

Avaya Network Management Console User Guide

May 2004

Avaya Network Management Console User Guide

© 2004 Avaya Inc. All rights reserved.

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this document. Avaya disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

Avaya™, P330™, P580/P882™, S8100™, S8300™, S8700™, DEFINITY®, and SMON™ are trademarks of Avaya Inc.

© 2004 Avaya Inc. All rights reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Release 2.002

Table of Contents

Preface viii

The Purpose of This Manual viii
Who Should Use This Manual viii
Organization of This Manual viii

Chapter 1 — Network Management in Standalone Mode. 1

Network Management In Standalone Mode Overview 2
Network Management in Standalone Mode Terms 3
What is Avaya Network Management Server 4
What is Avaya Network Management Console 4
What is a Network Map 5
What is Discovery 6
What is Event Handling 6
What is Remote Access 9

Chapter 2 — Avaya Network Management Server. 10

Introduction to Avaya Network Management Server 10
Starting Avaya Network Management Server 10
Stopping Avaya Network Management Server 12

Chapter 3 — Avaya Network Management Console Introduction . 13

Starting Avaya Network Management Console 13
Avaya Network Management Console User Interface 14
Toolbar 16
Network Tree 17
Network Table 17
Dialog Area 17
Status Bar 17
Using Tooltips 18
Requesting Write Permission 18
Avaya Network Management Console Options 20
SNMP Access Parameters 21
Default SNMP Access Parameters 21
Setting SNMP Access Parameters for IP Ranges 23
Setting Specific IP Parameters 25
Setting Connectivity Polling Parameters 26
Selecting a Default Map 27
Setting Read/Write Defaults 28

Using Avaya Network Management Console Tables 29
Using Avaya Network Management Console Help 29
Opening the Help to the Contents Page 29
Opening the Help to a Topic of Interest 29
Closing Avaya Network Management Console 30

Chapter 4 — Avaya Network Management Console Network Tree 31

Introduction to the Network Tree 31
Using the Network Tree 32
The Subnet View 33
The Device Type View 33
The System View 34
Custom Views 35
Creating Custom Views 36
Modifying Custom Views 36
Deleting Custom Views 37
Adding Branches in Custom Views 37
Modifying Branches in Custom Views 38
Deleting Branches in Custom Views 38
Printing the Network Tree 39
Searching the Tree 40

Chapter 5 — Avaya Network Management Console Network Table41

Using the Network Table 41
Network Table Fields 42
Network Table Colors 43
Managing Objects 44
Manually Adding Devices 45
Modifying Devices 46
Device Parameters 46
Deleting Devices 48

Chapter 6 — Avaya Network Management Console Application Launcher. 49

Launching Device Applications 49
Device Manager 50
Telnet 50
Web Session 50
PING 51
Avaya Site Administrator 51
Avaya MultiSite Administration 53
Avaya Fault and Performance Manager 53
Avaya VAL Manager 54
Avaya Wireless 54
Launching Network-wide Applications 55

Chapter 7 — Network Maps 56

Introduction to Network Maps 56
Managing Network Maps 56
Creating a Network Map 57
Opening a Network Map 58
Saving a Network Map to a Different Name 58
Printing a Network Map 59
Importing Devices into the Network Map 59
Exporting the Network Map 60
CSV File Structure 60

Chapter 8 — Introduction to the Discovery Window 62

Opening the Discovery Window 62
The Discovery User Interface 63
Discovery Toolbar 64
Subnets Table 65
Discovery Dialog Area 66
Discovery Log Area 66
Discovery Status Bar 66
Closing the Discovery Window 66

Chapter 9 — Discovering Your Network 67

Setting Discovery Options 67
Configuring Discovery Method and Range 68
Configuring Discovery's Naming Method 70
Selecting Device Types to Discover 73
Using the Discovery Scheduler 74
Discovering Subnets and Nodes 75
Discovering All Subnets and Nodes 76
Discovering Nodes on Specific Subnets 77
Manually Adding Subnets 79
Modifying Subnets 79
Subnet Parameters 81
Deleting Subnets 82
Using the Discovery Log 82
Configuring Router Access Parameters 83
Saving the Discovery Log 84
Deleting Log Entries 84
Clearing the Discovery Log 85
Manually Discovering System View 85
Using the System View Log 85

Chapter 10 — Introduction to the Event Manager 86

Event Manager Overview 86
Viewing the Event Manager 87
The Event Manager User Interface 87
The Event Log Browser User Interface 87

Event Log Browser Toolbar 88
The Trap Table 89
Status Line 90
The Event Configuration User Interface 90
Event Configuration Toolbar 91
The Event Table 91
Assign Action Form Area 92
Event Configuration Form Area 93
The Action List User Interface 94
Action List Toolbar 95
The Action Table 96
Action Form Area 96
Closing the Event Manager 96

Chapter 11 — Managing Events 97

Managing Traps 97
Trap Log Options 98
Filtering Traps 99
Filtering By Severity Level 99
Filtering By IP Address 100
Filtering By Device Type 101
Filtering By Acknowledged 101
Viewing All Traps 102
Acknowledging Traps 102
Deleting Traps 103
Editing Severity Levels 103
Saving the Trap Table 104
Defining Actions 105
Actions Overview 105
Adding Actions 106
Modifying Actions 107
Action Fields 108
Action Scripts 109
Action Audio Files 110
Deleting Actions 110
Applying Changes to the Action List 110
Action Options 111
Configuring Events 112
Assigning Actions to Events 112
Configuring Event Forwarding 114
Event Forwarding Sources 116
Configuring Forwarding Recipients 116

Chapter 12 — Remote Access 117

Introduction to Remote Access 117
Remote Access and Security 117
Starting a Remote Session 118

Appendix A — Network Management Menus 119

Avaya Network Management Console Menus 119
Avaya Network Management Console File Menu 119
Avaya Network Management Console Edit Menu 120
Avaya Network Management Console View Menu 121
Avaya Network Management Console Actions Menu 121
Avaya Network Management Console Tools Menu 122
Avaya Network Management Console Help Menu 123
Discovery Menus 123
Discovery File Menu 123
Discovery Edit Menu 124
Discovery View Menu 124
Discovery Actions Menu 124
Discovery Help Menu 124
Event Log Browser Menus 125
Event Log Browser File Menu 125
Event Log Browser Edit Menu 125
Event Log Browser View Menu 126
Event Log Browser Help Menu 126
Event Configuration Menus 127
Event Configuration File Menu 127
Event Configuration Edit Menu 127
Event Configuration Tools Menu 127
Event Configuration Help Menu 128
Action List Menus 128
Action List File Menu 128
Action List Edit Menu 128
Action List Tools Menu 129
Action List Help Menu 129

Index 130

Preface

Welcome to Avaya Network Management Console in Standalone Mode. This chapter provides an introduction to the structure and assumptions of this manual. It includes the following sections:

- **The Purpose of This Manual** - A description of the goals of this manual.
- **Who Should Use This Manual** - The intended audience of this manual.

The Purpose of This Manual

This manual contains information needed to use Avaya Network Management Console in Standalone Mode efficiently and effectively.

Who Should Use This Manual

This manual is intended for network managers familiar with network management and its fundamental concepts.

Organization of This Manual

This manual is structured to reflect the following conceptual divisions:

- **Preface** - A description of the manual's purpose, intended audience, and organization.
- **Network Management in Standalone Mode** - An overview of Avaya Network Management Console in Standalone Mode, including a discussion of basic network management concepts.
- **Avaya Network Management Server** - An overview of Avaya Network Management Server including instructions on starting Avaya Network Management Server from your computer.

- **Avaya Network Management Console Introduction** - An introduction to Avaya Network Management Console, including instructions on starting Avaya Network Management Console, a detailed description of Avaya Network Management Console's user interface, and instructions on how to use Avaya Network Management Console's on-line help.
- **Avaya Network Management Console Network Tree** - A description of the Avaya Network Management Console network tree including its default views - the Subnet View and Device Type View - and the System View for networks containing VoIP devices. It also includes instructions on how to create custom views and search the tree.
- **Avaya Network Management Console Network Table** - A description of the Avaya Network Management Console network table and instructions on how to add, delete, and modify objects in the table.
- **Avaya Network Management Console Application Launcher** - Instructions on how to launch device-specific and network-wide applications from Avaya Network Management Console.
- **Network Maps** - An explanation of Network Maps, instructions on how to create, open, save, and print Network Maps, and instructions on importing devices into Network Maps and exporting devices from Network Maps.
- **Introduction to the Discovery Window** - Instructions on how to open and close the Discovery window and a description of the Discovery window.
- **Discovering Your Network** - Instructions on how to use Network Management in Standalone Mode to discover the subnets, nodes and VoIP devices on your network. It also includes an explanation of the Discovery Log and how to configure a router's access parameters including SNMP V1 or SNMP V3 protocol.
- **Introduction to the Event Manager** - Instructions on how to open and close the Event Manager and a description of the Event Manager.
- **Managing Events** - Instructions on how to use the Event Manager to view, filter, and delete events from the Event Log Browser, define event actions, and assign actions to events.
- **Remote Access** - Instructions on running Avaya Network Management Console remotely, including security issues.

1 Network Management in Standalone Mode

This chapter provides an overview of Network Management in Standalone Mode and provides a general description of network management using Network Management in Standalone Mode. This chapter includes the following sections:

- **Network Management In Standalone Mode Overview** - A general description of Network Management in Standalone Mode.
- **Network Management in Standalone Mode Terms** - Definitions of terms used in this documentation.
- **What is Avaya Network Management Server** - A description of the Avaya Network Management Server and its functions.
- **What is Avaya Network Management Console** - A description of Avaya Network Management Console and its functions.
- **What is a Network Map** - A description of Network Maps and their functions.
- **What is Discovery** - A description of Network Management's Discovery feature.
- **What is Event Handling** - A description of events and how to view them using the Event Manager.
- **What is Remote Access** - An description of the remote access capability of Network Management in Standalone Mode.

More detailed information about each of the topics can be found in subsequent chapters.

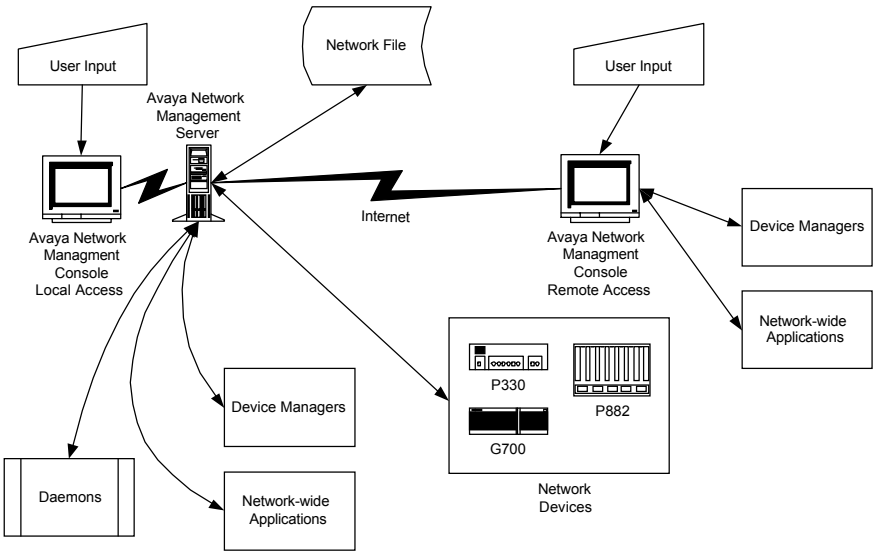
Network Management In Standalone Mode Overview

Network Management in Standalone Mode includes Avaya Network Management Server, and Avaya Network Management Console, an application that allows you to view the devices in your network. Avaya Network Management Console also provides a platform from which you can launch applications to manage network devices and monitor the traffic on your network. In addition, Network Management in Standalone Mode provides a Discovery service which can search your network for devices and an Event Log which reports network events.

Network Management in Standalone Mode uses a client/server architecture allowing multiple users to access the Avaya Network Management Server simultaneously. Web based technology provides a method for accessing and managing your network from any computer with Internet access.

The figure below illustrates the flow of information between the different components that comprise Network Management in Standalone Mode and Network Management applications.

Figure 1-1. Network Management Overview



When Avaya Network Management Server is launched, it runs a number of daemons which poll the network devices listed in the default Network Map to determine their status and updates their colors in the Avaya Network Management Console View Area. Users can manage devices or launch network-wide applications via Avaya Network Management Console. Avaya Network Management Console communicates these requests to Avaya Network Management Server which launches the correct applications. When run remotely, these applications are uploaded from Avaya Network Management Server to the remote station.

Network Management in Standalone Mode Terms

The following table provides a list of terms used in Network Management in Standalone Mode documentation with their descriptions.

Table 1-1. Network Management Terms

Term	Description
Best Name	The best name for a device known to Network Management. For information on defining the method used by Network Management to arrive at the Best Name, refer to "Configuring Discovery's Naming Method" on page 70.
Branch	An intermediate level in the Network Tree. Branches include device types, subnets, and user defined branches in custom views of the network.
Network File	A file where information about the devices in the Network Map is stored.
Network Map	The set of devices that are known to Avaya Network Management Server.
Node	A network device. Nodes include (but are not limited to) switches, hubs, routers, network printers, and computers.
Object	A branch or node in the network.
Poll	A request by an application for information from a device.

What is Avaya Network Management Server

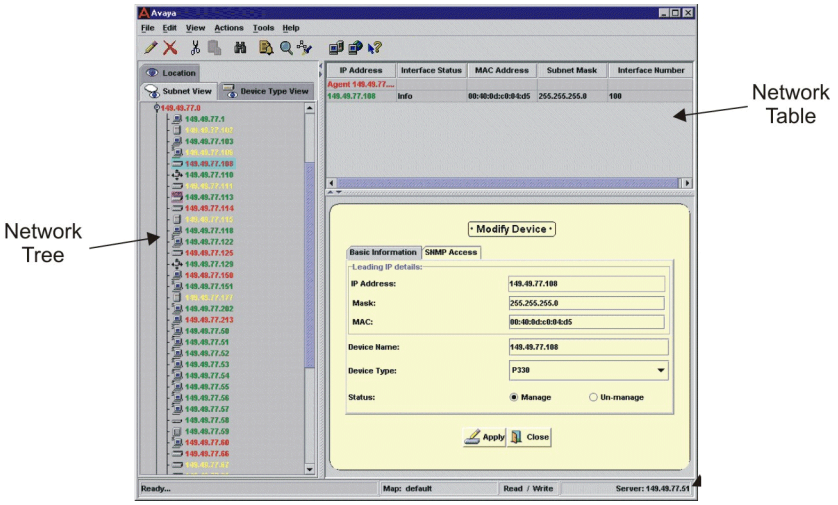
Avaya Network Management Server communicates with the devices in the network via Simple Network Management Protocol (SNMP) V1 or V3. It receives user input via Avaya Network Management Console and updates Avaya Network Management Console with information from the network devices. Avaya Network Management Server runs in the background as a Windows 2000/XP service. The server provides a central address for event reporting. It passes traps to Avaya Network Management Console for display in the Event Log Browser. For more information about event handling and traps, refer to "What is Event Handling" on page 6.

In addition, Avaya Network Management Server allows you to operate Avaya Network Management Console from a remote location. This feature provides a method for managing your network from any computer connected to the Internet. By pointing your web browser to Avaya Network Management Server's IP address, you can access Avaya Network Management Console and manage your network. For more information on running Avaya Network Management Console from a remote location, refer to "What is Remote Access" on page 9.

What is Avaya Network Management Console

Avaya Network Management Console is the user interface to Avaya Network Management Server. It receives information from Avaya Network Management Server and sends the server information input by the user. Avaya Network Management Console displays the devices in the current Network Map using a hierarchical tree. The tree can be organized by subnet or device type, or logically by systems. Additionally, you can create custom views of the network.

Figure 1-2. Avaya Network Management Console



When a device in the Network Tree is selected, information about the selected device appears in the Network Table. You can then modify the device's parameters. Avaya Network Management Console also provides the ability to launch applications that communicate directly with the device. These applications allow you to manage the device via its Command Line Interface (CLI) or Device Manager, and monitor the traffic on the device. For example, if you select an Avaya P330 Device in the Network Table, you can launch Telnet to configure the device via its CLI or launch Avaya P330 Device Manager to configure and monitor the device via its management application and monitor the device using Avaya P330 SMON Manager.

In addition, Avaya Network Management Console allows you to launch network-wide applications such as, Avaya Software Update Manager for updating embedded software, Avaya VLAN Manager for managing VLANs across the entire network, and Avaya SMON Manager for monitoring network traffic.

What is a Network Map

A Network Map consists of all of the devices known to Avaya Network Management Server. The list of devices is stored in the Network File, along with basic information about each device. When Avaya Network Management Console opens, Avaya Network Management Server extracts information about the devices in the Network Map from the Network File. These devices are displayed in the Network Tree.

Devices can be added to the current Network Map using Discovery or the Add Device dialog box. Devices in the Network Map can also be modified. All changes to the Network Map are stored in the Network File.

You can maintain multiple Network Maps by saving individual maps with unique names. The Network Map whose devices are visible in Avaya Network Management Console is the current Network Map.

You can also create a text file that contains the necessary information about each device you want to add to the current Network Map and import the devices listed in the file into the Network Map. For more information on importing devices into the Network Map, refer to "Importing Devices into the Network Map" on page 59.

Avaya Network Management Server can also export the information in the current Network Map to a CSV file. For more information on exporting the device information from the current Network Map, refer to "Exporting the Network Map" on page 60.

What is Discovery

Network Management in Standalone Mode can 'discover' the subnets and nodes on your network. The Discovery tool uses SNMP MIB-II on network nodes to search your network. In addition, you can instruct Discovery to use ICMP Echo (ping) to search the network. You can instruct Discovery to search your entire network for subnets and nodes, limit the search to selected subnets, or update information about the objects in the Network View.

The Discovery window shows a list of the subnets discovered with the number of nodes found in each subnet. You can apply the results of a Discovery to the current Network Map.

What is Event Handling

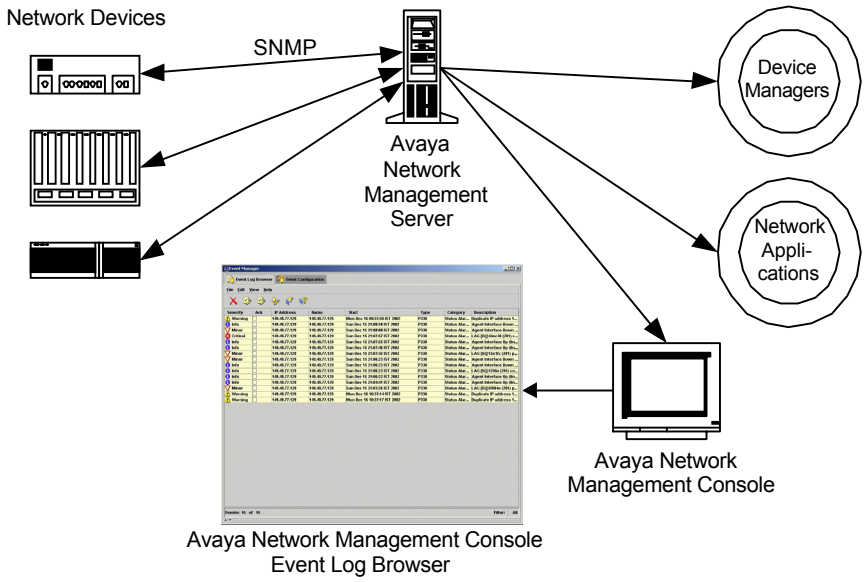
Events are unexpected or extraordinary occurrences in your network. Examples of events include the loss of a port's connection, the insertion or removal of a module from a device, and the failure of a fan or power supply. Network Management provides a method of reporting network events.

*** Note:** For the purposes of this document, the terms 'event' and 'trap' are used interchangeably.

Network Management communicates with device agents using SNMP. Device agents can send traps to Avaya Network Management Server reporting on the status of their ports, modules, etc. The server then passes traps to the relevant managers of the device involved and updates the Event Manager.

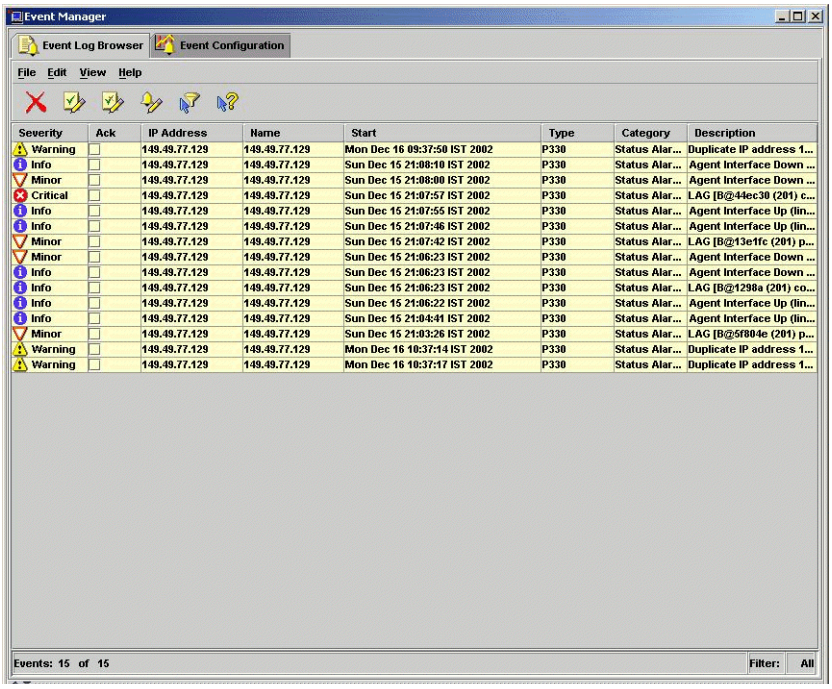
To receive traps using Network Management in Standalone Mode, network devices must be configured to send traps to the Avaya Network Management Server. For information on configuring Avaya LAN and backbone devices to send traps to Avaya Network Management Server, refer to the User Guide or Device Manager User Guide for the devices in your network. The Event Manager maintains a log of all traps received from the devices in the network. These traps can be viewed in the Event Log Browser.

Figure 1-3. Event Handling Flow



Traps are categorized by their severity. Some traps report events that are not problems. An example of this type of trap is the insertion of a module into a device. These traps have a severity level of **Info**. Other traps require more attention, such as the loss of a regular port's connection. Traps of this type have a severity level of **Warning**. Finally, there are traps, such as the failure of a backbone link, which require immediate attention. These traps have a severity level of **Minor**, **Major**, or **Critical**.

Figure 1-4. Event Log Browser



The Event Manager displays all of the traps sent by Avaya Network Management Server. In the Event Manager you can:

- Sort the Event Log Browser by any of its fields.
- Filter the traps displayed and change the severity of selected traps.
- Acknowledge traps to help you remember which traps you have already seen.
- Define the format of the description field.
- Delete traps, signifying that the problem causing the trap was resolved.

In addition, the Event Manager allows you to define event actions. Event actions can include notification via a pop-up, audible, or e-mail message or the running of a script. Actions can be assigned to any network events. You can also limit the action to events from specified sources. This feature enables you to receive immediate notification of important network events.

The Event Manager can also act as a trap surrogate, forwarding all, or selected, traps to other devices.

What is Remote Access

Avaya Network Management Console can be accessed remotely using a web browser. This allows you to manage your network from a computer where Network Management is not installed. When you point your browser to the Avaya Network Management Server's IP address, a Java applet prepares your browser to communicate with Avaya Network Management Server. A welcome screen appears, followed by a password screen. Once you enter a valid user name and password, Avaya Network Management Console opens in a special browser window.

2 Avaya Network Management Server

This chapter provides a detailed description of Avaya Network Management Server. It includes the following sections:

- **Introduction to Avaya Network Management Server** - An introduction to Avaya Network Management Server.
- **Starting Avaya Network Management Server** - Detailed instructions on how to start Avaya Network Management Server.
- **Stopping Avaya Network Management Server** - Detailed instructions on how to shut down Avaya Network Management Server.

Introduction to Avaya Network Management Server

Avaya Network Management Server communicates with network devices. It passes information to Avaya Network Management Console and handles requests to launch applications. In addition, Avaya Network Management Server enables remote sessions of Avaya Network Management Console. Ensure that Avaya Network Management Server is running on the host computer before starting Avaya Network Management Console locally, and that it is running on the remote server before starting a remote session of Avaya Network Management Console.

Avaya Network Management Server can import devices from CSV (Comma Separated Value) files into the Network Map. Avaya Network Management Server can also export the Network Map to a CSV file, for use with other applications, such as a Microsoft Excel.

Starting Avaya Network Management Server

Avaya Network Management Server is a Windows Service. When Windows starts on the server station, Avaya Network Management Server starts automatically. Using Windows' Service Manager, you can configure Avaya Network Management Server so that it does not start automatically.

If Avaya Network Management Server is shut down, you will need to start it manually. To manually start or stop Avaya Network Management Server, you must be logged in to Windows with Administrator privileges. When you log off the computer, Avaya Network Management Server continues running.

To start Avaya Network Management Server:

Select **Start > Programs > Avaya > Network Manager > Start Avaya Network Management Server**.

Or

From a command prompt type **`cvserver start`**.

Or

1. Open Windows' Control Panel.
2. Double-click **Services**.
3. Select **Avaya Network Management Server** from the list of services.
4. Click **Start**.

If Avaya Network Management Server starts successfully, a window opens with the message "`Avaya Network Management Server successfully started.`"

If Avaya Network Management Server is already running on the system, a window opens with the message "`The Avaya Network Management Server is already running.`"

If Avaya Network Management Server cannot start, a window opens with the message "`The Avaya Network Management Server failed to start. Reason: X`", where *X* is the reason Avaya Network Management Server failed to start.

To view the status of Avaya Network Management Server:

Select **Start > Programs > Avaya > Network Manager > Avaya Network Management Server Status**.

Or

From a command prompt type **`cvserver status`**. A window opens with the current status of Avaya Network Management Server (running or not running).

Stopping Avaya Network Management Server

To stop Avaya Network Management Server:

1. Select **Start > Programs > Avaya > Network Manager > Stop Avaya Network Management Server**.

   Or

   From a command prompt type **`cvserver stop`**. A confirmation dialog box opens.

2. Click **Yes**.

Or

1. Open Windows' Control Panel.
2. Double-click **Services**.
3. Select **Avaya Network Management Server** from the list of services.
4. Click **Stop**. Avaya Network Management Server shuts down. If Avaya Network Management Console is open, a window opens with the message that Avaya Network Management Console is closing.

3 Avaya Network Management Console Introduction

This chapter provides an introduction to Avaya Network Management Console. It includes the following sections:

- **Starting Avaya Network Management Console** - Instructions on how to start Avaya Network Management Console.
- **Avaya Network Management Console User Interface** - An introduction to Avaya Network Management Console's user interface, including instructions on how to use the toolbar buttons.
- **Requesting Write Permission** - Instructions on how to request and release Read/Write permissions for a specific Avaya Network Management Console session.
- **Avaya Network Management Console Options** - Instructions on how to set Avaya Network Management Console's options.
- **Using Avaya Network Management Console Tables** - An explanation of symbols used in Avaya Network Management Console tables.
- **Using Avaya Network Management Console Help** - An explanation of the options for accessing on-line help in Avaya Network Management Console.
- **Closing Avaya Network Management Console** - Instructions on how to close Avaya Network Management Console.

Starting Avaya Network Management Console

Avaya Network Management Console can be run locally or via a remote web server. For information on running Avaya Network Management Console via a remote web server, refer to "Starting a Remote Session" on page 118.

The Avaya Network Management Console can configure Network Management's Login Mode for use with SNMPv3. This enables user authentication to limit access to network management. The user authentication can also be used as a mechanism for supplying user credentials for the SNMPv3 messaging engine.

To start a local session of Avaya Network Management Console from Windows:

Double-click the Avaya Network Management Console icon on the Windows desktop.

Or

Select **Start > Programs > Avaya > Network Manager > Avaya Network Management Console**.

Or

Type **`cvconsole`** at a command prompt.

Or

Press **CTRL** + **ALT** + **c**. One of the following occurs:

— If Login Mode is enabled, the Enter User Name and Passwords dialog box opens. Enter your user name and passwords and click **OK**. Avaya Network Management Console opens.

— If Login Mode is disabled, Avaya Network Management Console opens.

For more information about Login Mode, refer to the *Avaya Network Manager User Administration User's Guide*.

Avaya Network Management Console User Interface

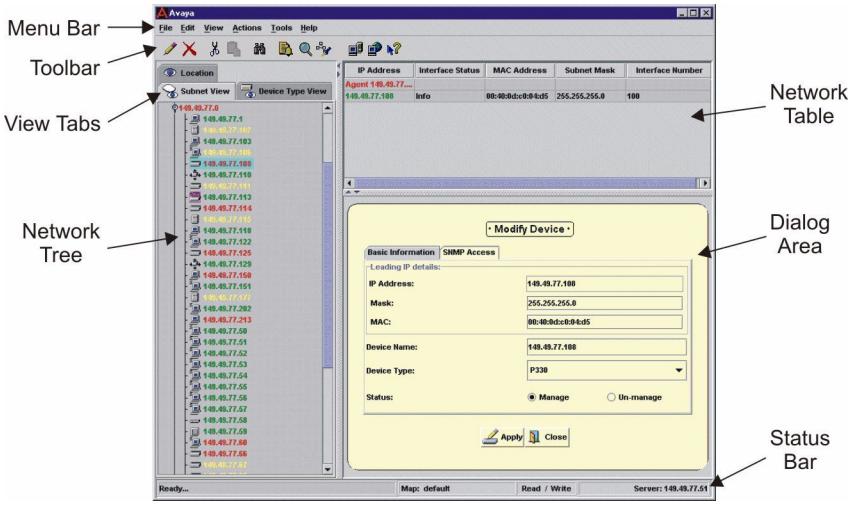
The user interface consists of the following elements:

- **Menu Bar** - Menus for accessing Avaya Network Management Console management functions. For more information on menus, refer to Appendix A, Network Management Menus.
- **Toolbar** - Toolbar buttons for accessing Avaya Network Management Console management functions.
- **Network Tree** - A resizeable window containing a hierarchical representation of the Network Map.
- **View Tabs** - Tabs for switching between the various views of the network.
- **Network Table** - A table where details about the branches and nodes in the Network Tree are displayed.

- **Dialog Area** - A resizeable window where all dialog boxes open.
- **Status Bar** - Displays information about the current Avaya Network Management Console session.

The figure below shows the user interface, with its various parts labeled.

Figure 3-1. Avaya Network Management Console Interface



To resize the three main areas of the user interface, the Network Tree, the Network Table, and the Dialog Area, use the splitter bars and their arrows.

Toolbar

The Toolbar provides shortcuts to the main Avaya Network Management Console functions.

The table below describes the buttons on the Toolbar and gives the equivalent menu options.

Table 3-1. Avaya Network Management Console Toolbar

Button	Description	Menu Item
	Opens the Modify dialog box for the selected object.	**Edit > Modify**
	Deletes the selected object from the Network Map.	**Edit > Delete**
	Cuts the selected object from a custom view to the clipboard.	**Edit > Cut**
	Pastes the object from the clipboard into a custom view.	**Edit > Paste**
	Opens the Find dialog box.	**Edit > Find**
	Opens the Event Manager.	**Actions > Event Manager**
	Launches the device manager for the selected device.	**Tools > Device Manager**
	Opens the Discovery window.	**Actions> IP Discovery**
	Launches a Telnet session to the selected device.	**Tools > Telnet**
	Launches a web session to the selected device.	**Tools > Web**
	Opens context-sensitive help.	**Help > Help On**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

Network Tree

The Network Tree shows either a hierarchical representation of the subnets in the Network Map or a representation of the Network Map grouped by device type or logically organized by systems. You can also create customized views of the Network Map. For more information about the Network Tree, refer to Chapter 4, Avaya Network Management Console Network Tree.

Network Table

The Network Table provides details of the subnets, device types, or devices under the selected branch of the tree. For more information about the Network Table, refer to Chapter 5, Avaya Network Management Console Network Table.

Dialog Area

The area under the Network Table is where all dialog boxes open. This area can be resized by dragging the horizontal splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the Dialog Area.

Status Bar

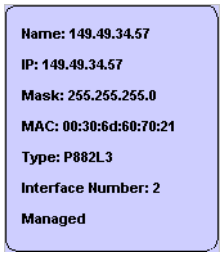
The Status Bar provides information about the Avaya Network Management Console session. It includes the following information:

- Name of the open map.
- Read/Write mode of Avaya Network Management Console.
- IP address/Name of the Avaya Network Management Server.

Using Tooltips

Avaya Network Management Console includes a tooltip feature which allows you to display additional information about devices in the Network Map. To display additional information about a device, place the cursor on the device's icon in the Network Tree or Network Table. After about one second, the tooltip appears.

Figure 3-2. Avaya Network Management Console Tooltip



The tooltip provides the following information about the device:

- **Name** - The Best Name of the device.
- **IP** - The IP address of the device.
- **Mask** - The device's IP subnet mask.
- **MAC** - The device's MAC address.
- **Type** - The device type.
- **Interface Number** - The interface number of the displayed IP address of this device.
- **Management Status** - The device's management status. This can be either **Managed** or **Unmanaged**.

To toggle the tooltips feature, select **View > ToolTip**.

Requesting Write Permission

There are two levels of permission for users logging into Avaya Network Management Console:

- **Read-only** - You are able to view network and devices, but unable to make changes.
- **Read-write** - You are able to both view and make changes to the network and devices.

The following are the assigned permissions at login:

- No read/write console exists - read/write permission is automatically assigned to your console.
- Read/Write console currently exists - your console is assigned read only permission.

*** Note:** Only one console may have read/write permission at any given time.

If your console is opened with read only permission, you can request write permission. The console that currently has read/write permission receives a request from Network Management Console to release the write permission. There is an allotted amount of time in which the console with read/write permission must respond to the request. If the console with read/write permission agrees to the request, or does not refuse the request in the allotted amount of time, the read/write permission is transferred to the requesting console automatically.

For instructions on setting the Timeout value, see "Setting Read/Write Defaults" on page 28.

All functionality is enabled for a console with read/write permission. This is true whether you are running Avaya Network Management Console locally or remotely.

All functions that update the server (i.e., adding and removing a device from the map, or running a discovery process) are disabled on a console with read only permission and all update commands are inactive. If an update dialog box is open while the console is losing write permission, the Apply button of the dialog box becomes inactive until write permission is returned. This also applies to the trap manager.

A console with an open discovery window automatically retains its write permission. Any requests for write permission from a console with an open discovery window are automatically denied.

To request read/write permission:

1. Select **Actions > Get Write Permission.** The Write Permission Request dialog box opens.
2. Click **OK**.
3. If the console that currently has write permission agrees to your request, the Write Permission Received dialog box opens. Click **OK** to receive write permission.

4. If the console that currently has write permission refuses your request, the Write Permission Refused dialog box opens. Click **OK** to proceed with read only permission.

If your console currently has read/write permission and a request is made for write permission by another console, the Remote Request dialog box opens.

To release read/write permission in response to another console's request:

1. Click **OK** to release write permission to the requesting console.
2. To refuse write permission to the requesting console, click **Refuse**.

*** Note:** If you don't click OK or Refuse before the Timeout value expires, write permission is automatically released to the requesting console.

To release read/write permission without a direct request from another console, select **Actions > Release Write Permission**.

Avaya Network Management Console Options

You can use Avaya Network Management Console's Options dialog box to set SNMP Access parameters and connectivity polling parameters and to select a default Network Map.

To open the Avaya Network Management Console Options dialog box, select **File > Options**. The Avaya Network Management Console Options dialog box opens.

The following console options are discussed in this section:

- **SNMP Access Parameters**
- **Setting Connectivity Polling Parameters**
- **Selecting a Default Map**
- **Setting Read/Write Defaults**

SNMP Access Parameters

Using the SNMP Access parameters page of the Avaya Network Management Console Options dialog box, you can set basic SNMP parameters for specific devices, ranges of devices, and all unspecified devices. Avaya Network Management Server recognizes the following SNMP protocols: V1 and V3. SNMP access parameters for SNMP V1 include read and write community properties. For SNMP V3, the SNMP access parameters include a user name defined in the User Administration. For both versions of SNMP, access parameters include timeout and retry values. Each of the three tabs in the SNMP Access parameters page enables you to set SNMP access parameters for different groups of devices.

- **Default** - To configure all devices with IP addresses not included in the other tabs.
- **IP Wildcards** - To configure SNMP access parameters for devices whose IP addresses fall in a specified range and not in the Specific IP's tab.
- **Specific IP's** - To configure SNMP access parameters for specific devices.

When polling a device, Avaya Network Management Server uses the device's SNMP access parameters. The server first checks the Specific IP's list. If the device is listed in the Specific IP's list, the SNMP access parameters for the specific device are used. If not, the server checks the IP Wildcards list. If the device's IP address is in any of the ranges listed in the IP Wildcards list, the SNMP access parameters for the matching range are used. If the device's IP address does not match any of the ranges in the IP Wildcards list, the default SNMP access parameters are used.

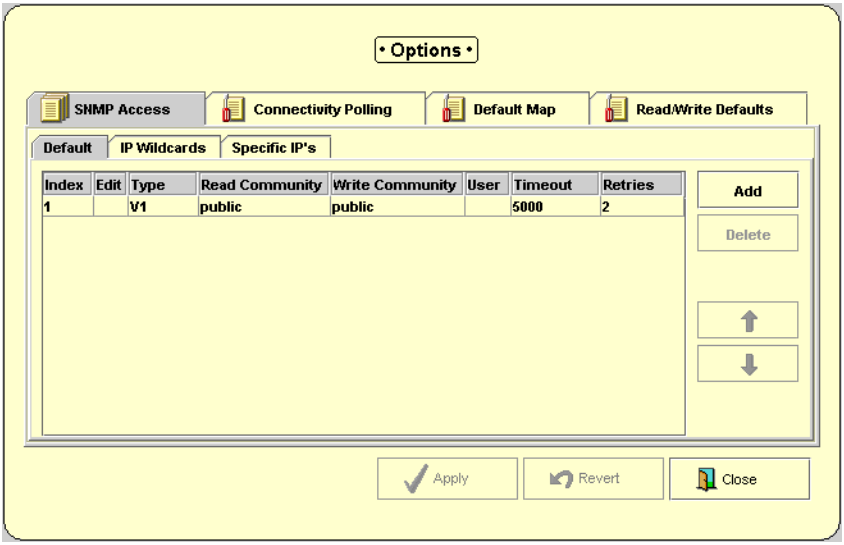
Default SNMP Access Parameters

The Default page enables you to configure multiple default SNMP communities.

If no Specific IP definition and IP Wildcards match the IP address to be polled, Avaya Network Management Server tests the addresses of the devices against the list of definitions in the Default list. The order of the list in the table is important, because the SNMP access parameters of the first rule in the list that matches a device's SNMP access parameters are used for that device.

To view the list of default SNMP access parameters, click the **Default** tab on the SNMP Access page of the Avaya Network Management Console Options dialog box. The Default page appears.

Figure 3-3. Avaya Network Management Console Options Dialog Box - Default Page



To add a new set of SNMP default parameters to the list:

1. Click **Add**. A new row opens in the Default table.
2. Select V1 or V3 (login mode only) from the Type pull-down listbox.
3. If you selected V1 in the Type field, enter read and write community values in their respective fields.
4. If you selected V3 in the Type field, select a user name from the User pull-down listbox. The user name must have been defined in the User Administration Window. For more information, refer to the Network Management User Administration User's Guide.
5. Enter a number in the Timeout [ms] field for the number of milliseconds Avaya Network Management Server will wait for a response when polling a device.
6. Enter a number in the Retries field for the number of times Avaya Network Management Server will try to poll a device.
7. Click **Apply**. The new default SNMP parameters definition is added to the Default table.

To change the position of a row in the Default table:

1. Select a row.
2. Click the arrows to move the row up or down in the table.
3. Click **Apply**. The new row position is saved.

To edit entries in the in the Default table:

1. Click the field you want to edit.
2. Edit the information in the field.
3. Click **Apply**. The changes are saved in the table.

To remove a range from the Default table:

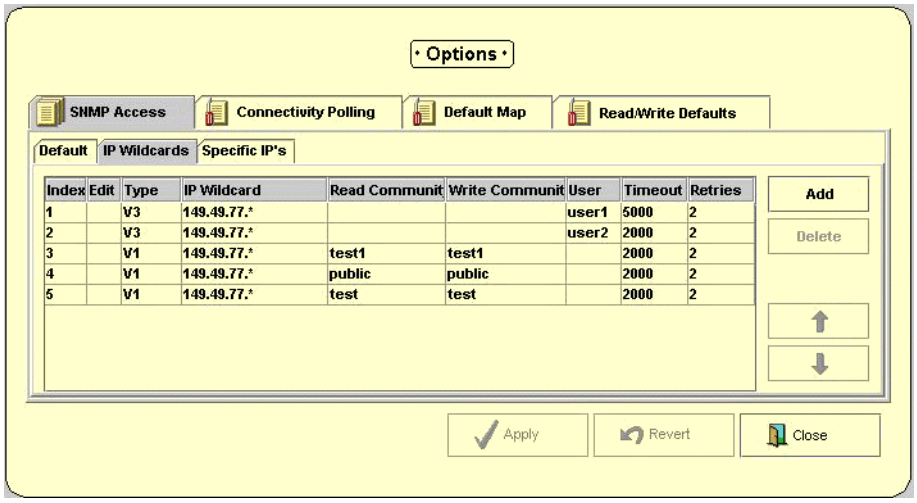
1. Select a row.
2. Click **Delete**.
3. Click **Apply**. The range is deleted from the Default table.

Setting SNMP Access Parameters for IP Ranges

The IP Wildcard page enables you to configure SNMP access parameters for ranges of devices. Avaya Network Management Server tests the IP address of devices to poll against the list of devices in the IP Wildcards list. If the IP address matches a range, the server uses the range's SNMP access parameters when polling the device. The order in the list is important, because the SNMP access parameters of the first range in the list that matches a device's IP address are used for that device.

To view SNMP access parameters for IP ranges, click the **IP Wildcard** tab on the SNMP Access page of the Avaya Network Management Console Options dialog box. The IP Wildcard page appears.

Figure 3-4. Avaya Network Management Console Options Dialog Box - IP Wildcard Page



To add a new IP range to the list:

1. Click **Add**. A new row opens in the IP Wildcards table.

2. Select V1 or V3 (login mode only) from the Type pull-down listbox.
3. Enter an IP Wildcard in the IP Wildcard field.
4. If you selected V1 in the Type field, enter read and write community values in their respective fields.
5. If you selected V3 in the Type field, select a user name from the User pull-down listbox. The user name must have been defined in the User Administration window. For more information, refer to the Network Management User Administration User's Guide.
6. Enter timeout and retry values in their respective fields.
7. Click **Apply**. The new range is added to the IP Wildcards table.

To change the position of a row in the IP Wildcards table:

1. Select a row.
2. Click the arrows to move the row up or down in the table.
3. Click **Apply**. The new position table is applied.

To edit entries in the in the IP Wildcards table:

1. Click the field you want to edit.
2. Edit the information in the field.
3. Click **Apply**. The changes are saved in the table.

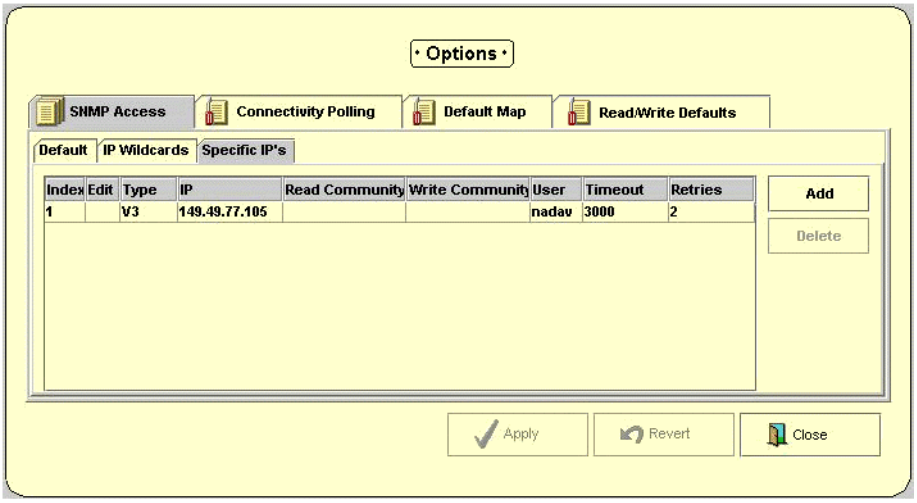
To remove a range from the IP Wildcards table:

1. Select a row.
2. Click **Delete**.
3. Click **Apply**. The range is deleted from the IP Wildcards table.

Setting Specific IP Parameters

To view SNMP access parameters for specific devices, click the **Specific IP's** tab on the SNMP Access page of the Avaya Network Management Console Options dialog box. The Specific IP's page appears.

Figure 3-5. Avaya Network Management Console Options Dialog Box - Specific IP's Page



To add a new device to the list:

1. Click **Add**. A new row opens in the Specific IP's table.
2. Select V1 or V3 (login mode only) from the Type pull-down listbox.
3. Enter the device's IP address in the IP field.
4. If you selected V1 in the Type field, enter read and write community values in their respective fields.
5. If you selected V3 in the Type field, select a user name from the User pull-down listbox. The user name must be defined in the User Administration Window. For more information, refer to the Network Management User Administration User's Guide.
6. Enter timeout and retry values in their respective fields.
7. Click **Apply**. The device is added to the Specific IP's table.

To edit entries in the Specific IP's table:

1. Click the field you want to edit.
2. Edit the information in the field.
3. Click **Apply**. The changes are saved in the table.

To remove a device from the Specific IP's table:

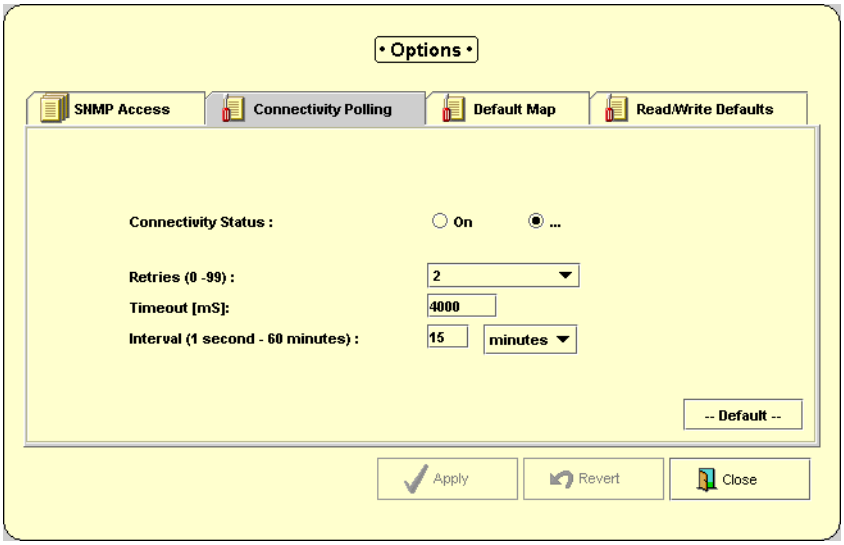
1. Select a device.
2. Click **Delete**.
3. Click **Apply**. The device is deleted from the Specific IP's table.

Setting Connectivity Polling Parameters

Connectivity polling parameters determine whether Avaya Network Management Server will use PING to determine the status of devices that do not support SNMP, the interval between PINGs, and the number of times that Avaya Network Management Server will unsuccessfully PING a node before declaring it to be unreachable. To set default connectivity polling parameters:

1. Click the **Connectivity Polling** tab at the top of the Avaya Network Management Console Options dialog box. The Connectivity Polling page appears.

Figure 3-6. Avaya Network Management Console Options Dialog Box - Connectivity Polling Page



2. Select a Connectivity Status. **On** means that devices will be PINGed. **Off** means that devices will not be PINGed.
3. Enter a number in the Retries field. This is the number of times Avaya Network Management Server will unsuccessfully PING a node before declaring it to be unreachable.

4. Enter a number in the Timeout field. This is the number of milliseconds Avaya Network Management Server will wait for a response when PINGing a node before declaring it to be unreachable.

5. Enter a number in the Interval field and select either **minutes** or **seconds**. This is the amount of time between PINGs.

6. To return the values to the default settings, click **Default**.

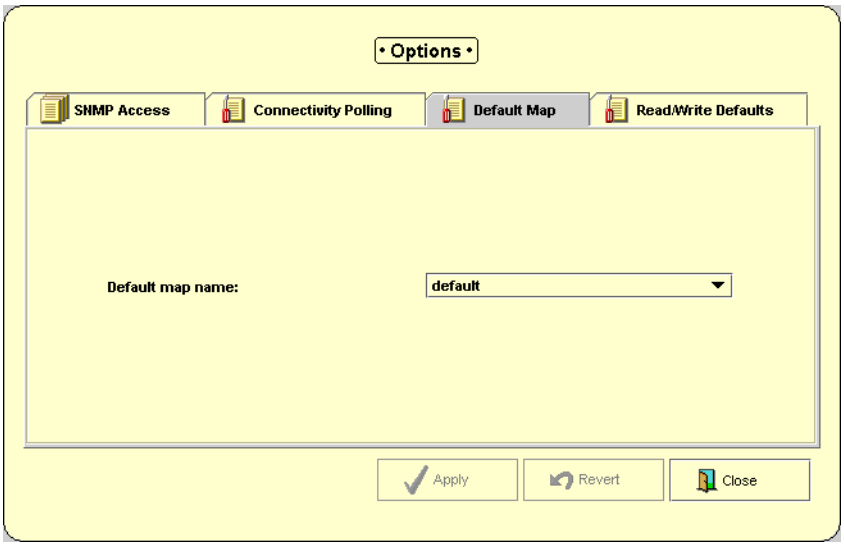
7. Click **Apply**. The network is configured with the new connectivity polling parameters.

Selecting a Default Map

The Default Map page of the Avaya Network Management Console Options dialog box enables you to select the Network Map that is used when Avaya Network Management Server starts. To select a default Network Map:

1. Click the **Default Map** tab at the top of the Avaya Network Management Console Options dialog box. The Default Map page appears.

Figure 3-7. Avaya Network Management Console Options Dialog Box - Default Map Page



2. Select a Network Map from the Default map name pull-down listbox.

3. Click **Apply**. The selected map is now the default Network Map.

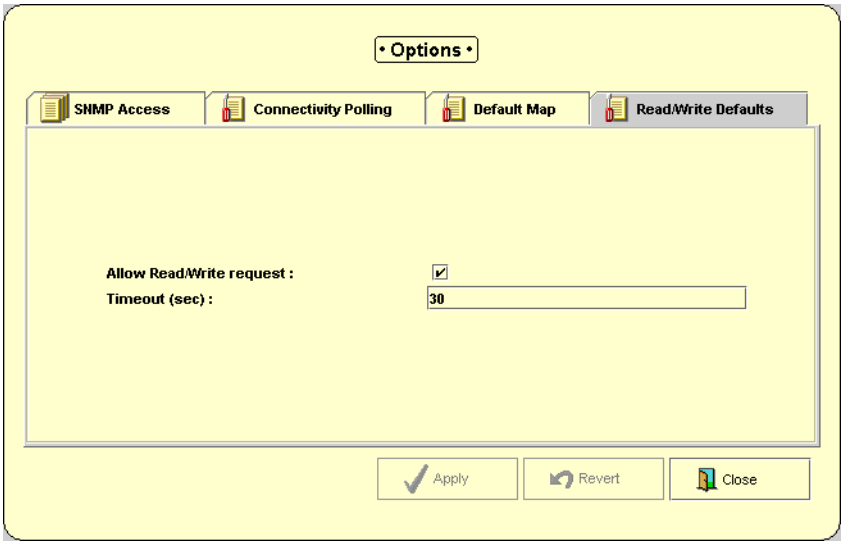
Setting Read/Write Defaults

The Read/Write Defaults page of the Avaya Network Management Console Options dialog box enables you to set the default read/write permissions.

To set read/write defaults:

1. Click the **Read/Write Defaults** tab at the top of the Avaya Network Management Console Options dialog box. The Read/Write Defaults page appears.

Figure 3-8. Avaya Network Management Console Options Dialog Box - Read/Write Defaults Page



2. Check the Allow Read/Write request checkbox to enable a user to request read/write permission. If this checkbox is not checked, then the first console opened receives read/write permission. Any other console window that requests read/write permission is refused.

3. Enter the interval of time in seconds in the Timeout (sec) field that the holder of the read/write permission is allotted to respond to the read/write request.

4. Click **Apply**.

Using Avaya Network Management Console Tables

Avaya Network Management Console informs you of the status of each row in a table. The following table shows symbols that appear at the start of a row, with their corresponding explanations.

Table 3-2. Row Status

Symbol	Explanation
	The row is a new entry.
	The row is to be deleted.
	The row has been modified.

Using Avaya Network Management Console Help

This section explains how to use the on-line help in Avaya Network Management Console. The on-line help can be opened to the contents page or directly to a topic of interest. For more information, refer to:

- Opening the Help to the Contents Page
- Opening the Help to a Topic of Interest

Opening the Help to the Contents Page

To open the help to the contents page, select **Help > Contents**. The on-line help opens to the contents page.

Opening the Help to a Topic of Interest

To open the help directly to a topic of interest:

1. Click .

   Or

   Select **Help > Help On**. The cursor changes to the shape of an arrow with a question mark.

2. Click on a point of interest in Avaya Network Management Console. The help opens to a topic explaining the clicked feature.

Closing Avaya Network Management Console

To close Avaya Network Management Console, select **File > Exit**. Avaya Network Management Console closes.

4 Avaya Network Management Console Network Tree

This chapter provides a detailed description of the Network Tree. It includes the following sections:

- **Introduction to the Network Tree** - An introduction to the Network Tree.
- **Using the Network Tree** - A detailed description of the Network Tree and its hierarchy, and instructions on how to customize the Network Tree.
- **Printing the Network Tree** - Instructions on how to print the Network Tree.
- **Searching the Tree** - Instructions on using the Find feature to search for elements in the Network Tree.

Introduction to the Network Tree

When viewing the network, you may want to view:

- The structure of the network by subnet.
- The information categorized by the different types of devices in the network.
- The system view, which includes the voice elements in a data network, and the relationships between VoIP end points, gatekeepers, and call managers.

Avaya Network Management Console's user interface provides an integrated view of the structure of the network, along with details about specific elements.

In addition, you may want to categorize the devices in your network by other criteria, such as workgroups or location. Avaya Network Management Console allows you to create user defined views of your network and assign devices to custom categories. You can create up to five custom views of your network.

The left side of the user interface is the Network Tree. This provides a hierarchical view of the network. The right side of the user interface contains the Network Table. Together, these views provide details about specific elements in the network.

When an element in the tree is selected, the elements immediately below the selected element appear in the Network Table. Elements in the Network Table are accompanied by fields providing details about the elements.

Using the Network Tree

There are two default views of the Network Tree - the Subnet View and the Device Type View. A third view, the System View, appears for networks containing VoIP devices. In addition, you can define up to five custom views of the network. The Subnet View shows a hierarchical representation of the subnets in the network. The Device Type View shows a view of the network grouped by device type. The System View shows a hierarchical representation of the voice devices in the network. To switch to a different view, click the appropriate tab above the tree.

To expand the view of a contracted element in the tree or to contract the view of an expanded element in the tree:

Double-click the element.

Or

Click the handle next to the element you want to expand or contract.

The following sections describe the following views of the Network Tree:

- **The Subnet View** - A description of the hierarchy and elements of the Subnet View of the network.
- **The Device Type View** - A description of the hierarchy and elements of the Device Type View of the network.
- **The System View** - A description of the hierarchy and elements of the System View of the network.
- **Custom Views** - Instructions on how to create custom views of your network.

The Subnet View

The Subnet View tree shows a hierarchical view of the subnets in the network. The Subnet View of the network contains the following levels:

1. **My Network** - An icon representing the entire network. When the icon representing the network is selected, all subnets appear in the Network Table.
2. **Subnets** - Icons representing the subnets in the network. When an icon representing a subnet is selected, all devices with IP addresses in the selected subnet appear in the Network Table.
3. **Devices** - Each icon representing a device is labeled with the logical name or IP address of the device. When an icon representing a device is selected, the device's interfaces appear in the Network Table.

The Device Type View

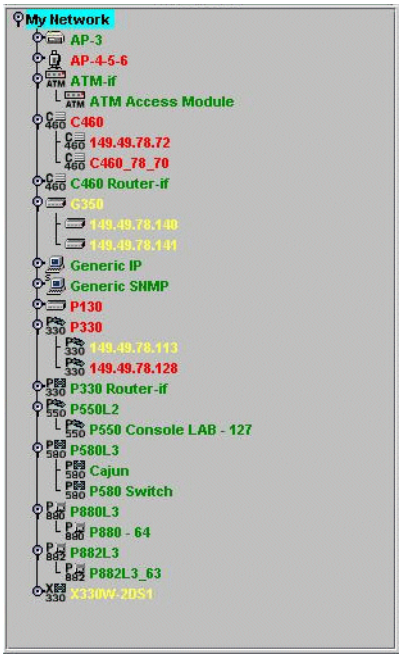
The Device Type View tree shows the network grouped by device type. The Device Type View of the network contains three levels.

1. **My Network** - An icon representing the network. When the icon representing the network is selected, all supported device types in the network appear in the Network Table.
2. **Device Types** - Icons representing all supported device types that appear in the network. When an icon representing a device type is selected, all devices of the selected type appear in the Network Table.
3. **Devices** - Icons representing the devices in the network. Each icon is labeled with the name of the device. When an icon representing a device is selected, the device's interfaces appear in the Network Table.

The System View

The System View tree shows a hierarchical view of the voice devices in the network. The tree is organized with the voice device controllers on the higher levels and the controlled voice devices on lower levels.

Figure 4-1. System View



The root of the System View tree is **My Network**. This icon represents all voice devices in the network. The root splits into two branches - **CM Servers** (Communication Manager Media Servers) and **Other**.

Under the **CM Servers** branch, the tree splits into locations. For each location, Communication Manager Media Servers and voice adjuncts (e.g., Intuity Audix) appear.

For S8700 Communication Manager Media Servers, the tree displays CLANs and VAL boards. Under the CLANs, IP phones with their extension numbers and Media Gateways (MGs) are displayed. Entries for the active and standby Communication Manager Media Servers are also displayed.

For S8300 Communication Manager Media Servers, the tree displays IP phones with their extension numbers and MGs.

The **Other** branch splits into three. The **S8100** branch displays S8100 Devices in the network. The **Unaffiliated** branch displays IP phones with their extension numbers and MGs, whose affiliation with a Communication Manager Media Server cannot be determined. The **Remote Controller** branch displays IP phones with their extension numbers and MGs, whose Communication Manager Media Servers were not discovered in the network.

To refresh the System View tree, select **Actions > System View Discovery**. The System View Discovery runs, and the System View tree is updated This function is not available for stations running Network Management Console remotely.

*** Note:** If the System View tab does not appear, run Discovery or System View Discovery. The tab appears with the discovered devices in the tree.

Custom Views

Avaya Network Management Console allows you to create custom views of your network. This enables you to design a view of your network based on criteria that are important to you. For example, you can design a custom view based on the location of devices or based on the functions that devices perform (i.e., backbone switches, servers, important users, etc.). This can help you focus on a particular set of devices. The following topics are discussed in this section:

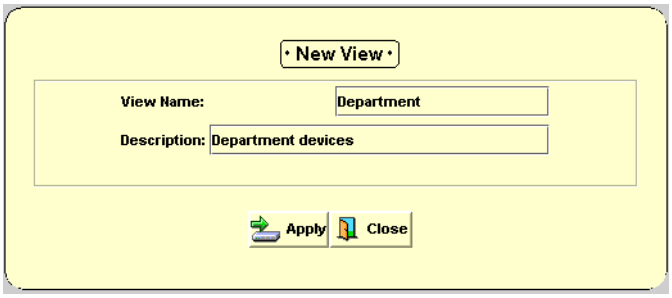
- **Creating Custom Views**
- **Modifying Custom Views**
- **Deleting Custom Views**
- **Adding Branches in Custom Views**
- **Modifying Branches in Custom Views**
- **Deleting Branches in Custom Views**

Creating Custom Views

To create a custom view:

1. Select **File > View > New**. The New View dialog box opens.

Figure 4-2. New View Dialog Box



2. Enter a name for the view in the View Name field.

*** Note:** View names cannot contain periods.

3. Enter a description of the view in the Description field.

4. Click **Apply**. The view is added to Avaya Network Management Console with the top level My Network. All devices in the network are added to a branch labeled Unassigned.

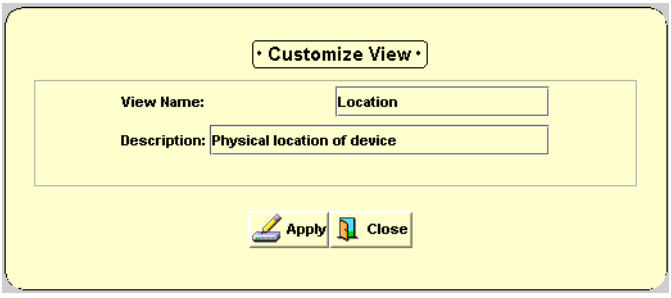
Modifying Custom Views

To modify a custom view:

1. Click the View Tab associated with the custom view you want to modify.

2. Select **Edit > Modify View**. The Customize View dialog box opens.

Figure 4-3. Customize View Dialog Box



3. Change the name for the view in the View Name field.

*** Note:** View names cannot contain periods.

4. Change the description of the view in the Description field.

5. Click **Apply**. The view is modified.

Deleting Custom Views

To delete a custom view of the network:

1. Click the View Tab associated with the custom view you want to modify.
2. Select **Edit > Delete View**. A confirmation dialog box opens.
3. Click **Yes**. The custom view is deleted.

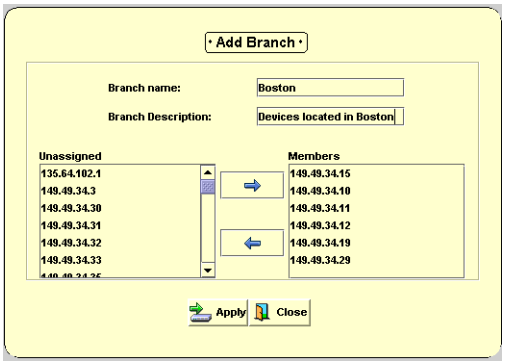
Adding Branches in Custom Views

You can add branches to a custom view of the network and populate the branches with devices or nested branches.

To add branches to a custom view of the network:

1. Select the icon in the Network Tree to which you want to add a branch.
2. Select **File > New > Branch**. The Add Branch dialog box opens.

Figure 4-4. Add Branch Dialog Box



3. Enter a name for the branch in the Branch name field.

*** Note:** Branch names cannot contain periods.

4. Enter a description of the branch in the Branch Description field.
5. Assign devices to the branch using the following procedure:
   - To add devices to the Members list:
     a. Select the devices you want to add to the branch in the Unassigned list.
     b. Click . The devices appear in the Members list.

— To remove devices from the Members list:

a. Select the devices you want to remove from the branch in the Members list.

b. Click . The devices are removed from the Members list.

6. Click **Apply**. The branch and its devices are added to the selected part of the tree.

Modifying Branches in Custom Views

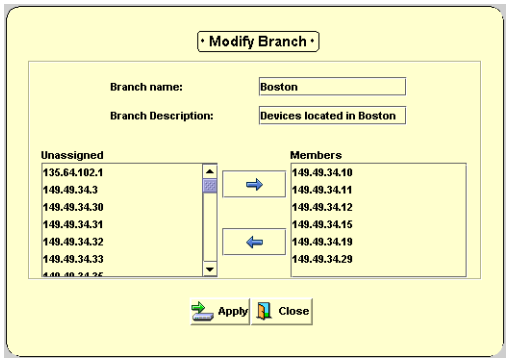
You can add and remove devices from branches in a custom view of the network. To modify a branch of a custom view of the network:

1. Select the branch you want to modify in the Network Tree.

*** Note:** The Unassigned branch cannot be modified.

2. Select **Edit > Modify**. The Modify Branch dialog box opens.

Figure 4-5. Modify Branch Dialog Box



3. Change the name of the branch using the Branch Name field.

*** Note:** Branch names cannot contain periods.

4. Change the comment attached to the view in the Branch Description field.

5. Assign devices to the branch. For instructions on assigning devices to the branch, refer to "Adding Branches in Custom Views" on page 37.

6. Click **Apply**. The branch is modified.

Deleting Branches in Custom Views

You can delete branches from a custom view of the network. To delete a branch of a custom view of the network:

1. Select the branch you want to delete in the Network Tree.

*** Note:** The Unassigned branch cannot be deleted.

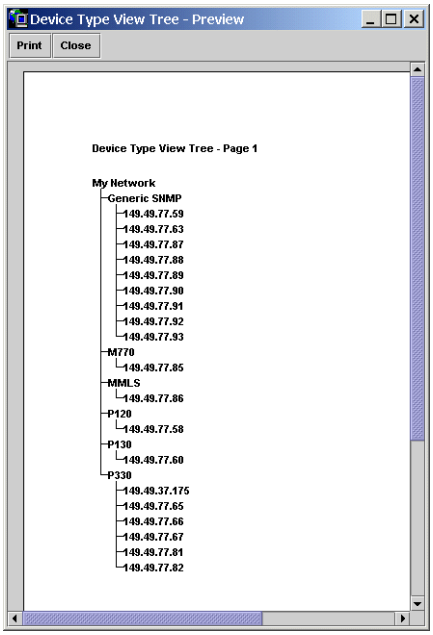
2. Select **Edit > Delete**. A confirmation dialog box opens.
3. Click **Yes**. The branch is deleted, and all its devices appear in the Unassigned list.

Printing the Network Tree

To print the current view of the Network Map, select **File > Print**. The current view of the Network Map is printed.

To view a preview of the printed Network Map, select **File > Print Preview**. The preview of the Network Tree opens.

Figure 4-6. Network Tree Print Preview



To print the Network Map, click **Print**.

To close the Preview window without printing the map, click **Close**.

Searching the Tree

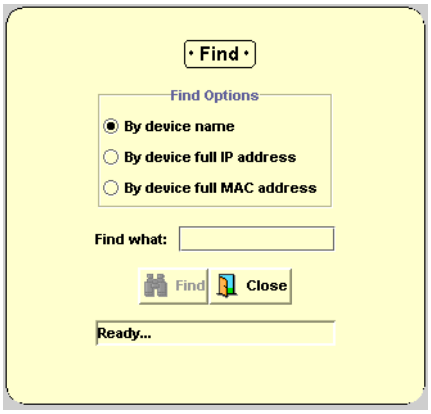
Avaya Network Management Console enables you to search the Network Map for specific elements. To search the Network Map:

1. Click .

   Or

   Select **Edit > Find**. The Find dialog box opens.

Figure 4-7. Find Dialog Box



2. Select one of the Find Options option buttons.
3. Enter the device's name (or part of it), IP address, or MAC address in the Find What field.
4. Click **Find**. The element you searched for appears highlighted in the tree.

To find the next element that matches the search criteria, click **Find Next**. The element you searched for appears highlighted in the tree.

To close the Find dialog box, click **Cancel**.

5 Avaya Network Management Console Network Table

This chapter provides a detailed description of the Network Table. It includes the following sections:

- **Using the Network Table** - A detailed description of the information in the Network Table.
- **Managing Objects** - Instructions on how to manage and unmanage objects in the Network Map.
- **Manually Adding Devices** - Instructions on how to add devices to the Network Map.
- **Modifying Devices** - Instructions on how to modify device parameters.
- **Device Parameters** - A detailed description of device parameters.
- **Deleting Devices** - Instructions on how to delete devices from the Network Map.

Using the Network Table

The Network Table provides information about the objects in the selected branch of the Network Tree. The information in the Network Table varies depending on the element selected in the Network Tree. The following sections provide an explanation of the fields and the color of devices in the Network Table:

- **Network Table Fields**
- **Network Table Colors**

Network Table Fields

The following table lists the columns in the Network Table when the root of the Network Tree is selected in Subnet View.

Table 5-1. Network Table - Subnets

Field	Description
Name	IP address of the subnet.
Status	The status of the subnet.
No. of Devices	The number of registered devices in the subnet.

The following table lists the columns in the Network Table when the root of the Network Tree is selected in Device Type View.

Table 5-2. Network Table - Device Types

Field	Description
Name	The device type.
No. of Devices	The number of registered devices of the device type in the current Network Map.

The following table lists the columns in the Network Table when a subnet or device type is selected in the Network Tree.

Table 5-3. Network Table - Devices

Field	Description
Name	The Best Name of the device known to Avaya Network Management Console.
Device Status	The status of the device.
IP address	The IP address of the device.
Subnet Mask	The subnet mask of the device's IP address.
Device Type	The device type.

The following table lists the columns in the Network Table when a device is selected in the Network Tree.

Table 5-4. Network Table - Interfaces

Field	Description
IP Address	The IP address of the interface.
Interface Status	The status of the interface.
MAC Address	The MAC address of the device.
Subnet Mask	The subnet mask of the device's IP address.
Interface Number	The number of the interface.

Network Table Colors

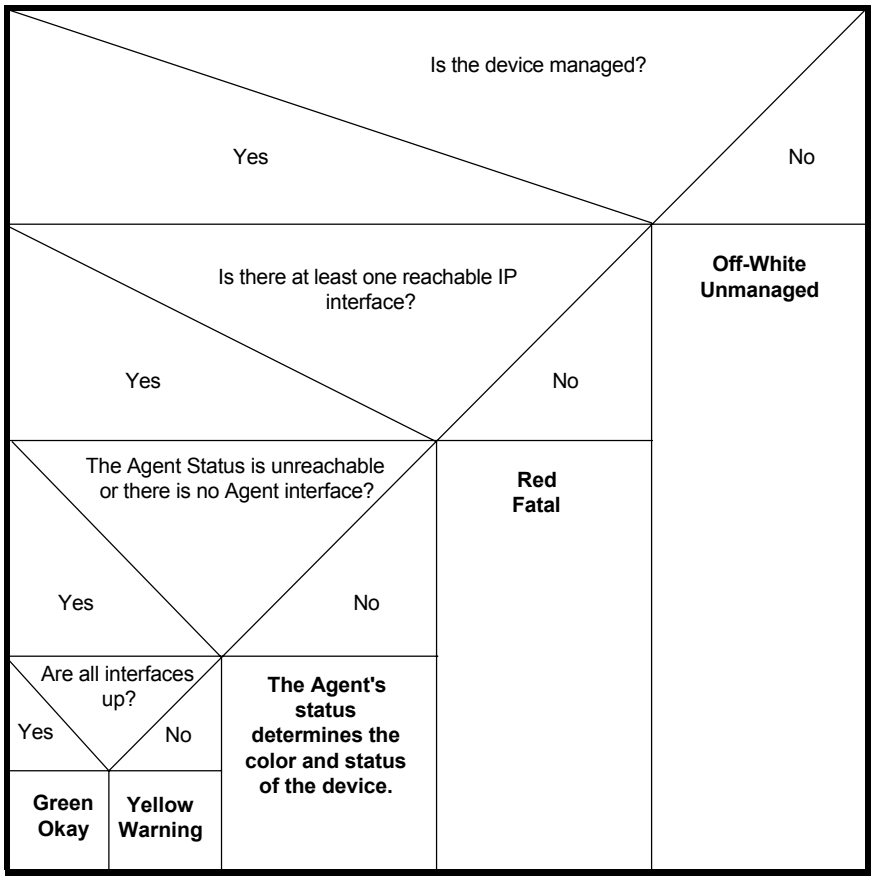
Devices and interfaces viewed in the Network Table are colored based on their status. The following table provides a list of colors and the statuses they represent.

Table 5-5. Device and Interface Status Colors

Color	Device Status
Green	The device/interface status is Okay.
Yellow	The device status is Warning.
Red	The device/interface status is Fatal.
Off-White	The device is unmanaged.
Blue	The agent interface does not respond to SNMP. (Probably caused by an incorrect read community.)

The following diagram outlines the method used by Network Management to determine the color of a device in the Network Table.

Figure 5-1. Device Coloring Method



Managing Objects

The Network Map includes all devices that have been discovered. You can control which of these devices are managed (monitored by Avaya Network Management Server) and which of these devices are unmanaged (not monitored by Avaya Network Management Server). If there are many objects in your Network Map, managing all of the objects may put stress on your network resources. You may also want to keep devices that do not need management, such as workstations, in the Network Map.

When an object in the Network Map is unmanaged, you cannot communicate with the device using Avaya Network Management Console, and the device's color in the Network Table is off-white. In addition, Network Management will not test the device's connectivity status (PING) or receive any traps from an unmanaged device.

To unmanage an object:

1. Select the object in the Network Table.
2. Select **Edit > Unmanage.** The selected object is unmanaged.

To manage an unmanaged object:

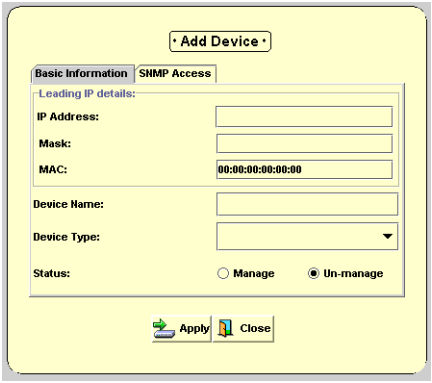
1. Select the object in the Network Table.
2. Select **Edit > Manage.** The selected object is managed.

Manually Adding Devices

You can manually add devices to the Network Map. To manually add a device to the current Network Map:

1. Select **File > New > Device**. The Add Device dialog box opens.

Figure 5-2. Add Device Dialog Box



2. Enter the device's parameters in the dialog box.
3. To edit the device's SNMP parameters, click the **SNMP Access** tab.
4. Enter the SNMP parameters.
5. Click **Apply**. The device is added to the Network Map.

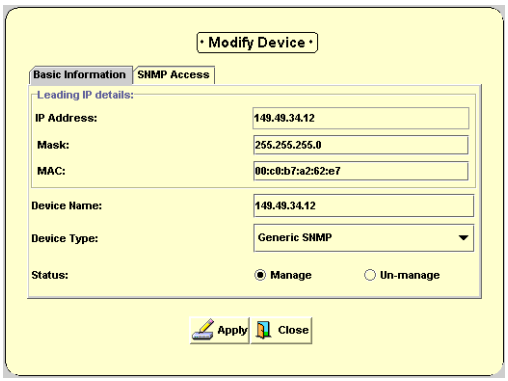
For information on the fields in the Add Device dialog box, refer to "Device Parameters" on page 46.

Modifying Devices

To modify the device or SNMP parameters of a device in the current Network Map:

1. Select a device.
2. Select **Edit > Modify**. The Modify Device Parameters dialog box opens with the selected device's parameters.

Figure 5-3. Modify Device Parameters Dialog Box



3. Modify the parameters in the dialog box.
4. To edit the device's SNMP parameters, click the **SNMP Access** tab.
5. Enter the SNMP parameters.
6. Click **Apply**. The parameters are modified.

For information on the fields in the Modify Device Parameters dialog box, refer to "Device Parameters" on page 46.

Device Parameters

The following table provides a list of the parameters in the Add Device and Modify Device dialog boxes.

Table 5-6. Device Parameters

Parameter	Description
IP Address	IP address of the device.
Mask	The IP subnet mask.
MAC	The MAC address of the agent.

Table 5-6. Device Parameters (Continued)

Parameter	Description
Device Name	The name or best name of the device.
Device Type	Type of device. Possible types are: • **Auto Discover** - Avaya Network Management Server polls the device to determine the device type. • *Avaya Device* - Where *Avaya Device* is the name of an Avaya Device. • **Generic SNMP** - For other SNMP Devices. • **Generic IP** - For IP Devices that do not use SNMP. • *Other Device* - Where *Other Device* is another recognized device type.
Status	The managed status of the device. Possible statuses are: • **Manage** - The device is managed by Network Management. • **Un-manage** - The device is not managed by Network Management.
SNMP	The SNMP protocol. Possible SNMP protocols are: • **Snmp V1** • **Snmp V3**
Read Community	The device's read community. Only applicable for SNMP protocol V1.
Write Community	The device's write community. Only applicable for SNMP protocol V1.
User	A user name as defined in the User Administration. Only applicable for SNMP protocol V3.
Retries	The number of times an application will poll a device without receiving a response before timing out.
Timeouts (milliseconds)	The number of milliseconds an application will poll a device without receiving a response before timing out.

Deleting Devices

To delete selected devices from the current Network Map:

1. Select a device.
   — To select more than one device, press **CTRL** while selecting additional devices.
2. Select **Edit > Delete**. A confirmation dialog box appears.
3. Click **Yes**. The selected device is deleted from the Network Map.

6 Avaya Network Management Console Application Launcher

This chapter provides detailed instructions on launching applications from Avaya Network Management Console. It includes the following sections:

- **Launching Device Applications** - Instructions on launching device-specific applications from Avaya Network Management Console.
- **Launching Network-wide Applications** - Instructions on launching network-wide applications from Avaya Network Management Console.

For information specific to an application, refer to the application's User Guide or on-line help.

Launching Device Applications

This section provides instructions on launching the following device specific applications from Avaya Network Management Console:

- **Device Manager**
- **Telnet**
- **Web Session**
- **PING**
- **Avaya Site Administrator**
- **Avaya MultiSite Administration**
- **Avaya Fault and Performance Manager**
- **Avaya VAL Manager**
- **Avaya Wireless**

Device Manager

To launch the Device Manager for a managed device in the current Network Map:

1. Select the device.
2. Click .

   Or

   Select **Tools > Avaya Device Manager**.

Or

Double-click the device. The Device Manager for the selected device opens.

*** Note:** When running a remote session of Avaya Network Management Console, Device Manager can only be launched for devices that can be managed remotely.

Telnet

Telnet can be used to access the Command Line Interface (CLI) of a network device. This allows you to change the device's setup. If you are running Avaya Network Management remotely, you can use Telnet to manage devices whose Device Managers cannot be run remotely.

To launch a Telnet session to a managed device in the current Network Map:

1. Select the device.
2. Click .

   Or

   Select **Tools > Telnet**. A Telnet session opens to the device.

Web Session

Web Sessions can be used to manage devices that support Web Sessions over the Internet. These devices include some Avaya devices. In addition, non-Avaya devices that support Web Sessions can be managed from both local and remote sessions of Avaya Network Management.

To launch a Web Session:

1. Select a device that supports Web Sessions.
2. Click .

   Or

   Select **Tools > Web**. A Web Session opens to the device.

PING

The PING application enables you to PING devices from within Avaya Network Management Console. If you are having a problem communicating with the device via SNMP, try to ping the device. This will help you to determine whether the cause of the problem is related to the device's SNMP parameters or to a general communication problem with the device.

To PING a managed device:

1. Select the device.
2. Select **Tools > Ping**. The results of the PING appear in the Command window.

Avaya Site Administrator

Avaya Site Administrator (ASA) is a system management tool designed for user administration and maintenance of IP enabled Avaya Communication Manager telephony systems and IP phones. ASA also provides terminal emulation capabilities for general administration of other types of voice devices.

*** Note:** ASA is part of Avaya Integrated Management.

Avaya Network Manager Console in Standalone Mode will recognize Media Servers and IP phones that can be managed by ASA. If you have ASA installed on your computer, you can launch ASA to manage an appropriate device from Avaya Network Management Console.

To launch the main ASA window, select **Tools > Avaya Site Administration** with no telephony device selected. The main ASA window opens.

To launch ASA on an appropriate switch, gateway, or IP phone:

1. Select an appropriate managed telephony device.
2. Select **Tools > Avaya Site Administration**.

   Or

   Double-click an appropriate managed telephony device.

   — If you selected a Communication Manager Media Server, ASA connects to the device and opens the appropriate form for the server.

   — If you selected an IP phone, ASA connects to the Communication Manager Media Server controlling the selected phone and opens the appropriate form for the phone's extension.

Avaya MultiSite Administration

Avaya MultiSite Administration is a system management tool designed for configuration of Communication Manager Media Servers and Media Gateways, and upgraded DEFINITY® servers.

*** Note:** Avaya MultiSite Administration is part of Avaya Integrated Management.

To launch the main Avaya MultiSite Administration window:

Select **Tools > Avaya MultiSite Administration** with no device selected. The main Avaya MultiSite Administration window opens.

To launch Avaya MultiSite Administration on an appropriate device:

1. Select an appropriate managed device.
2. Select **Tools > Avaya MultiSite Administration**. Avaya MultiSite Administration opens on the selected device.

Avaya Fault and Performance Manager

Avaya Fault and Performance Manager is a system management tool designed for monitoring the performance and viewing faults on Avaya Media Servers and Gateways, and upgraded DEFINITY® servers.

*** Note:** Avaya Fault and Performance Manager is part of Avaya Integrated Management.

To launch the main Avaya Fault and Performance Manager window, select **Tools > Avaya Fault and Performance Manager** with no device selected. The main Avaya Fault and Performance Manager window opens.

To launch Avaya Fault and Performance Manager on an appropriate device:

1. Select an appropriate managed device.
2. Select **Tools > Avaya Fault and Performance Manager**. Avaya Fault and Performance Manager opens on the selected device.

Avaya VAL Manager

Avaya VAL Manager is a system management tool designed for Voice Announcements over LAN (VAL) on Avaya switches that support VAL.

*** Note:** Avaya VAL Manager is part of Avaya Integrated Management.

To launch the main Avaya VAL Manager window, select **Tools > Avaya VAL Manager** with no device selected. The main Avaya VAL Manager window opens.

To launch Avaya VAL Manager on an appropriate VAL board:

1. Select an appropriate VAL board.
2. Select **Tools > Avaya VAL Manager**.

   Or

   Double-click an appropriate managed device. Avaya VAL Manager opens on the selected device.

Avaya Wireless

Avaya Wireless is a system management tool designed for configuration of Avaya Wireless (AP 1 and 2) devices.

To launch Avaya Wireless on an appropriate Access Point (AP) device:

1. Select an appropriate managed device.
2. Select **Tools > Avaya Wireless**.

   Or

   Double-click an appropriate managed device. Avaya Wireless opens on the selected switch.

Launching Network-wide Applications

To launch a network-wide application, select **Tools >** *Application Name*, where *Application Name* is the name of the network-wide application you want to run. The network-wide application opens.

*** Note:** Avaya SMON Manager is only available with the purchase of an SMON license. For more information on SMON licenses, refer to Appendix B, *Setting up the SMON License* in the *Avaya SMON Manager User Guide*.

*** Note:** Not all network-wide applications can be launched when running a remote session of Avaya Network Management Console.

If you configured Network Management's Login Mode for use with SNMPv3, you are prompted to log in to each network-wide application when it starts up.

7 Network Maps

This chapter provides a detailed description of Network Maps in Avaya Network Management Console. It includes the following sections:

- **Introduction to Network Maps** - An introduction to Network Maps.
- **Managing Network Maps** - Instructions on how to create, open, save, and print Network Maps.
- **Importing Devices into the Network Map** - Detailed instructions on importing devices into the Network Map.
- **Exporting the Network Map** - Detailed instructions on exporting the devices in a Network Map to a file.

Introduction to Network Maps

The Network Map is the set of devices that can be viewed in Avaya Network Management Console. The Network File provides a method of storing information about the devices in a Network Map. You can create a number of Network Maps and save each one to a separate file. This can be useful in maintaining backups when major changes are made to the Network Map. When changes are made to a Network Map, they are saved in the map's Network File.

Devices can be imported into a Network Map from a text file. In addition, you can export the Network Map for use with other applications. For more information on exporting the current Network Map, refer to "Exporting the Network Map" on page 60.

Managing Network Maps

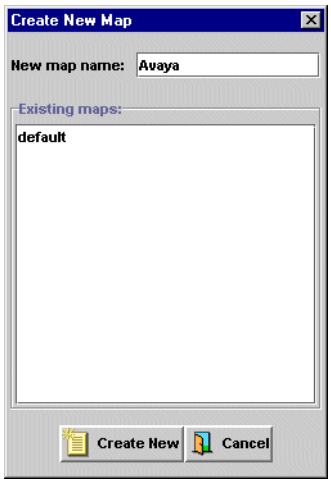
The following sections provide instructions for creating, opening, saving, and printing Network Maps.

Creating a Network Map

To create a new Network Map:

1. Select **File > New > Map**. The Create New Map dialog box opens.

Figure 7-1. Create New Map Dialog Box



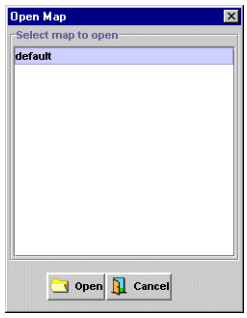
2. Enter a name for the file in the New map name field.
3. Click **OK**. A new Network Map is created.
4. Add subnets and devices to the Network Map using one of the following methods:
   - **Discovery** - For more information, refer to "Discovering Subnets and Nodes" on page 75.
   - **Manual Entry** - For more information, refer to "Manually Adding Devices" on page 45.
   - **Importing** - For more information, refer to "Importing Devices into the Network Map" on page 59.

Opening a Network Map

To open a Network Map:

1. Select **File > Open > Map**. The Open Map dialog box opens.

Figure 7-2. Open Map Dialog Box



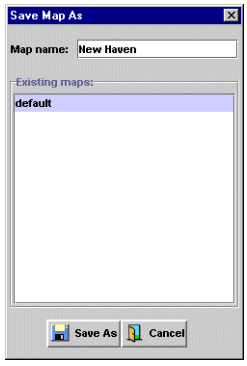
2. Select a Network Map from the list.
3. Click **Open**. The selected Network Map opens.

Saving a Network Map to a Different Name

To save a Network Map to a different Name:

1. Select **File > Save As**. The Save Map As dialog box opens.

Figure 7-3. Save Map As Dialog Box



2. Enter a name for the file in the Map Name field.
3. Click **Save As**. The Network Map is saved.

Printing a Network Map

To print a Network Map, select **File > Print**. The Network Map is printed.

Importing Devices into the Network Map

Devices can be imported from a text file into the Network Map. The information for each device must be on a single line, with the various information fields for the device separated by commas. This file is referred to as a Comma Separated Value (CSV) file.

The following is an example of rows in a CSV file:

```
.1.3.6.1.4.1.23.1.6.4.11,149.49.32.253,149.49.48.215,255.255.255.0,00:C0:4F:91:1A:26,Days
2,Days2,30,5
.1.3.6.1.4.1.23.1.6.4.11,149.49.32.184,149.49.48.91,255.255.255.0,00:C0:3E:11:B3:14,Venus,,
,45,6
.1.3.6.1.4.1.23.1.6.4.11,149.49.32.251,149.49.43.210,255.255.0.0,00:C0:1F:01:C2:11,Lazy23,
Lazy23,20,3
,149.49.48.204,255.255.255.0,00:A7:F2:11:BA:34,Oddball,Harpo,Harpo,60,7
```

*** Note:** The information fields of the CSV file will be different depending on whether SNMP V1 or V3 is active.

For information on the structure of CSV files of devices to import to a Network Map, refer to "CSV File Structure" on page 60.

To import devices from a CSV file into the current Network Map:

1. Select **File > Import**. A standard file browser opens.
2. Browse to the CSV file.
3. Click **Open**. The devices in the CSV file are imported into the current Network Map.

If a device listed in the file has the same IP address as a device already existing in the Network Map, the device details in the CSV file overwrite those in the Network Map. If a syntax error exists in the CSV file, the import stops after it has processed all the devices listed before the error.

Exporting the Network Map

The current Network Map can be exported to CSV files for use with applications, such as Microsoft Excel. For information on the structure of CSV files of exported Network Maps, refer to "CSV File Structure" on page 60.

To export devices from the current Network Map to a CSV file:

1. Select **File > Export > Map**. A standard file browser opens.
2. Browse to the directory to which you want to save the file.
3. Enter a name for the CSV file in the Name field.
4. Click **Save**. The current Network Map is exported to the specified CSV file.

CSV File Structure

The structure of the information in the CSV file is described in the following table.

Table 7-1. CSV Network File Syntax

Field	Description
Device Type SysOId	The SysOId that defines the type of device. *** Note:** For IP Devices that do not use SNMP, this field is empty.
IP Address	The IP address of the device.
IP Subnet Mask	The IP subnet mask.
Agent MAC Address	The MAC address of the agent.
Name	The name or best name of the device.
Read Community	The read community of the device. Only applicable for SNMP protocol V1.
Write Community	The write community of the device. Only applicable for SNMP protocol V1.
User	A user name as defined in the User Administration. Only applicable for SNMP protocol V3.

Table 7-1. CSV Network File Syntax (Continued)

Field	Description
Retries	The number of times an application will poll the device without receiving a response before timing out.
Timeouts	The number of milliseconds an application will poll the device without receiving a response before timing out.

8 Introduction to the Discovery Window

This chapter provides an introduction to the Discovery window. It includes the following sections:

- **Opening the Discovery Window** - Instructions on how to open the Discovery window.
- **The Discovery User Interface** - A description of the Discovery window.
- **Closing the Discovery Window** - Instructions on how to close the Discovery window.

Opening the Discovery Window

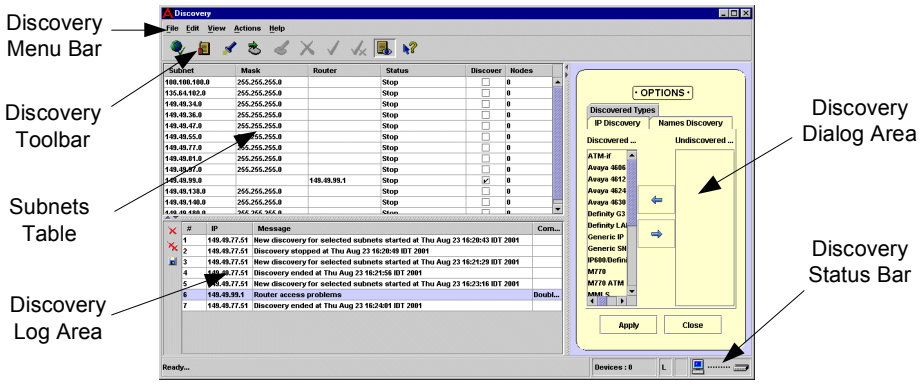
To open the Discovery window:

Click .

Or

Select **Actions > Discovery**. The Discovery window opens.

Figure 8-1. Discovery Window



The Discovery User Interface

The Discovery user interface consists of the following elements:

- **Discovery Menu Bar** - Menus for accessing Discovery functions. For more information on Discovery menus, refer to Appendix A, Network Management Menus.
- **Discovery Toolbar** - Toolbar buttons for accessing Discovery functions.
- **Subnets Table** - A table of subnets listed in the Network View and discovered subnets.
- **Discovery Dialog Area** - A resizeable window where all dialog boxes open.
- **Discovery Log Area** - A resizeable window where the Discovery Log opens.
- **Discovery Status Bar** - Displays information about the current Discovery session.

Discovery Toolbar

The table below describes the buttons on the Discovery Toolbar and gives the equivalent menu options.

Table 8-1. Discovery Toolbar

Button	Description	Menu Item
	Saves the current Discovery settings.	**File > Save As**
	Opens the Discovery Options dialog box.	**File > Options**
	Starts a Discovery based on the default routers of the management station and the contents and settings of the Subnet Table.	**Actions > Discover**
	Stops a Discovery process.	**Actions > Stop Network Discovery**
	Adds a subnet to the Subnet Table.	**Edit > Add**
	Opens the Modify Subnet dialog box.	**Edit > Modify**
	Deletes the selected subnet from the Subnet Table.	**Edit > Delete**
	Checks the Discover field for the selected subnet.	**Edit > Select**
	Unchecks the Discover field for the selected subnet.	**Edit > Unselect**
	Opens the Discovery Log.	**View > Discovery Log**
	Opens context-sensitive help.	**Help > Help On**

Subnets Table

The Subnets Table contains a list of subnets from the following sources:

- The current Network Map.
- Subnets added to the Subnets Table manually by the user.
- Subnets found in a Discovery.

The following table provides a list of the fields in the Subnets Table and provides an explanation of each field.

Table 8-2. Subnets Table Fields

Field Name	Description
Subnet	The IP address of the subnet.
Mask	The subnet mask.
Router	The IP address of the subnet's router.
Status	The status of Discovery on this subnet. Possible statuses are: • **Stop** - The Discovery was stopped by the user. • **In progress** - Discovery on this subnet is currently in progress. • **Done** - Discovery on this subnet has been completed.
Discover	A checkbox determining whether or not Discovery should search for nodes on the subnet. • Checked: Discovery will search for nodes on this subnet. • Unchecked: Discovery will not search for nodes on this subnet.
Nodes	The numbers of nodes discovered in the subnet.

To sort the Subnet Table by one of the fields, click the field's column header. To reverse the sort order, click the column header again.

Discovery Dialog Area

The area at the right of the Subnets Table is where all dialog boxes open. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the Dialog Area. When no dialog box is open, the Dialog Area disappears and the Subnets Table expands to take its place.

Discovery Log Area

The area under the Subnets Table is where the Discovery Log opens. This area can be resized by dragging the horizontal splitter bar with the mouse. When the Discovery Log is closed, the Log Area disappears and the Subnets Table expands to take its place.

Discovery Status Bar

The Discovery Status Bar provides information about the current Discovery including:

- **Current Discovery Phase** - The phase of the current Discovery. Possible phases are:
  - **Ready** - There is no Discovery in progress.
  - **Discovering Devices** - Discovery is searching for subnets and routers.
- **Devices** - The total number of devices found in the current Discovery.
- **Entries in the Log** - If there are entries in the Discovery Log, the letter '**L**' appears in the Status Bar. For information on viewing the Discovery Log, refer to "Using the Discovery Log" on page 82.
- **Changes Found** - If Discovery found subnets and/or nodes that are not in the current Network File, the letter '**D**' appears in the Status Bar.

Closing the Discovery Window

To close the Discovery window, select **File > Exit**. The Discovery window closes.

9 Discovering Your Network

This chapter provides detailed instructions on how to use Avaya Network Management Console's Discovery feature. It includes the following sections:

- **Setting Discovery Options** - Instructions on how to set Discovery options.
- **Discovering Subnets and Nodes** - Instructions on how to discover the subnets and devices in your network.
- **Using the Discovery Log** - A description of the information in the Discovery Log and instructions on how to handle problems accessing routers, save the Discovery Log, and delete log entries.
- **Manually Discovering System View** - Instructions on how to discover the VoIP devices in your network.
- **Using the System View Log** - Instructions on how to open the System View Log.

*** Note:** All toolbar buttons and menu items referred to in this chapter are in the Discovery Window.

Setting Discovery Options

The Discovery Options dialog box allows you to configure Discovery options. Using the Discovery Options dialog box, you can configure the method and range of Discovery, the method Discovery uses for selecting names for discovered nodes, and the types of nodes Discovery will find. The following topics are discussed in this section:

- **Configuring Discovery Method and Range**
- **Configuring Discovery's Naming Method**
- **Selecting Device Types to Discover**

To configure Discovery options:

Click  in the Discovery toolbar.

Or

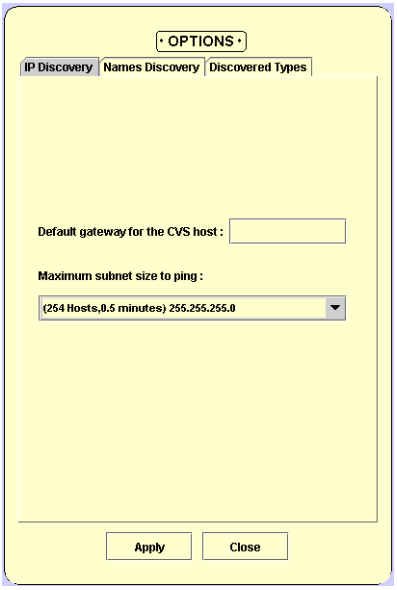
Select **File > Options** in the Discovery menu bar. The Discovery Options dialog box opens.

Configuring Discovery Method and Range

To configure the method and range of Discovery:

1. Click the **IP Discovery** tab at the top of the Discovery Options dialog box. The IP Discovery page of the Discovery Options dialog box appears.

Figure 9-1. IP Discovery Options Dialog Box



2. Configure the IP Discovery options.
3. Click **Apply**. IP Discovery Options are configured.

The following table provides a list of the fields in the IP Discovery page of the Discovery Options dialog box.

Table 9-1. IP Discovery Options

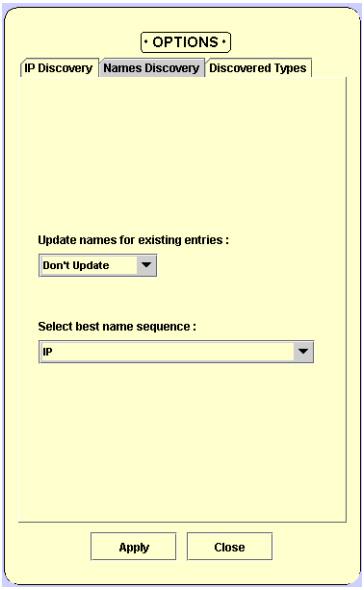
Field Name	Description
Default gateway for the CVS host	The IP address of the default gateway used for Discovery. By default, this is the Gateway IP Address for the Network Management management station.
Maximum subnet size to ping	The mask applied to the subnet address to determine the number of IP addresses in the subnet. Possible values are: • **Disable Ping** (Ping is not used to discover devices.) • **255.255.255.252** (2 hosts) • **255.255.255.248** (6 hosts) • **255.255.255.240** (14 hosts) • **255.255.255.224** (30 hosts) • **255.255.255.192** (62 hosts) • **255.255.255.128** (126 hosts) • **255.255.255.0** (254 hosts) • **255.255.254.0** (510 hosts) • **255.255.252.0** (1022 hosts) • **255.255.248.0** (2046 hosts) • **255.255.240.0** (4094 hosts) • **255.255.224.0** (8190 hosts) • **255.255.192.0** (16382 hosts) • **255.255.128.0** (32766 hosts) • **255.255.0.0** (65534 hosts) *** Note:** The larger the maximum number of IP addresses per subnet the longer it will take for Discovery to finish.

Configuring Discovery's Naming Method

To configure the method Discovery uses for selecting names for discovered nodes:

1. Click the **Names Discovery** tab at the top of the Discovery Options dialog box. The Names Discovery page of the Discovery Options dialog box appears.

Figure 9-2. Names Discovery Options Dialog Box



2. Configure the Names Discovery options.
3. Click **Apply**. Names Discovery Options are configured.

The following table provides a list of the fields in the Names Discovery page of the Discovery Options dialog box.

Table 9-2. Names Discovery Options

Field Name	Description
Update names for existing entries	This determines whether Discovery updates the names for nodes already listed in the Network Map. Possible states are: • **Update** - Discovery updates the names of all discovered nodes. User defined names will be replaced by the best name discovered. • **Don't Update** - The names of existing entries to the Network Map will not be replaced.

Table 9-2. Names Discovery Options (Continued)

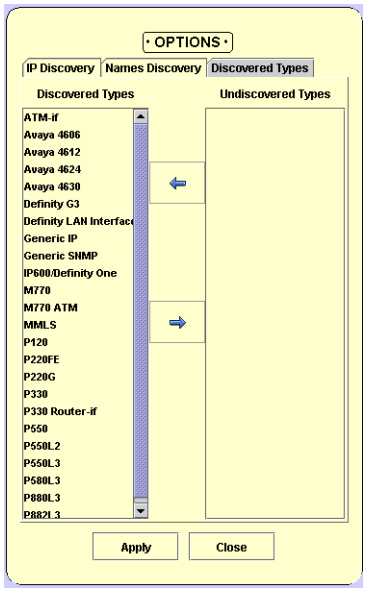
Field Name	Description
Select best name sequence	This determines the order Discovery uses to define names for discovered nodes. Discovery can use the following sources to determine the name of a node: • IP - The IP address of the node. • SNMP system name - The value assigned to the device's sysName MIB. • Name Service - The name assigned to the node via a Name Service application. Possible orders are: • **IP** - Discovery will use the IP address of the node as its name. • **SNMP sysName > IP** - If there is an SNMP system name, Discovery will use it as the node's name. Otherwise, Discovery will use the node's IP address. • **Name Service > SNMP sysName > IP** - If there is a Name Service defined name, Discovery will use it as the node's name. If there is no Name Service defined name, but there is an SNMP system name, Discovery will use it as the node's name. Otherwise, Discovery will use the node's IP address. • **SNMP sysName > Name Service > IP** - If there is an SNMP system name, Discovery will use it as the node's name. If there is no SNMP system name, but there is a Name Service defined name, Discovery will use it as the node's name. Otherwise, Discovery will use the node's IP address.

Selecting Device Types to Discover

To configure the types of devices Discovery will find:

1. Click the **Discovered Types** tab at the top of the Discovery Options dialog box. The Discovered Types page of the Discovery Options dialog box appears.

Figure 9-3. Discovered Types Options Dialog Box



2. Configure the Discovered Types options.
3. Click **OK**. Discovered Types Options are configured.

The Discovered Types page of the Discovery Options dialog box has two listboxes. Only devices in the Discovered Types listbox will be found by Discovery. Devices listed in the Undiscovered Types listbox are ignored.

To add device types to the Discovered Types list:

1. Select a device type from the Undiscovered Types list.
2. Click . The device type is moved to the Discovered Types list.

To remove device types from the Discovered Types list:

1. Select a device type from the Discovered Types list.
2. Click . The device type is removed from the Discovered Types list.

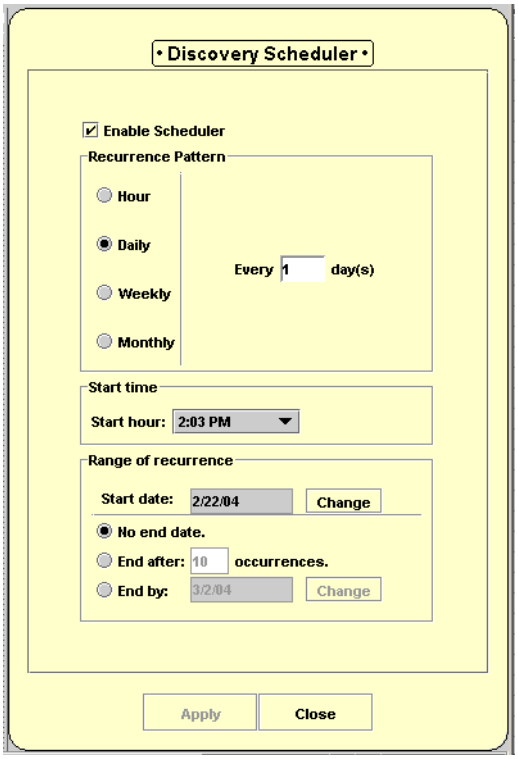
Using the Discovery Scheduler

The Discovery Scheduler can be used to set Network Discovery to run at regular intervals and from specific start to end dates.

To schedule network discovery:

1. Select **Actions > Schedule Network Discovery** in the Discovery menu bar. The Discovery Scheduler dialog box opens.

Figure 9-4. Discovery Scheduler Dialog Box



2. Configure the Discovery Scheduler options.

3. Click **Apply**. Discovery Scheduler parameters are configured.

*** Note:** At different stages while Network Discovery is running, certain operations of Network Management Console are disabled.

The following table provides a list of the fields in the Discovery Scheduler dialog box.

Table 9-3. Discovery Scheduler

Field Name	Description
Enable Scheduler	When checked, the Discovery Scheduler is enabled.
Recurrence Pattern	The frequency to run Network Discovery. Possible values are: • **Hour** - Select the hourly interval between each discovery. • **Daily** - Select the daily interval between each discovery. • **Weekly** - Select the weekly interval between each discovery. • **Monthly** - Select the monthly interval between each discovery.
Start time	Select the time to start the scheduled discovery.
Range of recurrence	Select the start date and end parameter for the schedule. Possible end values are: • **No end date** • **End after *x* occurrences** - Enter the number of times after which Discovery Scheduler does not run Network Discovery. • **End by** - Enter the date after which Discovery Scheduler does not run Network Discovery.

Discovering Subnets and Nodes

The Discovery function can be used to discover all the subnets and nodes in your network, or search for nodes on specific subnets.

For information on configuring Discovery Options, refer to "Setting Discovery Options" on page 67.

Problems during Discovery are reported in the Discovery Log. For more information, refer to "Using the Discovery Log" on page 82.

The following topics are discussed in this section:

- Discovering All Subnets and Nodes
- Discovering Nodes on Specific Subnets
- Manually Adding Subnets
- Modifying Subnets
- Subnet Parameters
- Deleting Subnets

Discovering All Subnets and Nodes

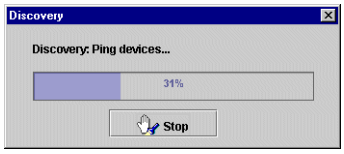
To discover all the subnets and nodes in your network:

1. Select **Edit > Delete All** in the Discovery menu bar. A confirmation dialog box opens.
2. Click **OK**. All subnets in the Subnets Table are deleted.
3. Click  in the Discovery toolbar.

   Or

   Select **Actions > Discover** in the Discovery menu bar. The Discovery process begins, and the Discovery Progress window opens.

Figure 9-5. Discovery Progress Window



To stop the Discovery, click **Stop**. A confirmation dialog box opens. Click **Yes**. Discovery finishes adding the current node to the table and stops.

When the Discovery finishes, the Subnets Table will contain a list of the subnets discovered in your network.

4. Click  in the Discovery toolbar.

   Or

   Select **File > Update Map** in the Discovery menu bar. The Network Map is updated with the results of the Discovery and saved to its corresponding Network File. After the Network Map is updated, System View Discovery runs automatically and the Network Map is updated with the System View tab.

Discovering Nodes on Specific Subnets

To select subnets upon which Discovery will search for nodes:

1. Check the Discover checkbox for each subnet upon which you want to discover nodes.

Or

1. In the Subnets Table, select the subnets upon which you want to discover nodes.

   To select more than one subnet:

   — Press **SHIFT** and select the last subnet in a contiguous selection.

   — Press **CTRL** and select additional subnets for a non-contiguous selection.

2. Click  in the Discovery toolbar.

   Or

   Select **Edit > Select**. The Discover checkbox for each selected subnet is checked.

*** Note:** If the subnet you want to discover does not appear in the Subnets Table, add it manually. For more information on adding Subnets to the Subnets Table, refer to "Manually Adding Subnets" on page 79.

To unselect subnets upon which Discovery will search for nodes:

1. Uncheck the Discover checkbox for each subnet upon which you do not want to discover nodes.

Or

1. In the Subnets Table, select the subnets upon which you do not want to discover nodes.

To unselect more than one subnet:

— Press **SHIFT** and select the last subnet in a contiguous selection.

— Press **CTRL** and select additional subnets for a non-contiguous selection.

2. Click  in the Discovery toolbar.

Or

Select **Edit > Unselect**. The Discover checkbox for each unselected subnet is unchecked.

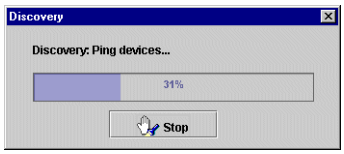
To start Discovery on the subnets whose Discover checkbox is checked:

Click  in the Discovery toolbar.

Or

Select **Actions > Discover** in the Discovery menu bar. The Discovery process begins searching for nodes on the subnets whose Discover checkbox is checked, and the Discovery Progress window opens.

Figure 9-6. Discovery Progress Window



To stop the Discovery, click **Stop**. A confirmation dialog box opens. Click **Yes**. Discovery finishes adding the current node to the table and stops.

Discovery searches for nodes in the selected subnet. When the Discovery finishes, it updates the Subnets Table with the information discovered.

To update the Network Map with the updated information:

Click  in the Discovery toolbar.

Or

Select **File > Update Map** in the Discovery menu bar. The Network Map is updated with the results of the Discovery and saved to its corresponding Network File. After the Network Map is updated, System View Discovery runs automatically and the Network Map is updated with the System View tab.

Manually Adding Subnets

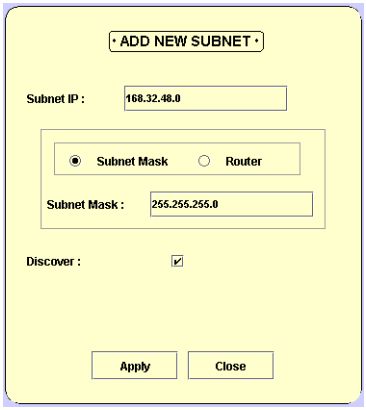
To manually add a subnet to the Subnets Table:

1. Click  in the Discovery toolbar.

   Or

   Select **Edit > Add** in the Discovery menu bar. The Add Subnet dialog box opens.

Figure 9-7. Add Subnet Dialog Box



2. Enter the subnet parameters in the dialog box. For information on the fields in the Add Subnet dialog box, refer to "Subnet Parameters" on page 81.

3. Click **Apply**. The subnet is added to the current Network Map.

4. Click  in the Discovery toolbar.

   Or

   Select **File > Update Map** in the Discovery menu bar. The Network Map is updated with the results of the Discovery and saved to its corresponding Network File. After the Network Map is updated, System View Discovery runs automatically and the Network Map is updated with the System View tab.

Modifying Subnets

To modify a subnet in the current Network Map:

1. Select a subnet in the Subnets Table.

2. Click  in the Discovery toolbar.

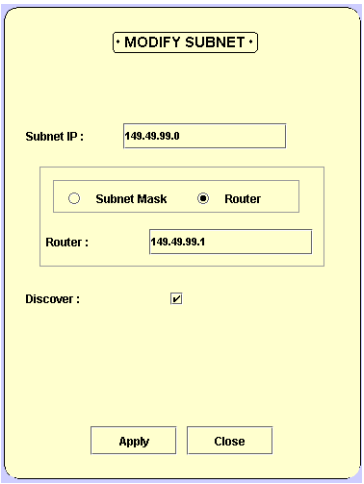
Or

Double-click the selected subnet.

Or

Select **Edit > Modify** in the Discovery menu bar. The Modify Subnet dialog box opens.

Figure 9-8. Modify Subnet Dialog Box



3. Modify the parameters in the dialog box. For information on the fields in the Add Subnet dialog box, refer to "Subnet Parameters" on page 81.

4. Click **Apply**. The subnet is modified in the current Network View.

5. Click  in the Discovery toolbar.

Or

Select **File > Update Map** in the Discovery menu bar. The Network File is updated with the information in the Network Map. After the Network Map is updated, System View Discovery runs automatically and the Network Map is updated with the System View tab.

Subnet Parameters

The following table provides a list of the parameters in the Add Subnet and Modify Subnet dialog boxes.

Table 9-4. Subnet Parameters

Parameter	Description
Subnet IP	IP address of the subnet.
Mask IP/Router IP	Determines whether a subnet mask or a specific router is used for the subnet. • **Subnet Mask** - A subnet mask is used for the subnet. You must enter a valid subnet mask in the IP Subnet Mask field. The Router field is ignored. • **Router** - The subnet's router is used for the subnet. You must enter the router's IP address in the Router field. The IP Subnet Mask field is ignored.
IP Subnet Mask	The IP subnet mask.
Router	The IP address of the subnet's router.
Discover Nodes	Determines whether Discovery will search for nodes on the subnet. If checked, Discovery will search for nodes on the subnet. If unchecked, Discovery will not search for nodes on the subnet.

Deleting Subnets

To delete a subnet from the Subnets Table:

1. Select a subnet in the Subnets Table.

   — To select multiple subnets, press **CTRL** while selecting additional subnets.

2. Click  in the Discovery toolbar.

   Or

   Select **Edit > Delete** in the Discovery menu bar. A confirmation dialog box opens.

3. Click **Yes**. The selected subnets are deleted from the Subnets Table.

Using the Discovery Log

The progress of the Discovery process is reported in the Discovery Log. If the Discovery Log contains entries, an "**L**" appears in the Status Bar of the Discovery window. Error entries are bold in the Discovery Log.

To view the Discovery Log:

Click  in the Discovery toolbar.

Or

Select **View > Log Report** in the Discovery menu bar. The Discovery Log opens under the Subnets Table.

Figure 9-9. Discovery Log

#	IP	Message	Comment
1	149.49.77.51	New discovery for selected subnets started at Thu Aug 23 16:20:43 IDT 2001	
2	149.49.77.51	Discovery stopped at Thu Aug 23 16:20:49 IDT 2001	
3	149.49.77.51	New discovery for selected subnets started at Thu Aug 23 16:21:29 IDT 2001	
4	149.49.77.51	Discovery ended at Thu Aug 23 16:21:56 IDT 2001	
5	149.49.77.51	New discovery for selected subnets started at Thu Aug 23 16:23:16 IDT 2001	
6	149.49.99.1	Router access problems	Double click to change ro...
7	149.49.77.51	Discovery ended at Thu Aug 23 16:24:01 IDT 2001	

The Discovery Log enables performing the following actions:

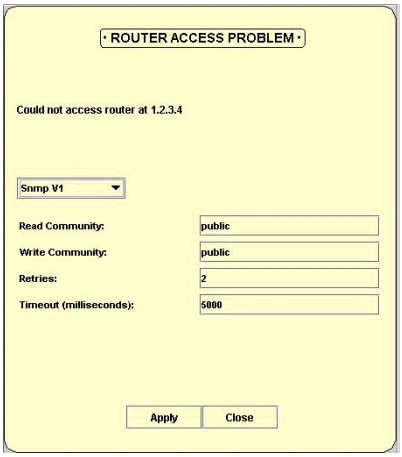
- **Configuring Router Access Parameters**
- **Saving the Discovery Log**
- **Deleting Log Entries**

- Clearing the Discovery Log

Configuring Router Access Parameters

You can configure the SNMP parameters for a router that Discovery could not access. This may allow Discovery to search the router's subnets for nodes. To view router access parameters, click the router's access error message in the Discovery Log. The Router Access Configuration dialog box opens.

Figure 9-10. Router Access Configuration Dialog Box



The dialog box contains the router access error message and the current router access configuration parameters. The following table provides a list of the parameters in the Router Access Configuration dialog box and their descriptions.

Table 9-5. Router Access Configuration Parameters

Field Name	Description
SNMP	The SNMP protocol. Possible SNMP protocols are: • **Snmp V1** • **Snmp V3**
Read community	The read community of the router. Only applicable for SNMP protocol V1.
Write community	The write community of the router. Only applicable for SNMP protocol V1.
User	A user name as defined in the User Administration. Only applicable for SNMP protocol V3.

Table 9-5. Router Access Configuration Parameters (Continued)

Field Name	Description
Retries	The number of times Discovery will ping the router with no response before giving up.
Timeout (milliseconds)	The amount of time (in milliseconds) Discovery will ping the router with no response before timing out.

To change the router access configuration and retry discovering nodes on the subnet:

1. Change some of the router access configuration parameters.
2. Click **OK**. The router access configuration is changed, and Discovery will try to find nodes on the subnet.

Saving the Discovery Log

To save the Discovery Log to a file:

1. Click  next to the Discovery Log. The Save As dialog box opens.
2. Enter a filename, and browse to the directory in which to save the file.
3. Click **Save**. The Discovery Log is saved to the specified file.

Deleting Log Entries

To delete an entry from the Discovery Log:

1. Select an entry.
   - To select multiple entry, press **CTRL** while clicking on additional entries.
2. Click  next to the Discovery Log. The selected entries are deleted from the Discovery Log.

Clearing the Discovery Log

To clear all entries from the Discovery Log:

1. Click  next to the Discovery Log.
2. Confirm your selection. The Discovery Log is cleared.

Manually Discovering System View

To manually discover the System View:

Select **Actions> System View Discovery** in the Console menu bar. System View Discovery is performed and the Network Map is updated.

Using the System View Log

The progress of the most recent System View Discovery process is reported in the System View Log.

To view the System View Log, select **View > System View Log** in the Console menu bar. The System View Log opens in Notepad.

10 Introduction to the Event Manager

This chapter provides a detailed description of the Event Manager, and includes the following sections:

- **Event Manager Overview** - An overview of the Event Manager.
- **Viewing the Event Manager** - Detailed instructions on how to view the Event Manager.
- **The Event Manager User Interface** - A description of the Event Log Browser, Event Configuration window, and Action List window.
- **Closing the Event Manager** - Instructions on how to close the Event Manager.

Event Manager Overview

Device agents send SNMP traps to Avaya Network Management Server. These are received by the Event Manager. The Event Manager can be viewed using Avaya Network Management Console. The Event Log Browser window of the Event Manager provides a list of traps in a table. Each row contains information about a single trap.

*** Note:** To receive device traps in Event Manager, include Avaya Network Management Server on the list of each device's trap managers. For information on configuring Avaya Network Management Server as a trap manager, refer to the device's User Guide or on-line help.

In addition, the Event Manager can notify multiple management hosts of network events. It can also open a pop-up message, play of a sound file, or send an e-mail to notify managers of important network events. In addition, you can configure a network event to trigger a pre-defined script. The Event Configuration window of the Event Manager provides a method for defining actions and assigning actions to specific traps.

Viewing the Event Manager

To view the Event Manager:

Click .

Or

Select **Actions > Event Manager**. The Event Manager opens showing the Event Log Browser.

The Event Manager User Interface

The Event Manager consists of three windows, whose user interfaces are described in this section:

- **The Event Log Browser User Interface**
- **The Event Configuration User Interface**
- **The Action List User Interface**

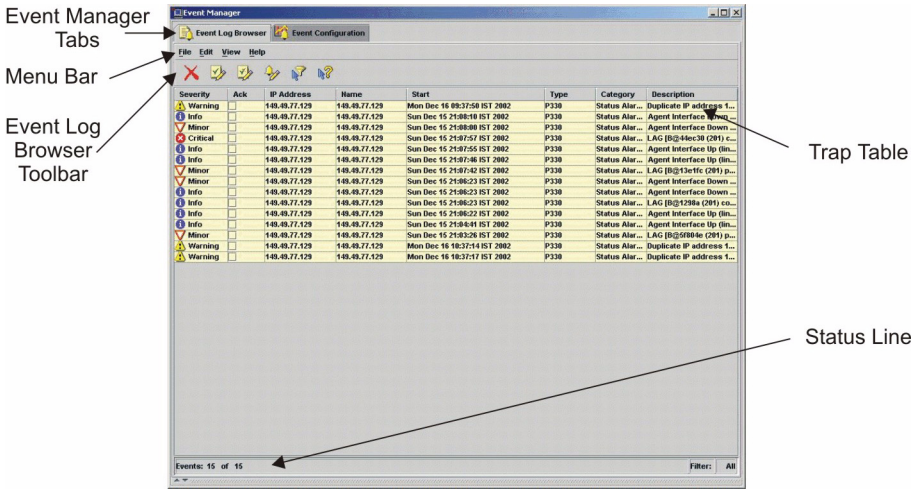
Use the Tabs at the top of the Event Manager for switching between the Event Log Browser and Event Configuration windows. The Action List window can only be reached from the Event Configuration window.

The Event Log Browser User Interface

The Event Log Browser user interface consists of the following elements:

- **Event Manager Tabs** - Tabs for switching between the Event Log Browser and the Event Configuration window.
- **Menu Bar** - Menus for accessing Event Log Browser functions. For more information on Event Log Browser menus, refer to Appendix A, Network Management Menus.
- **Event Log Browser Toolbar** - Toolbar buttons for accessing Event Log Browser functions.
- **The Trap Table** - An area where a table of traps in the log appears.
- **Status Line** - Displays information about the number of traps in the Event Log Browser.

Figure 10-1. Event Log Browser User Interface



Event Log Browser Toolbar

The table below describes the buttons on the Event Log Browser Toolbar and gives the equivalent menu options.

Table 10-1. Event Log Browser Toolbar

Button	Description	Menu Item
	Deletes the selected traps.	**Edit > Delete**
	Marks the selected traps as acknowledged.	**Edit > Acknowledge**
	Marks the selected traps as unacknowledged.	**Edit > UnAcknowledge**
	Highlights the selected trap in the tree in the Event Configuration User Interface.	**Edit > Modify Event**
	Filters the traps viewed in the Trap Table.	**View > Filter**
	Opens context-sensitive help.	**Help > Help On**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

The Trap Table

By default, the Trap Table lists the traps sent to Avaya Network Management Server in the order in which they were sent. The information displayed in the Trap Table in the However, you can sort the Trap Table by any of its fields. To sort the Trap Table by one of its fields, click the field's column header. To reverse the sort order, click the column header again.

You can configure the information in the Trap Table using the Assign Action Form Area in the Event Configuration Window User Interface, refer to "Assign Action Form Area" on page 92.

*** Note:** The Trap Table can hold up to 10,000 traps.

The following table provides a list of the fields in the Trap Table and an explanation of each field.

Table 10-2. Trap Table Fields

Field	Description
Severity	An icon representing the severity of the trap: •  - Info •  - Warning •  - Minor •  - Major •  - Critical
Ack (Acknowledged)	This column shows a checkmark if a trap has been acknowledged.
IP Address	The IP address of the sender of the trap.
Name	The best name of the sender of the trap.
Start	The time the trap was sent.
Type	The type of device from which the trap was sent.
Category	The category of the event.
Description	A description of the trap. The information displayed in this field is configured in the Assign Action Form Area of the Event Configuration User Interface. For more information, refer to "Assign Action Form Area" on page 92.

To locate the device from which an event was sent, double-click the event in the Trap table and the device will be highlighted in the SNMP Console tree.

Status Line

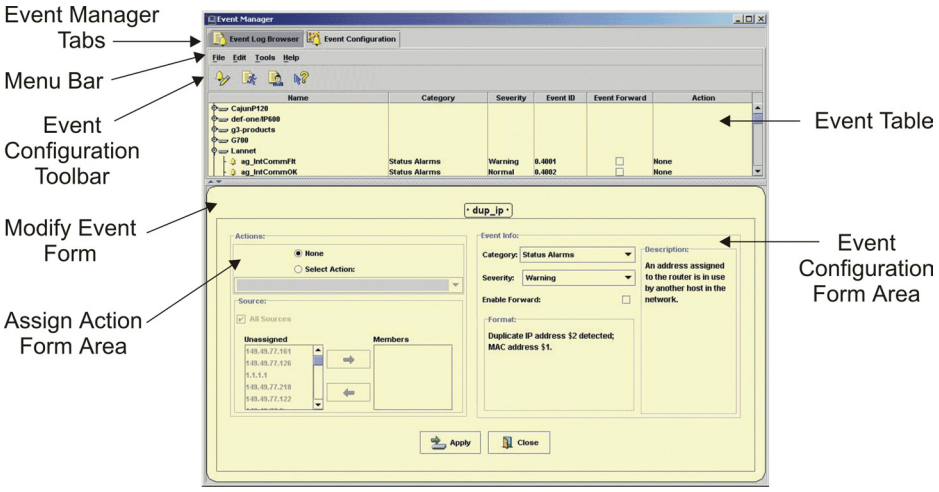
The Event Log Browser's Status Line displays the number of traps in the Event Log Browser. This number includes traps that are not currently displayed in the Trap Table. In addition, the Status Line displays the current filtering options.

The Event Configuration User Interface

The Event Configuration user interface consists of the following elements:

- **Event Manager Tabs** - Tabs for switching between the Event Log Browser and the Event Configuration window.
- **Menu Bar** - Menus for accessing Event Configuration functions. For more information on Event Configuration menus, refer to Appendix A, Network Management Menus.
- Event Configuration Toolbar - Toolbar buttons for accessing Event Configuration functions.
- **The Event Table** - A collapsible table providing a list of trappable network events and their configured responses.
- **Assign Action Form Area** - An area that contains the following dialog boxes:
  - Assign Action Form - used to assign actions to specific events.
  - Event Configuration Form - used to configure the display of events in the Event Log Browser.

Figure 10-2. Event Configuration User Interface



Event Configuration Toolbar

The table below describes the buttons on the Event Configuration toolbar and gives the equivalent menu options.

Table 10-3. Event Configuration Toolbar

Button	Description	Menu Item
	Opens the Modify Trap dialog box for the selected network event.	**Edit > Modify Event**
	Opens the Action List window.	**Tools > Action List**
	Opens the Event Forwarding dialog box.	**Tools > Event Forwarding**
	Opens context-sensitive help.	**Help > Help On**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

The Event Table

The Event Table lists network events in a collapsible tree. Each event category can be expanded or collapsed by clicking the handle next to the category. The following table provides a list of the fields in the Event Table and an explanation of each field.

Table 10-4. Event Table Fields

Field	Description
Name	The name of the event or event category.

Table 10-4. Event Table Fields (Continued)

Field	Description
Category	The category of the event.
Severity	The severity of the network event: • Normal • Warning • Minor • Major • Critical
Event ID	A numeric identifier for the event.
Event Forward	The state of event forwarding for the trap. If the checkbox is checked, the event is configured for forwarding. If the checkbox is not checked, the event has not been configured to be forwarded. *** Note:** If event forwarding is configured for all traps, the Event Forward checkbox is not relevant. All network events are forwarded.
Action	The defined action triggered by the event.

*** Note:** When running Network Management from a remote station, the Event Table is read-only.

Assign Action Form Area

The Assign Action Form Area provides a dialog box for assigning pre-defined actions to specific events. The following table provides a list of the fields in the Assign Action Form and an explanation of each field.

Table 10-5. Assign Action Form Fields

Field	Description
Actions	The action assigned to the selected event. Possible actions are: • **None** - No action is assigned to the selected event. • **Select Action** - The action displayed in the pull-down list box is assigned to the selected event.

Table 10-5. Assign Action Form Fields (Continued)

Field	Description
Source	The IP addresses of the sources of the selected event. Only if the selected event's trap is sent from one of the IP addresses listed in the Members listbox does the configured action occur. If All Sources is checked, the configured action occurs regardless of the source from which the trap is sent.

Event Configuration Form Area

The Event Configuration Area enables you to configure the information displayed in the Event Log Browser.

Table 10-6. Event Configuration Form Fields

Field	Description
Category	The type of event: • Log Only • Ignore (default for generic SNMP traps) • Error Alarms • Threshold Alarms • Status Alarms • Configuration Alarms • Application Alert Alarms • Network Topology Alarms *** Note:** Traps defined for Log Only and Ignore are not shown in the event browser.
Severity	The severity of the selected event: • Normal • Warning • Minor • Major • Critical
Enable Forward	If checked, the event is forwarded to selected stations. If unchecked, the event is not forwarded, unless you forward all events.

Table 10-6. Event Configuration Form Fields (Continued)

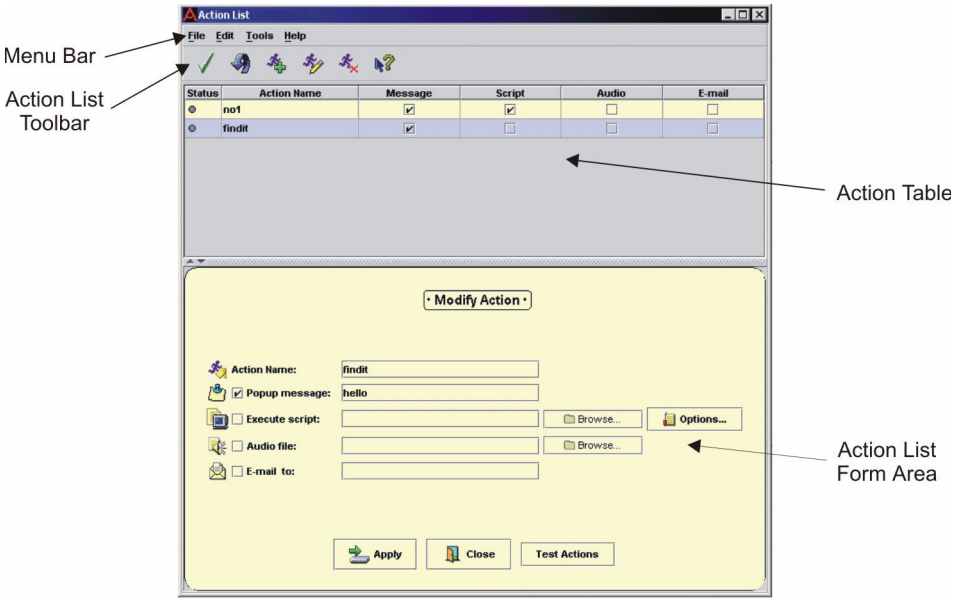
Field	Description
Format	The format in which the event will be displayed in the description field of the Event Log Browser. The following parameters are available for configuring the format: • **$e** - trap enterprise. • **$<number>** - retrieves the specified parameter from the trap. <number> denotes the order in which the parameter appears, i.e., the first parameter is denoted by "1", the second parameter is denoted by "2", etc. • **$A** - IP address of the agent who sent the trap. • **$#** - returns the number of parameters in the trap. • **$*** - enterprise:interface number. All arguments are separated by a colon. • **$E** - OID trap alias (i.e., the name of the group in which the trap is defined).
Description	A detailed description of the selected event. This information does not appear in the Event Log Browser.

The Action List User Interface

The Action List user interface consists of the following elements:

- **Menu Bar** - Menus for accessing Action List functions. For more information on Action List menus, refer to Appendix A, Network Management Menus.
- **Action List Toolbar** - Toolbar buttons for accessing Action List functions.
- **The Action Table** - A table providing a list of configured responses to network events.
- **Action Form Area** - An area where all dialog boxes appear.

Figure 10-3. Action List Window User Interface



Action List Toolbar

The table below describes the buttons on the Action List Toolbar and gives the equivalent menu options.

Table 10-7. Action List Toolbar

Button	Description	Menu Item
	Applies the changes to the Action List.	**Edit > Apply**
	Undoes all unapplied changes to the Action List.	**Edit > Revert**
	Adds a new action to the Action List.	**Edit > Add**
	Opens the Modify Action dialog box for the selected action.	**Edit > Modify**
	Deletes the selected action.	**Edit > Delete**
	Opens context-sensitive help.	**Help > Help on**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

The Action Table

The Action Table lists configured actions. Each row in the table represents an action that can be assigned to a trap. These actions are listed in the Action Form Area in the Event Configuration Window. The following table provides a list of the fields in the Action Table and an explanation of each field.

Table 10-8. Action Table Fields

Field	Description
Status	The status of the row in the table. For more information, refer to "Using Avaya Network Management Console Tables" on page 29.
Action Name	The user defined name of the action.
Message	If checked, the action includes a pop-up message.
Script	If checked, the action includes running a script.
Audio	If checked, the action includes an audible message.
E-mail	If checked, the action includes sending an e-mail.

*** Note:** When running Network Management from a remote station, the Action Table is read-only.

Action Form Area

The Action Form Area is where the Add Action and Modify Action dialog boxes open. For information on the fields in the Add Action and Modify Action dialog boxes, refer to "Action Fields" on page 108.

Closing the Event Manager

To close the Event Manager, select **File > Exit**. The Event Manager closes.

11 Managing Events

This chapter provides instructions on using the Event Manager. It includes the following sections:

- **Managing Traps** - Detailed instructions on how to filter, acknowledge, delete, edit, save, and archive traps.
- **Defining Actions** - Detailed instructions on how to define actions.
- **Configuring Events** - Detailed instructions on how to assign defined actions to network events.

Managing Traps

This topic provides instructions on managing traps and includes the following sections:

- **Trap Log Options** - Instructions on the options available for cleaning up the Trap Table.
- **Filtering Traps** - Instructions on how to filter the traps displayed in the Trap Table.
- **Acknowledging Traps** - Instructions on how to mark traps as acknowledged.
- **Deleting Traps** - Instructions on how to delete traps from the Trap Table.
- **Editing Severity Levels** - Instructions on how to edit the severity level of traps in the Trap Table.
- **Saving the Trap Table** - Instructions on how to save the contents of the Trap Table to a file.

For more information on the Event Manager user interface, refer to "The Event Manager User Interface" on page 87.

Trap Log Options

The Trap Log can hold up to 10,000 traps. When this limit is reached, traps must be removed from the Trap Log to provide room for new traps. You can configure Network Management to either discard old traps or archive them.

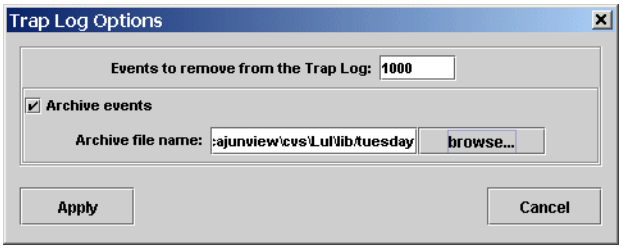
*** Note:** By default, when the Trap Log holds 10,000 traps, the oldest 1,000 traps are discarded.

*** Note:** Archived traps are appended to the event archive.

To configure the method Network Management uses to clean up the Trap Log:

1. Select **File > Options**. The Trap Log Options dialog box opens.

Figure 11-1. Trap Log Options Dialog Box



2. Enter a number between 1 and 9999 in the Events to remove from the Trap Log field. This is the number of events to be deleted when there are 10,000 events in the Trap Log.

3. If you want the deleted traps saved to an archive, check the Archive events checkbox.

   a. Enter a path and file name for the event archive in the Archive File name field. Ensure that the file extension is either **`csv`** for a Comma Separated Value file or **`xml`** for an XML file.

   Or

   a. Click **Browse**. A file browser dialog box opens.

   b. Browse to the directory in which you want to save the archive.

   c. Enter a file name in the File name field.

   d. Select a file type from the Files of type pull-down listbox. Available file types are CSV (comma separated value) and XML.

4. Click **Apply**. The clean up method for the Trap Log is configured. Whenever the Trap Log contains 10,000 events, this method will be used to remove the specified number of events from the Trap Log.

*** Note:** If you specify a CSV file for the trap archive and the file is open when traps need to be archived, a new file is created containing all of the traps in the old archive. Archiving continues using the new file.

Filtering Traps

By default, all traps in the Event Log Browser are displayed in the Trap Table. However, you can filter traps by severity level, source, device type, or acknowledgment status. When you filter the Trap Table, traps that do not meet the filtering criteria are hidden. However, they are not deleted from the Event Log. The following topics are discussed in this section:

- **Filtering By Severity Level**
- **Filtering By IP Address**
- **Filtering By Device Type**
- Filtering By Acknowledged
- **Viewing All Traps**

*** Note:** You can only filter by one criterion at a time.

Filtering By Severity Level

To view only traps of a given severity level:

1. Click . The cursor changes to a hand.
2. Click on the Severity column of a trap with the desired severity. Only traps with the selected severity are displayed in the Trap Table.

Or

1. Select **View > Filter > Severity Filter**. The Severity Filter dialog box opens.

Figure 11-2. Severity Filter Dialog Box



2. Check the checkboxes next to the severity levels of the traps you want displayed in the Trap Table.
3. Click **Apply**. Only traps of the checked severity levels are displayed in the Trap Table.

Filtering By IP Address

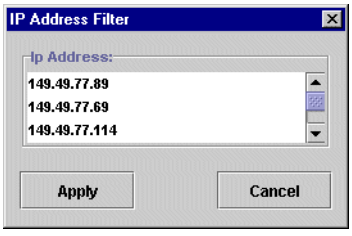
To view only traps from a specific IP address:

1. Click . The cursor changes to a hand.
2. Click on the From column of a trap from the desired device. Only traps from the selected IP address are displayed in the Trap Table.

Or

1. Select **View > Filter > IP Address Filter**. The IP Address Filter dialog box opens.

Figure 11-3. IP Address Filter Dialog Box



2. Select the IP addresses of the devices from which you want to view traps from the listbox.
3. Click **Apply**. Only traps from the selected IP addresses are displayed in the Trap Table.

Filtering By Device Type

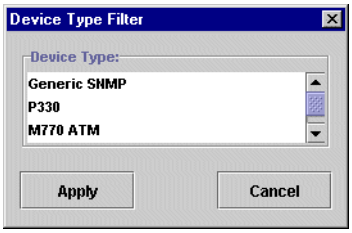
To view only traps from a specific device type:

1. Click . The cursor changes to a hand.
2. Click on the Device Type column of a trap from the desired device type. Only traps from devices of the selected device type are displayed in the Trap Table.

Or

1. Select **View > Filter > Device Type Filter**. The Device Type Filter dialog box opens.

Figure 11-4. Device Type Filter Dialog Box



2. Select device types from the listbox.
3. Click **Apply**. Only traps from devices of the selected types are displayed in the Trap Table.

Filtering By Acknowledged

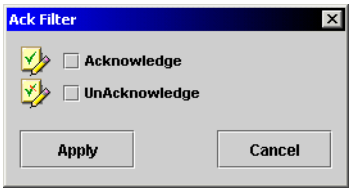
To filter traps by the Acknowledged field:

1. Click . The cursor changes to a hand.
2. Click on the Ack column of a trap with the desired Acknowledgement. Only traps with the same value in the Acknowledged field are displayed in the Trap Table.

Or

1. Select **View > Filter > Acknowledge Filter**. The Acknowledged Filter dialog box opens.

Figure 11-5. Acknowledged Filter Dialog Box



2. Check the checkboxes next to the Acknowledgement statuses of the traps you want displayed in the Trap Table.

3. Click **Apply**. Only traps with the checked Acknowledgement statuses are displayed in the Trap Table.

Viewing All Traps

To cancel the current filtering options and view all traps in the Trap Table, select **View > Filter > No Filter**. All traps are displayed in the Trap Table.

Acknowledging Traps

It is useful to acknowledge traps of which you are aware, even if you do not want to delete them. This can help focus your interest on traps that you have not yet seen.

To acknowledge a trap:

1. Select a trap.
   - To select multiple traps, press **CTRL** while clicking on additional traps.
   - To select all traps, select **Edit > Select All**.
2. Click .

   Or

   Select **Edit > Acknowledge**.

   Or

   Click the Acknowledge Icon field in a trap that was not yet acknowledged. The trap is marked with a checkmark.

To remove the acknowledge mark from a trap:

1. Select a trap.
   - To select multiple traps, press **CTRL** while clicking on additional traps.
   - To select all traps, select **Edit > Select All**.

2. Click .

   Or

   Select **Edit > UnAcknowledge**.

   Or

   Click the Acknowledge Icon field in an acknowledged trap. The trap is unmarked.

Deleting Traps

It is important to delete old traps from the Trap Table. This prevents the Event Manager from becoming unwieldy and allows you to focus on current network events.

To delete a trap:

1. Select a trap.
   - To select multiple traps, press **CTRL** while clicking on additional traps.
   - To select all traps, select **Edit > Select All**.
2. Click .

   Or

   Select **Edit > Delete**. A confirmation dialog box opens
3. Click **Yes**. The trap is deleted.

Editing Severity Levels

You can change the severity level of selected traps. This is useful when a trap is more (or less) important than it would be normally. The change in importance may be the result of an extraordinary load on the network, the trap's source being a monitored port, or any other cause.

To edit the severity level of a trap:

1. Select a trap.

2. Select **Edit > Change Severity > Change severity to** *Severity level,* where *Severity level* is the severity level for the trap.

   Or

   Select a severity level from the trap's Severity column. The trap's severity level is changed.

Saving the Trap Table

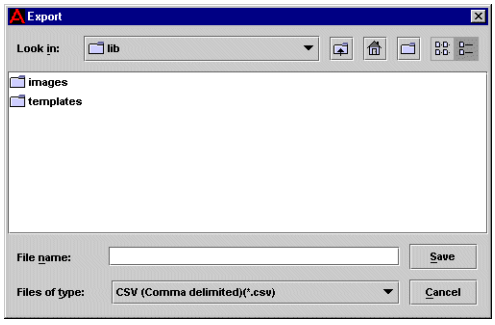
The Trap Table can be saved to a file. The file can be in one of the following formats:

- **Comma Separated Values (CSV)** - As a text file with the columns in each row separated by commas.
- **XML** - As an XML file.

To save the Trap Table to a file:

1. Click **File > Export**. A save as dialog box opens.

Figure 11-6. Export Dialog Box



2. Browse to the directory in which to save the file.
3. Enter a name for the file in the File name field.
4. Select the file format from the Files of type pull-down list.
5. Click **Save**. The Trap Table is saved to the specified file.

Defining Actions

This topic provides instructions on defining actions and includes the following sections:

- **Actions Overview** - An overview of trap actions in Avaya Network Management Console.
- **Adding Actions** - Instructions on how to add actions to the Action List.
- **Modifying Actions** - Instructions on how to modify actions.
- **Action Fields** - A description of each of the fields in the Add/Modify Action dialog box.
- **Deleting Actions** - Instructions on how to delete actions from the Action List.
- **Applying Changes to the Action List** - Instructions on how to apply Action List changes to the network.
- **Action Options** - Instructions on how to configure Avaya Network Management Console to use your SMTP server.

For information on the Action Table window, refer to "The Action List User Interface" on page 94.

Actions Overview

Actions are methods of notifying managers of important network events. Notification methods include the appearance of a pop-up window, the running of a script, the playing of a sound file, and the sending of an e-mail.

A defined action can include any combination of these notification methods. Once an action is defined, it can be assigned to selected traps. For more information on assigning actions to traps, refer to "Configuring Events" on page 112.

The Action Table includes a list of all configured actions.

Adding Actions

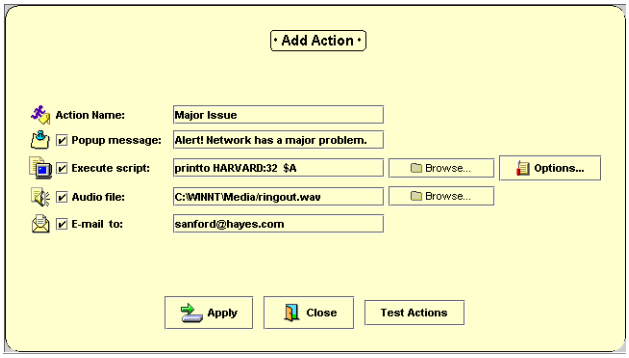
To add an action to the Action List:

1. Click .

   Or

   Select **Edit > Add Action**. The Add Action dialog box opens.

Figure 11-7. Add Action Dialog Box



2. Define the action using the Add Action dialog box fields. For information on the fields in the Add Action dialog box, refer to "Action Fields" on page 108.

3. To test the new action, click **Test Actions**. The defined actions occur.

4. Click **Apply**. The action is added to the Action List.

Modifying Actions

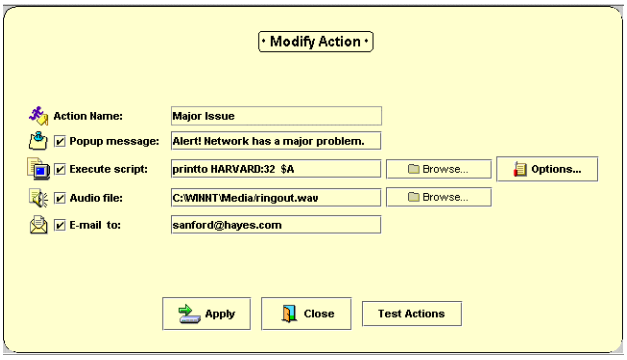
To modify an action in the Action List:

1. Select an action in the Action List.
2. Click .

   Or

   Select **Edit > Modify Action**. The Modify Action dialog box opens.

Figure 11-8. Modify Action Dialog Box



3. Edit the action using the Add Action dialog box. For information on the fields in the Modify Action dialog box, refer to "Action Fields" on page 108.
4. To test the modified action, click **Test Actions**. The defined actions occur.
5. Click **Apply**. The action in the Action List is modified.

Action Fields

The following topics are described in this section:

- **Action Scripts**
- **Action Audio Files**

The following table provides a list of the fields in the Add Action and Modify Action dialog boxes and an explanation of each field.

Table 11-1. Action Fields

Field	Description
Action Name	The name of the defined action.
Popup message	The state of the checkbox determines whether the action includes a pop-up message. The textbox contains the text of the pop-up message.
Execute script	The state of the checkbox determines whether the action includes running a script. The textbox contains the name of the script file. You can assign a script file by clicking **Browse** and using a standard file browser to find the script file. For more information on scripts, refer to "Action Scripts" on page 109.
Audio file	The state of the checkbox determines whether the action includes playing an audio file. The textbox contains the name of the audio file. You can assign an audio file by clicking **Browse** and using a standard file browser to find the audio file. For more information on audio files, refer to "Action Audio Files" on page 110.
E-mail to	The state of the checkbox determines whether the action includes sending an e-mail. The textbox contains the address to which the e-mail is sent.

Action Scripts

You can include any executable file in an action. Valid executable files are operating system dependant. For example, on a computer running Windows, BAT, COM, and EXE files are executables.

In addition, up to four variable command line parameters can be included in the command. The following table provides a list of the command line variables and their descriptions.

Table 11-2. Command Line Parameters

Parameter	Variable	Description
IP Address	`$A`	The IP address of the device from which the trap was sent.
SysOId + n	`$e`	The SysOId of the device followed by `.`*n* for predefined traps, or `0.`*n* for vendor specific traps, where *n* is the trap code.
Severity	`$s`	The severity of the event.
Event Message	`$f`	A formatted message describing the event.

To add command line parameters to the script:

1. Enter the parameters manually in the Execute Script field.

Or

1. Click **Options**. The Script Parameters dialog box opens.

Figure 11-9. Script Parameters Dialog Box



2. Check the checkboxes next to the parameters you want to add to the command.

3. Click **Apply**. The Script Parameters dialog box closes, and the selected parameters are inserted in the Execute Script field.

In addition, you can add command line parameters, specific to your system.

For example, the command **`print_report printer:BOSTON $A $e $f`**, may send the command `print_report printer:BOSTON 213.21.70.142 Major "Bus 10 internal clock fault"` to your computer.

*** Note:** Network Management is not responsible for validating any assigned scripts or ensuring that they can receive command line parameters.

Action Audio Files

You can select any audio file recognized by your computer for inclusion in an action. The file will be played by its associated application. If the file format is unrecognized by your operating system, an error will occur.

*** Note:** Network Management is not responsible for validating an audio file or format.

Deleting Actions

To delete an action from the Action List:

1. Select an action in the Action List.
2. Click .

   Or

   Select **Edit > Delete**. The selected action is marked for deletion in the Action List.

Applying Changes to the Action List

To apply the changes to the network:

Click .

Or

Select **Edit > Apply**. The changes are applied to the network.

Action Options

If you define actions that include e-mails, you must configure Avaya Network Management Console to use an appropriate SMTP server. In addition, you should specify an e-mail address as the sender of the e-mail. To define e-mail settings:

1. Select **Tools > Options**. The Action List Options dialog box opens.

Figure 11-10. Action List Options Dialog Box



2. Enter your SMTP server in the SMTP server field.
3. Enter the e-mail address you want to appear as the sender of e-mails in the Sender Address field.
4. Click **Apply**. Avaya Network Management Console is configured to use the specified SMTP server.

Configuring Events

Some network events are so important, that the reporting of the event in the Event Log Browser is not sufficient. The Event Configuration window allows you to configure additional notification methods for important traps. In addition, you can configure event forwarding from the Event Configuration window. The following topics are described in this section:

- **Assigning Actions to Events**
- **Configuring Event Forwarding**

To configure events and event forwarding, click the Event Configuration tab. The Event Configuration window appears.

For information on the Event Configuration user interface, refer to "The Event Configuration User Interface" on page 90.

Assigning Actions to Events

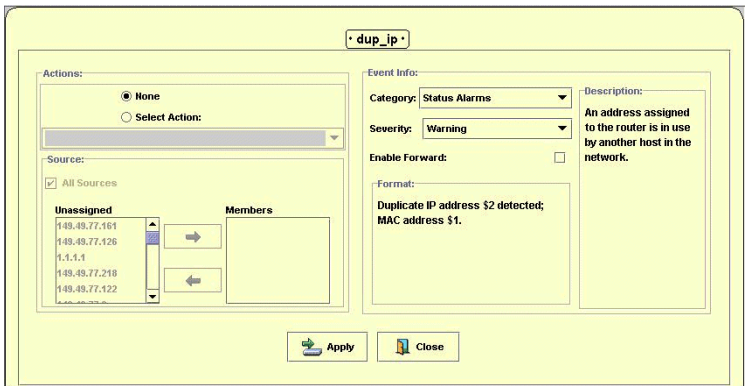
To assign an action to an event:

1. Click the handle next to the category of the event for which you want to define an action.
2. Select the event for which you want to define an action.
3. Click .

   Or

   Select **Edit > Modify Event**. The Action Definition dialog box opens under the Event Configuration window.

Figure 11-11. Action Definition Dialog Box



4. Click **Select Action**. To unassign an action, click **None**, and continue with step **7**.

5. Select a defined action from the pull-down listbox. For more information on defining actions, refer to "Defining Actions" on page 105.

6. Select source devices for the action. The Event Action is defined for only the devices in the Members listbox or for all devices.

   To define the action for all network devices, check the **Add All Sources** checkbox.

   To add individual devices to the Members list:

   a. Select a device in the Unassigned list.

   To select a contiguous group of devices, press the **SHIFT** key and select the last device in the group.

   To select a non-contiguous group of devices, press the **CTRL** key while selecting additional devices.

   b. Click . The selected devices are moved to the Members list.

   To remove individual devices from the Members list:

   a. Select a device in the Members list.

   To select a contiguous group of devices, press the **SHIFT** key and select the last device in the group.

   To select a non-contiguous group of devices, press the **CTRL** key while selecting additional devices.

   b. Click . The selected devices are moved to the Unassigned list.

7. Select a category from the Category pull-down listbox.

8. Select a severity from the Severity pull-down listbox.

9. If you want to enable event forwarding for the event, check the Enable Event Forward checkbox. The event will be forwarded to the IP addresses listed in the Event Forwarding Options dialog box. To prevent the event from being forwarded, clear the Enable Event Forward checkbox. The event will not be forwarded unless the All button is selected in the Event Forwarding Options dialog box.

10. Define the format in which to display the event in the Format area.

11. Enter a description of the event in the Description area.

12. Click **Apply**. The selected action is assigned to the selected event from the selected source.

*** Note:** Only one action can be assigned to a particular event.

To close the Action Definition dialog box, click **Close**. The Action Definition dialog box closes, and the Event Table expands to fill the window.

Configuring Event Forwarding

Event forwarding enables events to be posted to devices further up the network hierarchy. This is useful, because it minimizes the need to configure multiple trap recipients on the device level. Instead, traps from multiple devices can be forwarded to a single network device from which the traps can be sent to multiple recipients. In addition, you can forward all events or only specific events.

The following topics are described in this section:

- **Event Forwarding Sources**
- **Configuring Forwarding Recipients**

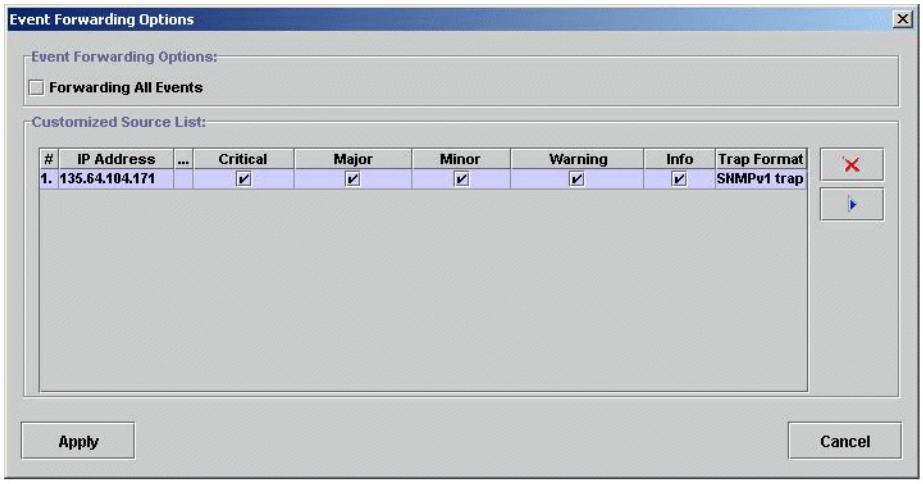
To open the Event Forwarding Options dialog box:

Click .

Or

Select **Tools > Event Forward**. The Event Forwarding Options dialog box opens.

Figure 11-12. Event Forwarding Options Dialog Box



To close the Event Forwarding dialog box, click **Cancel**.

Event Forwarding Sources

To configure event forwarding sources:

1. Do one of the following:
   - To forward all events, check the **Forwarding All Events** checkbox.
   - To forward only specific events, uncheck the **Forwarding All Events** checkbox. Only events configured with the Enable Event Forward checkbox in the Action Definition dialog box are forwarded. For more information, refer to "Action Options" on page 111.
2. Select the severity level of the alarm: **Critical**, **Major**, **Minor**, **Warning**, **Info**. You can select any number of levels.
3. Select the Trap Format: **SNMPv1 trap**, **Syslog**.
4. Click **Apply**. Event forwarding sources are configured.

Configuring Forwarding Recipients

You can configure up to ten devices to receive forwarded network events.

To add devices to the Recipients List:

1. Click . A row is added to Customized Source List.
2. Enter the IP address of a device to which you want to forward network events.
3. Click **Apply**. The recipient is added to the Customized Source List.

To modify a device's information in the Customized Source List, change the recipient's IP address in the Customized Source List and click **Apply**. The device's information is modified.

To remove devices from the Customized Source List:

1. Select the row with the device's IP address in the Customized Source List.
2. Click .
3. Click **Apply**. The device is removed from the Customized Source List.

12 Remote Access

This chapter provides information about Network Management's remote access capabilities and security issues. It includes the following sections:

- **Introduction to Remote Access** - An introduction to remote access issues.
- **Remote Access and Security** - Information about security issues when running a remote session of Network Management.
- **Starting a Remote Session** - Detailed instructions on how to start a remote session of Avaya Network Management Console.

Introduction to Remote Access

Network Management allows remote access to your network. This enables you to monitor your network from any computer with Internet access. Users can access their network by pointing a web browser at the IP address of their Avaya Network Management Server. The user must enter a username and password. Once these are authenticated, Avaya Network Management Console opens.

Remote Access and Security

Network Management's files are secured by Windows NT's NTFS file system. This prevents unauthorized users from changing Network Management's files. In addition, the web server should be configured to require authentication. This allows only authorized users to access Avaya Network Management Console remotely. For more information on NTFS and configuring the web server, refer to *Microsoft Windows NT/2000 User Guide* and *Avaya Network Manager 5.0 for Windows 2000/XP Installation Guide*.

Remote sessions of Avaya Network Management Console use SNMP version 1. Since this protocol transmits unencrypted information, a firewall will prevent remote access to Network Management if it is configured to do so. In addition, remote sessions of Avaya Network Management Console are read-only. Devices cannot be added, deleted, or modified to the Network Map via remote access.

Starting a Remote Session

To start a remote session of Avaya Network Management Console:

1. Point your web browser to **http://***IP_Address***/nm**, where *IP_Address* is the IP address of the Avaya Network Management Server. The Avaya Network Management Console Remote Entry Page opens.

Figure 12-1. Network Management



2. Click **Open Avaya Network Management Console**. The Java applet starts.

3. A window opens requesting your user name and password.

4. Enter your user name and password, and click **OK**. After a few seconds, Avaya Network Management Console opens.

A Network Management Menus

This appendix gives the full structure of the menus in Network Management. These menus include:

- Avaya Network Management Console Menus
- Discovery Menus
- Event Log Browser Menus
- Event Configuration Menus
- Action List Menus

Avaya Network Management Console Menus

This section gives the full structure of the menus in Avaya Network Management Console. These menus include:

- Avaya Network Management Console File Menu
- Avaya Network Management Console Edit Menu
- Avaya Network Management Console Actions Menu
- Avaya Network Management Console Tools Menu
- Avaya Network Management Console Help Menu

Avaya Network Management Console File Menu

Table A-1. Avaya Network Management Console - File Menu

Item	Description
New	Creates a new Network Object - Map, View, Branch, or Device.
Open	Opens a Network Object.
Save As	Saves a Network Object to a new name.
Import	Imports device information from a CSV file into the current Network Map.

Table A-1. Avaya Network Management Console - File Menu

Item	Description
Export	Exports device information from the current Network Map to a CSV file.
Print	Prints the current Network Map.
Print Preview	Opens the Print Preview window for the Network Map.
Options	Opens the Options dialog box.
Exit	Closes Avaya Network Management Console.

Avaya Network Management Console Edit Menu

Table A-2. Avaya Network Management Console - Edit Menu

Item	Description
Modify	Opens the Modify dialog box for the selected object.
Delete	Deletes the selected object from the Network Map.
Modify View	Opens the Modify View dialog box.
Delete View	Deletes the current custom view.
Cut	Cuts the selected object in a custom view to the clipboard.
Paste	Pastes the object from the clipboard into a custom view.
Manage	Manages a currently unmanaged Network Object.
Unmanage	Unmanages a currently managed Network Object.
Find	Opens the Find dialog box.

Avaya Network Management Console View Menu

Table A-3. Avaya Network Management Console - View Menu

Item	Description
System View Log	Opens the System View log.
Tooltip	Toggles the display of device tooltips.

Avaya Network Management Console Actions Menu

Table A-4. Avaya Network Management Console - Actions Menu

Item	Description
System View Discovery	Performs System View Discovery.
Event Manager	Opens the Event Log Browser.
IP Discovery	Opens the Discovery window.
Get Write Permission	Request read/write permission for your console session.
Release Write Permission	Release read/write permission for your console session.

Avaya Network Management Console Tools Menu

Table A-5. Avaya Network Management Console - Tools Menu

Item	Description
Voice Applications	Provides access to the following submenus: • **Avaya Site Administration** - Connects to the switch controlling a supported voice device and opens the appropriate form. • **Avaya Terminal Emulator** - Launches Avaya Terminal Emulator. • **Avaya SMON Manager** - Launches Avaya SMON Manager. • **Avaya MultiSite Administration** - Launches Avaya MultiSite Administration. • **Avaya Fault and Performance Manager** - Launches Avaya Fault and Performance Manager. • **Avaya VAL Manager** - Launches Avaya VAL Manager.
Avaya Software Update Manager	Launches Avaya Software Update Manager.
Avaya Device Manager	Launches the Device Manager for the selected device.
Avaya VLAN Manager	Launches Avaya VLAN Manager.
Avaya Network Configuration Manager	Launches Avaya Network Configuration Manager.
Avaya Address Manager	Launches Avaya Address Manager.
Avaya VPNmanager	Launches Avaya VPNmanager.
Avaya Wireless	Launches Avaya Wireless (AP) Manager.
Telnet	Launches a Telnet session to the selected device.
Web	Launches a Web session to the selected Avaya P330 or Avaya P580/P882 Device.
Ping	PINGs the selected device.

Avaya Network Management Console Help Menu

Table A-6. Avaya Network Management Console - Help Menu

Item	Description
Contents	Opens the on-line help to the contents page.
Help On	Activates context-sensitive help.
About Avaya Network Management Console	Opens the About dialog box showing the copyright and version information for Avaya Network Management Console.

Discovery Menus

This section gives the full structure of the menus in the Discovery window. These menus include:

- **Discovery File Menu**
- **Discovery Edit Menu**
- **Discovery View Menu**
- **Discovery Actions Menu**
- **Discovery Help Menu**

Discovery File Menu

Table A-7. Discovery - File Menu

Item	Description
Update Map	Updates the current Network Map with the results of the latest Discovery, and saves the Network Map to the Network File.
Options	Opens the Discovery options dialog box.
Exit	Closes the Discovery window.

Discovery Edit Menu

Table A-8. Discovery - Edit Menu

Item	Description
Add	Opens the Add Subnet dialog box.
Modify	Opens the Modify Subnet dialog box.
Select	Checks the Discover field for the selected subnets.
Unselect	Unchecks the Discover field for the selected subnets.
Delete	Deletes the selected subnet from the Subnets Table.
Delete All	Deletes all subnets from the Subnets Table.

Discovery View Menu

Table A-9. Discovery - View Menu

Item	Description
Discovery Log	Toggles the display of the Discovery Log.

Discovery Actions Menu

Table A-10. Discovery - Actions Menu

Item	Description
Discover	Starts a Discovery based on the contents of the Subnets Table.
Schedule Network Discovery	Opens the Scheduler dialog box.
Stop Network Discovery	Stops the Discovery process.

Discovery Help Menu

Table A-11. Discovery - Help Menu

Item	Description
Contents	Opens the on-line help to the first topic.

Table A-11. Discovery - Help Menu

Item	Description
Help On	Activates context-sensitive help.

Event Log Browser Menus

This section gives the full structure of the menus in the Event Log Browser. These menus include:

- Event Log Browser File Menu
- Event Log Browser Edit Menu
- Event Log Browser View Menu
- Event Log Browser Help Menu

Event Log Browser File Menu

Table A-12. Event Log Browser - File Menu

Item	Description
Options	Opens the Trap Log Options dialog box.
Export	Saves the Event Log to a file.
Exit	Closes the Event Log.

Event Log Browser Edit Menu

Table A-13. Event Log Browser - Edit Menu

Item	Description
Delete	Deletes the selected traps.
Acknowledge	Acknowledges the selected traps.
UnAcknowledge	Unacknowledges the selected traps.
Select All	Select all traps visible in the Trap Table.
Change Severity > Change severity to Info	Changes the severity of the selected traps to Info.
Change Severity > Change severity to Warning	Changes the severity of the selected traps to Warning.

Table A-13. Event Log Browser - Edit Menu

Item	Description
Change Severity > Change severity to Minor	Changes the severity of the selected traps to Minor.
Change Severity > Change severity to Major	Changes the severity of the selected traps to Major.
Change Severity > Change severity to Critical	Changes the severity of the selected traps to Critical.
Modify Event	Opens the Modify Event dialog box.

Event Log Browser View Menu

Table A-14. Event Log Browser - View Menu

Item	Description
Filter > Severity Filter	Opens the Severity Filter dialog box.
Filter > IP Address Filter	Opens the IP Address Filter dialog box.
Filter > Device Type Filter	Opens the Device Type Filter dialog box.
Filter > Acknowledge Filter	Opens the Acknowledged Filter dialog box.
Filter > No Filter	Displays all events in the Trap Table.

Event Log Browser Help Menu

Table A-15. Event Log Browser - Help Menu

Item	Description
Contents	Opens the on-line help to the first topic.
Help On	Activates context-sensitive help.

Event Configuration Menus

This section gives the full structure of the menus in the Event Configuration window. These menus include:

- Event Configuration File Menu
- Event Configuration Edit Menu
- Event Configuration Tools Menu
- Event Configuration Help Menu

Event Configuration File Menu

Table A-16. Event Configuration - File Menu

Item	Description
Exit	Closes the Event Log.

Event Configuration Edit Menu

Table A-17. Event Configuration - Edit Menu

Item	Description
Apply	Applies the changes to the Event Table to the network.
Revert	Undoes all unapplied changes.
Modify Event	Opens the Modify Event dialog box.

Event Configuration Tools Menu

Table A-18. Event Configuration - Tools Menu

Item	Description
Action List	Opens the Action List window.
Event Forwarding	Opens the Event Forwarding Options dialog box.

Event Configuration Help Menu

Table A-19. Event Configuration - Help Menu

Item	Description
Contents	Opens the on-line help to the first topic.
Help On	Activates context-sensitive help.

Action List Menus

This section gives the full structure of the menus in the Action List window. These menus include:

- Action List File Menu
- Action List Edit Menu
- Action List Tools Menu
- Action List Help Menu

Action List File Menu

Table A-20. Action List - File Menu

Item	Description
Exit	Closes the Action List.

Action List Edit Menu

Table A-21. Action List - Edit Menu

Item	Description
Apply	Applies the changes to the Action List to the network.
Revert	Undoes all unapplied changes.
Add	Opens the Add Action dialog box.
Modify	Opens the Modify Action dialog box.
Delete	Deletes the selected actions.

Action List Tools Menu

Table A-22. Action List - Tools Menu

Item	Description
Options	Opens the Action List Options dialog box.

Action List Help Menu

Table A-23. Action List - Help Menu

Item	Description
Contents	Opens the on-line help to the first topic.
Help On	Activates context-sensitive help.

Index

A
Acknowledging traps 102
Action
  audio files 110
  fields 108
  form area 96
  options 111
  scripts 109
  table 96
Action list
  applying changes 110
  Edit menu 128
  File menu 128
  Help menu 129
  menus 128
  toolbar 95
  Tools menu 129
  user interface 94
Actions
  adding 106
  defining 105
  deleting 110
  modifying 107
  overview 105
Adding
  actions 106
  devices to the network file 45
  subnets 79
Application launcher 49
Applying changes to the action list 110
Assign action
  fields 92
  form 92
Assigning actions to events 112
Audio files 110
Avaya Network Management console
  Actions menu 121
  Edit menu 120
  File menu 119
  help 29
  Help menu 123
  menus 119
  overview 4, 13
  starting 13
  starting a remote session 118
  status bar 17
  Tools menu 122
  user interface 14
  View menu 121
  what is 4
Avaya Network Management server 10
  introduction 10
  overview 4
  starting 10
  stopping 12
  what is 4

C
Closing the event manager 96
Configuring
  discovery method and range 68
  discovery options 67
  discovery's naming method 70
  event forwarding 114
  event forwarding recipients 116
  events 112
  router access parameters 83
  SMTP server 111
Connectivity polling 26

D
Defining actions 105
Deleting
  actions 110
  devices 48
  error messages from the discovery log 84
  subnets 82
  traps 103
Determining best names 70
Device
  applications 49
  manager 50
  modifying parameters 46
  parameters 46
  SMON 55
  type view 33, 34
Dialog area
  Avaya Network Management console 17
  discovery 66
Discovering
  all subnets and nodes 76

nodes on a specific subnets 77
subnets already in the network map 84
subnets and nodes 75
Discovery 67
Actions menu 124
closing the window 66
configuring method and range 68
configuring naming method 70
deleting error messages from the discovery log 84
dialog area 66
Edit menu 124
File menu 123
log 82
log area 66
menus 123
method 68
overview 6
range 68
saving the log 84
scheduling 74
selecting device types 73
setting options 67
starting 62
status bar 66
toolbar 64
user interface 63
View menu 124
what is 6
window 63

E

Editing severity levels 103
E-mail settings 111
Event configuration
Edit menu 127
File menu 127
Help menu 128
menus 127
toolbar 91
Tools menu 127
user interface 90
Event forwarding
configuring 114
configuring recipients 116
sources 116
Event handling
overview 6
what is 6
Event log browser
Edit menu 125
File menu 125
Help menu 126
menus 125
status line 90
toolbar 88
user interface 87
View menu 126
Event manager 86
closing 96
overview 86
user interface 87
viewing 87
Event table 91
Events
assigning actions to 112
configuring 112
Exporting the network file 60

F

Fields
action 108
action table 96
event table 91
Filtering traps 99
by acknowledged 101
by device type 101
by IP address 100
by severity level 99
Form area
action 96
assign action 92

H

Help
contents page 29
context sensitive 29
using 29
How to
acknowledge traps 102
add actions 106
add devices to the network file 45
apply changes to the actions list 110
assign actions to events 112
close the event manager 96
configure discovery method 68
configure discovery range 68
configure discovery's naming method 70
configure event forwarding 114
configure events 112
configure forwarding recipients 116
configure router access parameters 83
define actions 105
delete actions 110
delete devices 48
delete error messages from the discovery log 84
delete subnets 82

delete traps 103
discover all subnets and nodes 76
discover nodes on a specific subnet 77
edit severity levels 103
export network files 60
filter traps 99
filter traps by acknowledged 101
filter traps by device type 101
filter traps by IP address 100
filter traps by severity level 99
import devices into the network file 59
launch a web session 55
launch device manager 50
launch device SMON 55
launch Telnet 50
manage traps 97
manually add subnets 79
modify actions 107
modify device parameters 46
modify subnets 79
open context-sensitive help 29
open the help to a topic of interest 29
open the help to the contents page 29
print the network file 39
refresh the network map 84
save the discovery log 84
save the trap table 104
schedule discovery operation 74
search for a device 40
select default Network Map 27
select device types to discover 73
select elements 29
select event forwarding sources 116
set action options 111
set connectivity polling 26
set discovery options 67
set IP SNMP access parameters 25
set SNMP access parameters 21
set SNMP access parameters for IP ranges 23
set SNMP default access parameters 21
start a remote session of Avaya Network Management console 118
start Avaya Network Management console 13
start Avaya Network Management server 10
stop Avaya Network Management server 12
switch views 32
use Avaya Network Management console help 29
use the discovery log 82
use tool tips 18
view all traps 102
view the event manager 87

I

Importing devices into the network file 59
Introduction
Avaya Network Management server 10
event manager 86
network tree 31

L

Launching
device manager 50
device SMON 55
Telnet 50
web session 55

M

Managing
events 97
traps 97
Manually adding subnets 79
Modifying
actions 107
device parameters 46
subnets 79

N

Network
table 17
tree 31
Network file
adding devices 45
exporting devices 60
importing devices 59
printing 39
Network Management
concepts 1
definitions 3
in standalone mode concepts 1
overview 2
terms 3
Network Map
overview 5
selecting default 27
what is 5
Network view area, using 41
Network-wide applications 55

O

Opening the Discovery window 62
Options 67
Organization of this manual viii
Overview

actions 105
Avaya Network Management server 4
discovery 6
event handling 6
event manager 86
Network Management in standalone mode 2
Network Map 5
remote access 9

P
Permissions
read only 18
read/write 18
setting defaults 28
PINGing devices 51
Printing the network file 39
Purpose of this manual viii

R
Read/Write Defaults
setting 28
Refreshing the network map 79
Remote access
overview 9
what is 9
Requesting write permissions 18

S
Saving
the discovery log 84
trap table 104
Scheduling
discovery operation 74
Searching the tree view 40
Selecting
device types to discover 73
elements 29
Setting Read/Write Defaults 28
Severity levels, editing 103
SNMP access parameters
configuring 21
default parameters 21
IP ranges 23
specific IP parameters 25
Sources of events to forward 116
Specifying a subnet to discover 77
Starting
a remote session of Avaya Network Management console 118
Avaya Network Management console 13
Avaya Network Management server 10
Status bar
discovery 66
user interface 17
Status line, event log browser 90
Stopping Avaya Network Management server 12
Subnet
deleting 82
parameters 81
table 65
view 33

T
Table
row status, deleted 29
row status, modified 29
row status, new entry 29
subnets 65
Telnet 50
Toolbar 16
action list 95
discovery 64
event configuration 91
event log browser 88
Tooltips 18
Trap fields 89
Trap table
fields 89
saving 104
Traps
acknowledging 102
deleting 103
filtering 99
viewing 102
viewing all 102
Tree view 17, 32
searching 40

U
User Administration
Actions menu 124
User interface 14
action list 94
dialog area 17
event configuration window 90
event log browser 87
event manager 87
network table 17
status bar 17
toolbar 16
tooltips 18
tree view 17
Using
action scripts 109
Avaya Network Management console help 29

the discovery log 82
the network view area 41

V
View
device type 33, 34
subnet 33
Viewing
the event manager 87
traps 102

W
Web session 55
What is
Avaya Network Management console 4
Avaya Network Management server 4
discovery 6
event handling 6
remote access 9
Who should use this manual viii