each user account, create a line in file NetViewRealm.properties using the following format: `username : password,role;scope` For example, `janedoe : m89ko,Operator;Westford_LAN`

**Creating Administrative Realm Accounts:** Accounts in the NetView and Jetty administrative realm must be configured by editing the properties file. The format of both administrative realms is the same.

For each user account, create a line containing a user name, password, and role using the following format: `username : password,role`. For example, `jsmith : qaz321,Administrator`

Working With Logs
Log files provide a record of daemon activity, such as when a daemon was started and stopped, and any errors that occur. There are two types of log files:
- NetView log files, which contain information about NetView daemons including the netviewd daemon.
• Jetty log files, which contain information about the Web Console and Web Server.

Accessing Log Files

Use a browser to access log files as follows:
• Enter the following address:
  http://<hostname>:8090/
  
  where <hostname> is the host name of the machine running the Web server.
• Click either NetView Logs or Jetty Logs.
• Enter a SuperUser user ID and password.

Understanding Web Server Log Files

For UNIX, Web server log files are located at /usr/OV/www/logs. For windows, Web server log files are located at \usr\ov\www\logs. The daily Web server log files are named yyyy_mm_dd.request.log. Log files are retained for 90 days. Edit jetty.xml to change this value.

The web server log uses the Extended Common Log Format. Each line consists of the following nine fields separated by a space. If a field value is not known, the field contains a minus sign.
1. Remote hostname or IP address
2. Remote login name of the user
3. Authenticated username (available when using password protected WWW resources)
4. Date and time of the request
5. HTTP request
6. HTTP response code
7. Number of bytes transferred
8. URL the client was on before requesting this URL
9. User agent, which is the software the client is using

In addition to the Web server logs, there are two other log files: filechecker.log and netviewservlets.log. Each time the Web server is started, the following security configuration files are checked for consistency and the results are logged in filechecker.log:
• /usr/OV/www/conf/NetViewRealm.properties
• /usr/OV/www/conf/ScopeInfo.xml
• /usr/OV/www/webapps/netview/WEB-INF/web.xml
• /usr/OV/www/webapps/netview/warf/*.xml

Note: The Web server will not start if any errors are found in its security configuration files.

Diagnostic output from NetView servlets is logged in netviewservlets.log. Edit /usr/OV/www/classes/log4j.properties to configure the level of diagnostic output that is logged.

For more information about configuring the log4j log files go to http://jakarta.apache.org/log4j/docs/index.html.
Customizing the Web Server

Use the information in this section to customize the Web Server.

Customizing the Web Console Inactive Interval

By default, if the Web Console has not communicated with the Web Server for one hour, a dialog is displayed that indicates that you must restart the Web Console.

Use the following procedure to customize the amount of time the Web Server will wait for communications from the Web Console before you are required to restart the Web Console:

- Edit /usr/OV/www/webapps/netview/WEB-INF/web.xml
- Change the value of the maxInactiveIntervalSec parameter.
- Restart the Web Console.

Changing the Web Server Port

Use the following procedure to change the Web Server port:

- Open /usr/OV/www/conf/jetty.xml in a text editor.
- Find port 8080.
- Change 8080 to another port number.
- Save the file.
- Issue the following commands to restart the Web Server:
  
  ovstop webservice
  ovstart webservice
Index

Special Characters

A
accessibility information viii
accessing logs 51
acknowledging objects 10
ARP cache information 28

B
browser, event 44
browser, MIB 23

C
capability fields 10
check boxes 10
communication lights 9
community name 23
configuration, managing network using the web 31
connectivity, testing 34
connectivity information 35
connectivity testing networks 35
context 19
context menus
  description 7
  event browser 7
  submap explorer 7
customizing
  event browser 44
  web server inactive interval 52
  web server port 52

defining
  roles 48
  scope 49
  users 50
demand poll 33
desktop
  description 2
desktop menu 3
  file menu 4
  help menu 7
  monitor menu 5
  object menu 4
test menu 6
tools menu 6
  window menu 6
diamond symbol 19
disability information viii
displaying
  ARP cache information 28

displaying (continued)
  configured IP services 28
  interfaces 27
  LAN information 29
  MIB interface information 31
  MIB system information 31
  MPLS information 30
  node information 34
  remote SNMP node addresses 27
  routing table information 28
  system information 29
  TCP information 29

event browser
  customizing display 44
  description 44
  filtering 45
  graphing 45
  pausing 45
  starting 44
events
  description 43
  displaying 44
  generation reasons 43
  information provided 44

F
file menu 4
filter, table 8
filtering events 45
find function 18

G
graph MIBs 24
graphing events 45
green status light 9

H
help menu 7

I
icons 14
inactive interval 52
information, accessibility viii
information, disability viii
interfaces 27
internet submap 17
IP services 28
K
keyboard, shortcut keys viii

L
LAN information 29
lights, status 9
loading MIBs 25
logging on to the web console 2
logs
accessing 51
definition 50
filechecker 51
netviewservlets 51
web server 51

M
managing objects 10
maps, submaps 17
menus
context 7
event browser 7
submap explorer 7
description 3
desktop 3
file menu 4
help menu 7
monitor menu 5
object menu 4
test menu 6
tools menu 6
window menu 6
submap explorer 11
MIB
description 21
interface information 31
naming conventions 22
supported versions 21
system information 31
version 23
MIB browser 23
community names 23
graph function 24
setting values 24
walk function 24
MIB loader 25
MIB unloader 25
MIB variable, setting 24
monitor menu 5
MPLS information 30

N
naming conventions, MIB 22
network
connectivity testing 35
performance problems 38
polling 33
network submap 17
node information 34
node submap 18
nodes, determining routes between 35

O
object menu 4
objects
acknowledging and unacknowledging 10
capability fields 10
description 9
finding 18
managing and unmanaging 10
properties 10

P
pausing the event browser 45
performance problems, network 38
ping 34
polling the network 33
port, web server 52
property tips 14

Q
QuickTest 34

R
realms
creating user accounts
administrative realm 50
netview realm 50
definition 50
red status light 9
remote SNMP node addresses 27
roles 48
routes between nodes 35
routing table information 28

S
scope 49
security
starting security console 47
web console 47
security accounts 48
security console
starting 47
security realms 50
segment submap 17
shortcut keys, keyboard viii
starting
security console 47
web console 2
status
propagation 16
rules 16
symbols 15
status filter toolbar 8
status lights 9
status propagation, multiple interfaces 16
submap explorer
description 11
drop-down lists
property tip 14
view 13
menu bar 11
opening 11
tool bar 12
drop-down lists 13
submaps
description 17
hierarchy 17
internet 17
network 17
node 18
segment 17
symbols
behavior 15
description 14
label 15
status 15
types 15
system information 29

T
tables
description 8
filtering 8
using 8
TCP information 29
test menu 6
testing connectivity, Quicktest 34
toolbar
description 7
status filter 8
submap explorer
description 12
toolbar (continued)
submap explorer (continued)
drop-down lists 13
tools menu 6

U
unacknowledging objects 10
unload MIBs 25
unmanaging objects 10
users
defining 50
defining roles 48
defining scope 49
defining security accounts 48
definition 1

V
view drop-down list 13

W
walk, MIB 24
web console
description 1
logging on to 2
security 47
starting 2
web network device management 31
web server
communication lights
description 9
usage notes 9
customizing inactive interval 52
customizing port 52
logs 51
realms 50
window menu 6

Z
zoom function 18