Avaya Integrated Management Release 5.0

Network Management Console

14-300169
Issue 7
January 2008

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the website, simply go to http://www.avaya.com/support **and search for the document number in the search box.**

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Contents

Contents

Preface

Welcome to Avaya Network Management. 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.
- Organization of This Manual - The structure of this manual.

The Purpose of This Manual

This manual contains information needed to use Avaya Network Management, 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.
- Avaya Network Management - An overview of Avaya Network Management, 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 VoIP System View for networks containing VoIP devices. It also includes instructions on how to create custom views and search the tree.
- Launching Applications - Instructions on how to launch device-specific and network-wide applications from Avaya Network Management Console.
- Avaya Network Management Console Tables - A description of the contents of the Avaya Network Management Console network table in different views, and instructions on how to add, delete, and modify objects in the table.
- 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.
- Configuration Wizard - Information and instructions for using the Configuration Wizard.
- 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 Avaya Network Management 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 using 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.
- Network Management Menus - A description of the structure of the menus in the Network Management Console.

Chapter 1: Avaya Network Management

This chapter provides an overview and general description of Avaya Network Management. It includes the following sections:

- Avaya Network Management Overview - A general description of Avaya Network Management.
- Avaya Network Management 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.

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

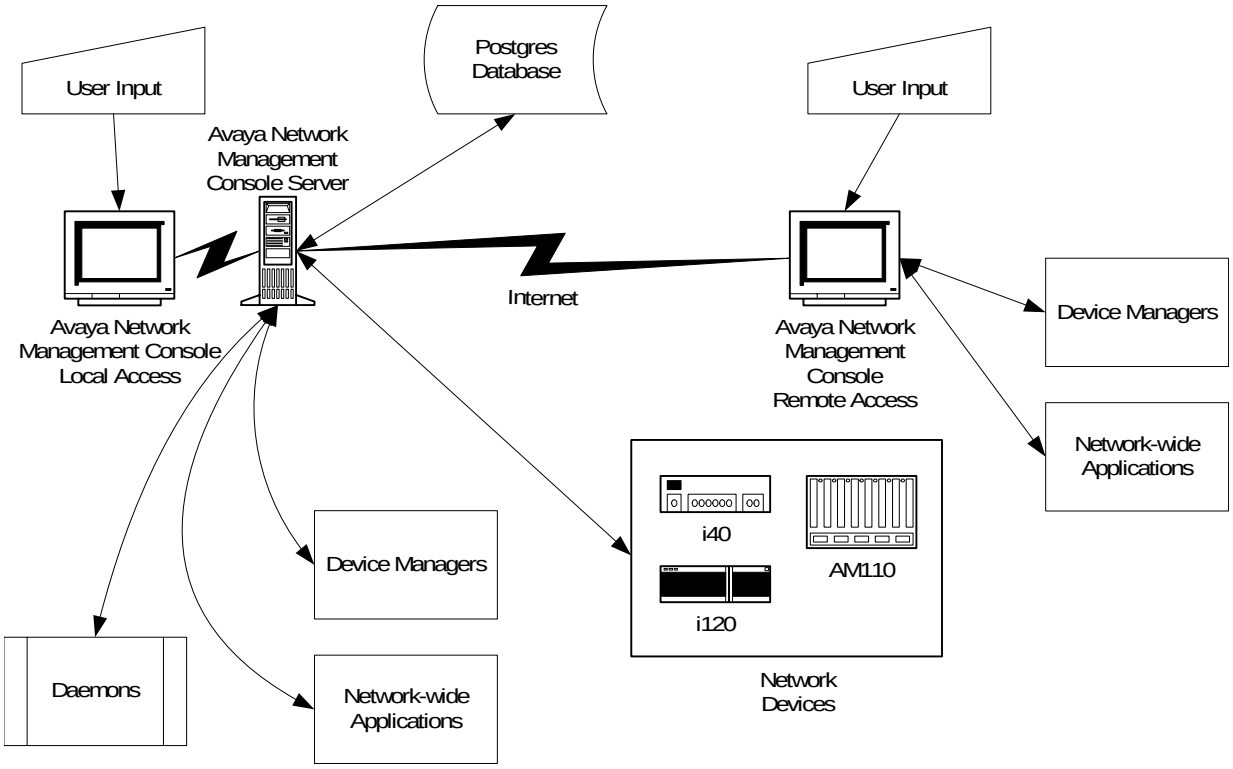
Avaya Network Management Overview

Avaya Network Management 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, Avaya Network Management provides a Discovery service that can search your network for devices and an Event Log that reports network events.

Avaya Network Management uses a client/server architecture, enabling 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 Avaya Network Management and Avaya Network Management applications.

Figure 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.

Avaya Network Management Terms

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

Table 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 116.
Branch	An intermediate level in the Network Tree. Branches include device types, subnets, and user defined branches in custom views of the network.
Postgres Database	A database 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

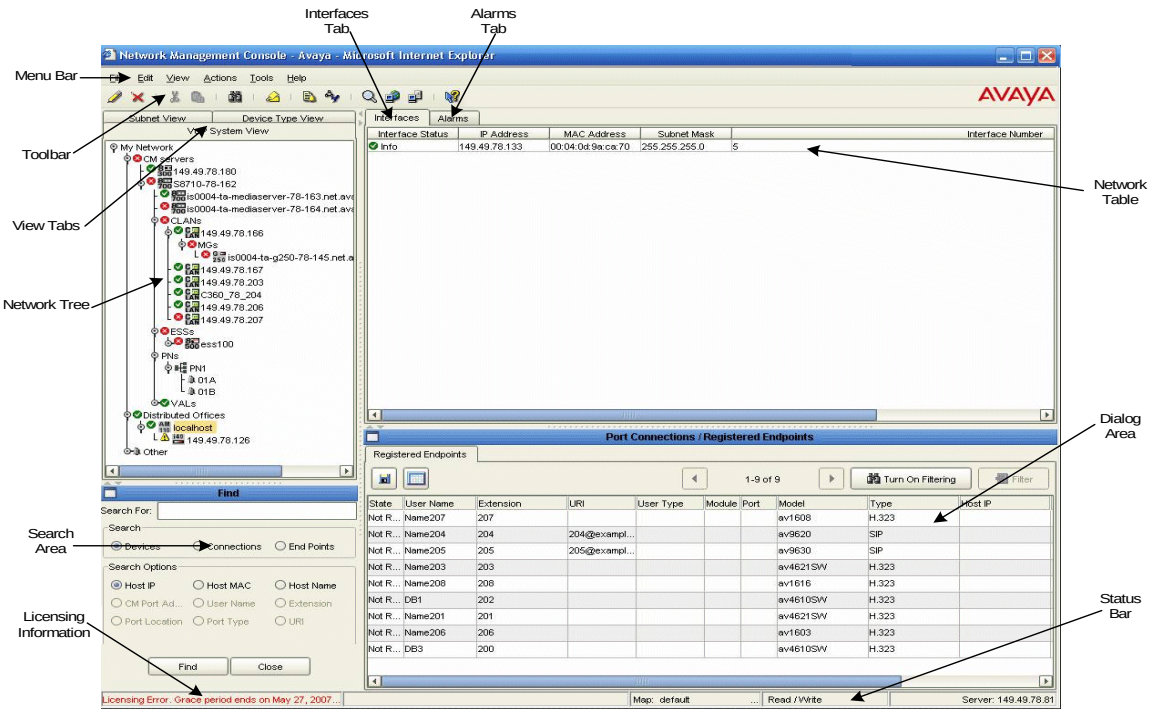
Avaya Network Management Server communicates with the devices in the network via Simple Network Management Protocol (SNMP) V1 or V3. It receives user input via Avaya Network Management Console and updates Avaya Network Management Console with information from the network devices. Avaya Network Management Server runs in the background as a Windows Vista/2003/2000/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 18.

In addition, Avaya Network Management Server enables 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 Starting Avaya Network Management Console on page 26.

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 voice system hierarchy. Additionally, you can create custom views of the network.

Figure 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 G350 Device in the Network Table, you can launch Telnet to configure the device via its CLI, or launch Avaya G350 Device Manager to configure and monitor the device via its management application. In addition, Avaya Network Management Console allows you to launch network-wide applications such as, Avaya Software Update Manager for updating embedded software.

What is a Network Map

A Network Map consists of all of the devices known to Avaya Network Management Server, their physical connectivity to ports, and their relationship in the voice hierarchy. The list of devices is stored in the database, 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 database. 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 database.

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.

Note:

Changing the map affects all open network-wide applications.

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 95.

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 95.

What is Discovery

Avaya Network Management uses Discovery to detect or ’discover’ your network. The Discovery tool discovers subnets and nodes, the physical port location of the devices, the Avaya VoIP hierarchy, phone information and phone locations for IP, analog and digital phones. 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, limit the search to selected subnets, or update information about the objects in the Network View.

The Discovery window displays the results of your search. 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.

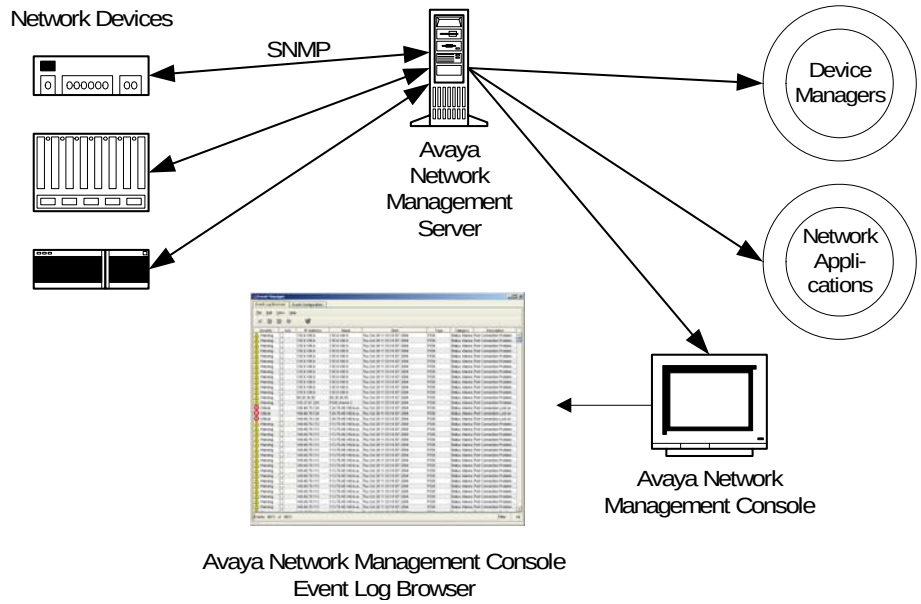
Note:

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.

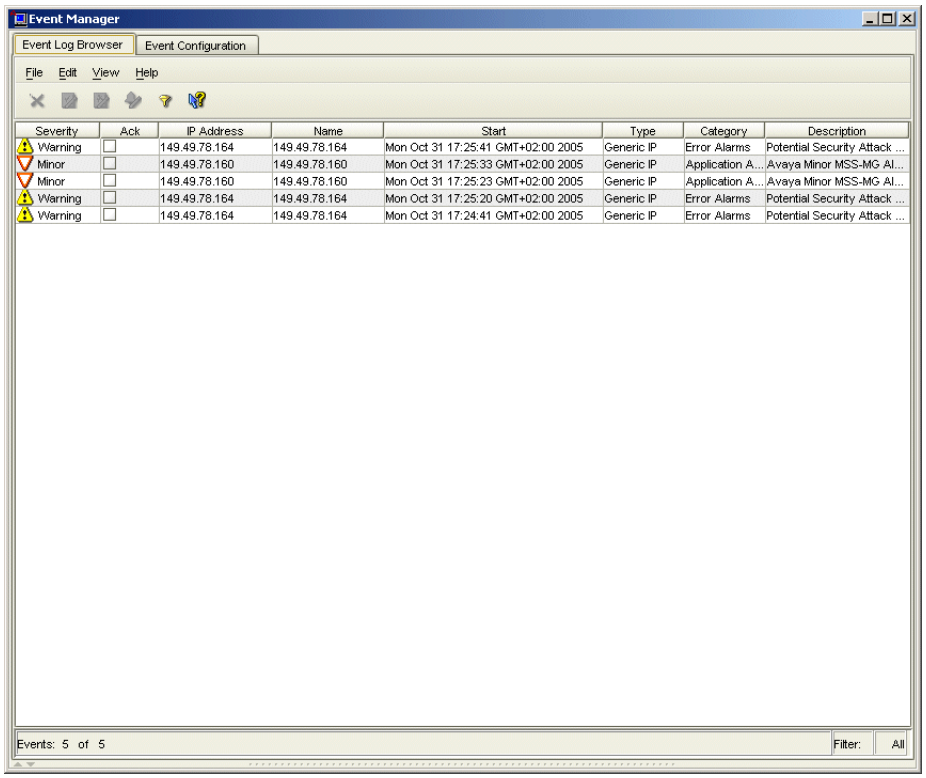
To receive traps using Avaya Network Management, network devices must be configured to send traps to the Avaya Network Management Server. For information on configuring Avaya LAN and backbone devices to send traps to Avaya Network Management Server, refer to the User Guide or Device Manager User Guide 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 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 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's New in This Release

Avaya Network Management Console Release 5.0 introduces the following enhancements:

- Support for Avaya Communication Manager Release 5.0:
  - You can automatically configure Avaya Communication Manager Release 5.0 to work with Avaya Network Management Console.
  - All digital and analog phones that work with Avaya Communication Manager Release 5.0 are discovered and displayed in Avaya Network Management Console.
- Support for the S8300C (Avaya Communication Manager/SES co-residency):
  - The S8300C is displayed in VoIP System View as a branch under the co-resident Avaya Communication Manager.
  - SIP phones registered to the SES are discovered and displayed in Avaya Network Management Console. You can search for these phones in the Port Connection table.
- Support for the G450 branch gateway (including discovery, display in System View, trap formatting, fault monitoring, administration, and port connections).
- Support for the G860 high density trunk gateway.
- Support for the following routers with the IG550 Integrated Gateway (including discovery, display in System View, trap formatting, fault monitoring, and administration):
  - J2320
  - J2350
- Support for the following media modules on the IG550 Integrated Gateway:
  - TIM508 (8-port FXS Analog Telephony Interface Module)
  - TIM516 (16-port FXS Analog Telephony Interface Module)
  - TIM518 (8+8-port FXS/FXO Analog Telephony Interface Module)
- Support for the following new set types:
  - 9630G IP Telephone
  - 9640G IP Telephone
- The ability to manage IP Office devices. You can now run IP Office Manager R6.1 and Avaya Provisioning and Installation Manager for IP Office from Network Management Console.

Chapter 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 > Start Avaya Services**.

To view the status of Avaya Network Management Server:

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

Stopping Avaya Network Management Server

To stop Avaya Network Management Server:

Select **Start > Programs > Avaya > Stop Avaya Services**.

Chapter 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, information about security issues when accessing Avaya Network Management Console from a web browser, and licensing information.
- 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.

Starting Avaya Network Management Console

Avaya Network Management Console is a java applet running in a browser. 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.

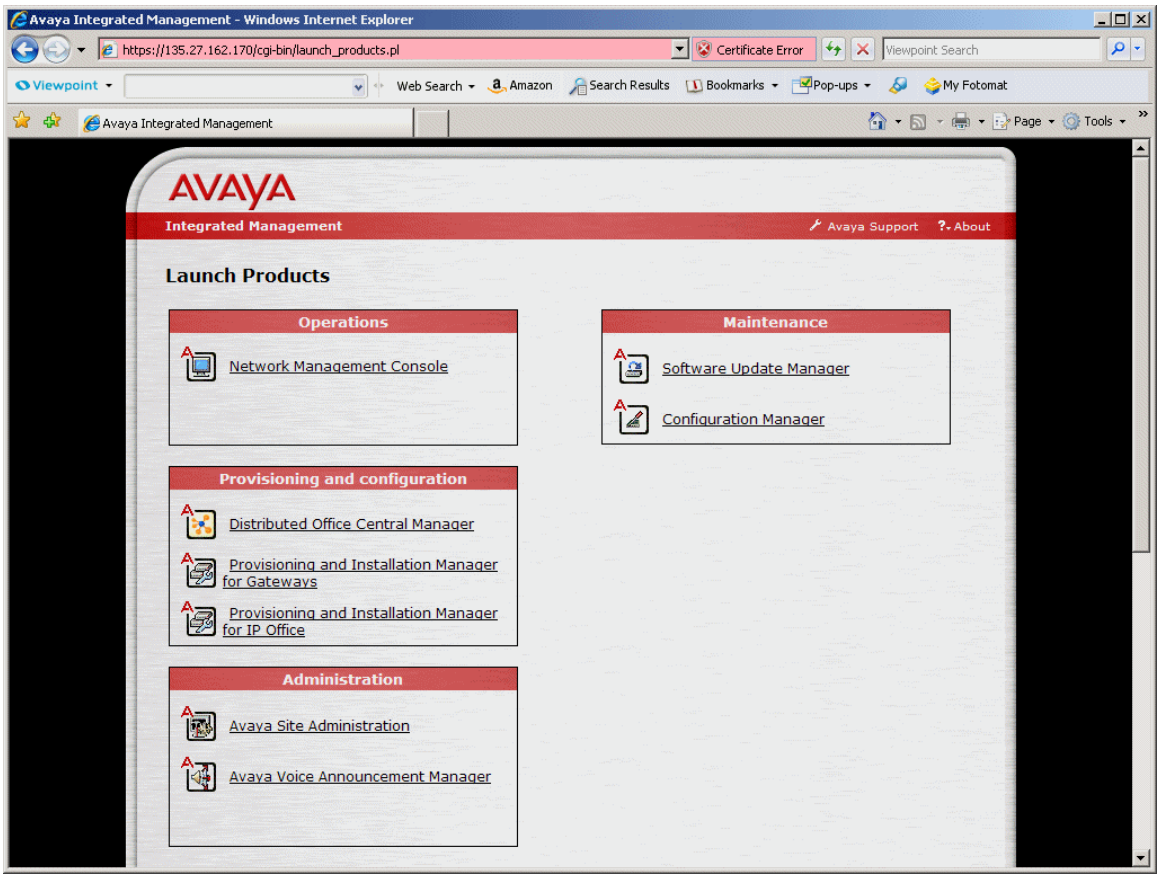
To start a local session of Avaya Network Management Console from the server:

1. Double-click the **Avaya Integrated Management** link on the Windows desktop. Avaya Integrated Management home page is launched.
2. From the Avaya Integrated Management home page, click the **Network Management Console** link to launch Avaya Network Management Console.

To start a session of Avaya Network Management Console from a client machine:

1. Point your web browser to **http://*IP_Address*/** where *IP_Address* is the IP address of the Avaya Network Management Server. The Avaya Integrated Management entry page opens (see Figure 5).

Figure 5: Avaya Integrated Management Home Page



2. Click **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.

Remote Access and Security

You can access Avaya Network Management Console from any computer, using a web browser. 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 is configured to work with HTTPS, and login to Avaya Network Management Console requires authentication. This enables only authorized users to access Avaya Network Management Console remotely. For more information on NTFS, refer to your Microsoft Windows user guide.

Avaya Network Management Console communicates with devices using SNMP. Only the SNMPv3 protocol is encrypted and requires authentication. It is, therefore, highly recommended that you use the SNMPv3 protocol.

Licensing Requirements

Avaya Network Management Console is a licensed product. Upon installation, you have 30 days to install a product license. Login will be disabled if your license is not installed after 30 days. A warning message displaying the product expiry date is shown during login and the license expiry date is displayed in the status bar, until the license is installed. For further details please refer to the *Avaya Integrated Management Release 5.0 Enterprise Network Management Installation and Upgrade Guide 14-300444*.

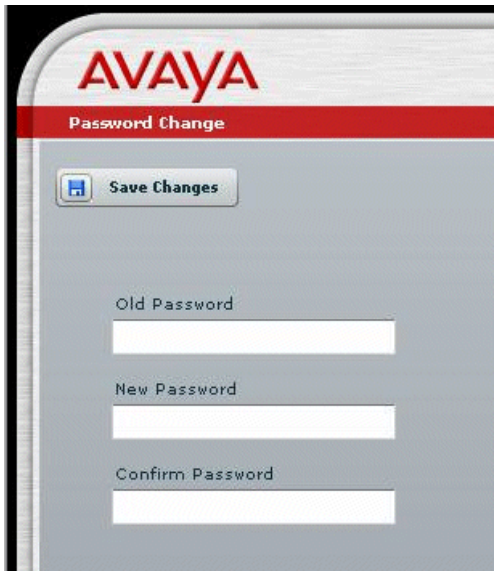
Changing Passwords

You can change your password through Avaya Network Management Console.

To change your password:

1. Select **Actions > Change Password**. The Password Change window opens.

Figure 6: Password Change Window



2. Enter your old password in the `Old Password` field.
3. Enter your new password in the `New Password` field.
4. Enter your new password in the `Confirm Password` field.
5. Click Save Changes.

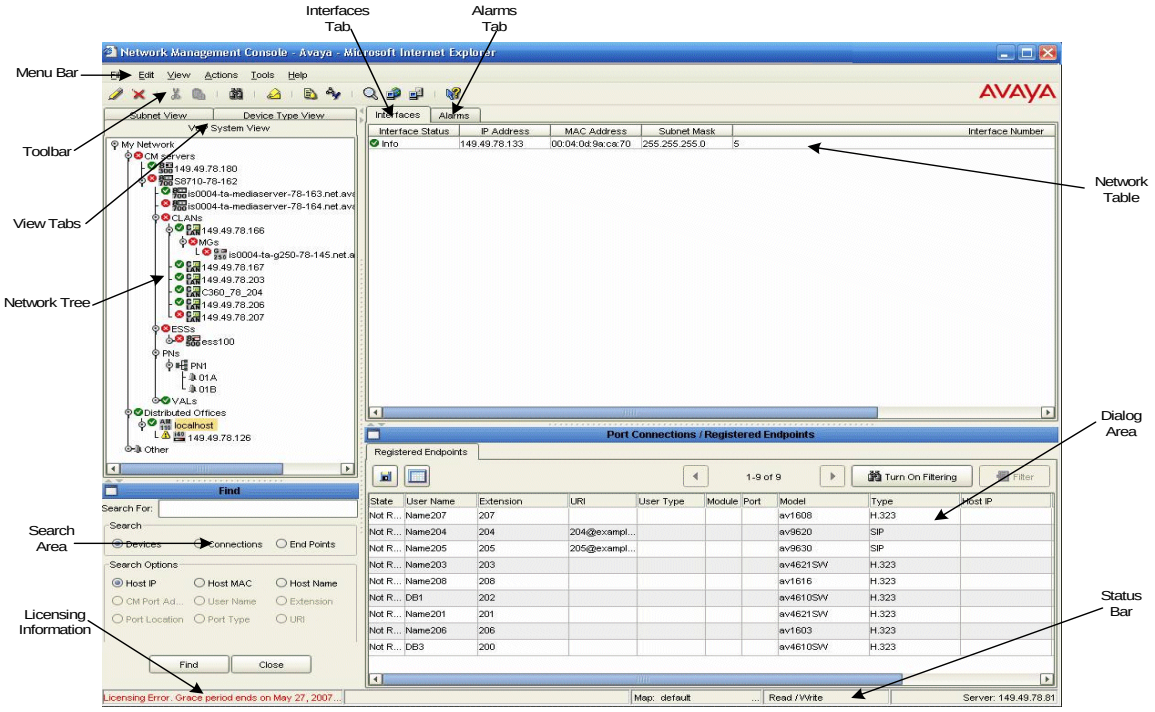
Avaya Network Management Console User Interface

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.
- Interfaces Tab - Displays a table where details about the branches and nodes in the Network Tree are displayed.
- Alarms Tab - Displays a table where alarms reported for devices on the network are displayed.
- Modules Tab - Displays a table where a list of modules and the module type are displayed.
- Dialog Area - A resizeable window where all dialog boxes open.
- Status Bar - Displays information about the current Avaya Network Management Console session and license expiry information.

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

Figure 7: 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 2: 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 object**
	Cuts the selected object from a custom view to the clipboard.	**Edit > Cut object**
	Pastes the object from the clipboard into a custom view.	**Edit > Paste object**
	Opens the Find dialog box.	**Edit > Find**
	Opens the Port Connections/Registered Endpoints Table.	**View > Connections/ Endpoints**
	Opens the Inventory Table.	**View > Inventory**
	Opens the Event Manager.	**Actions > Event Manager**
	Opens the Discovery window.	**Actions > IP Discovery**
	Launches the device manager for the selected device.	**Tools > Avaya Device Manager**
	Launches a web session to the selected device.	**Tools > Web**
	Launches a Telnet session to the selected device.	**Tools > Telnet**
	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 voice system hierarchy. 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.

Interfaces Tab

The Interfaces Tab displays the 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 6: Avaya Network Management Console Tables.

Alarms Tab

The Alarms Tab displays a list of alarms reported by the device selected in the Network Tree. The Alarms Tab is only enabled for devices supporting alarms. In the current release, only AM110 devices and IP Office devices are supported. The Alarms Tab displays current problems, faults associated with any device displayed, and severity. For more information about Alarms, refer to Viewing and Searching the Tables on page 74.

Modules Tab

The Modules Tab displays a list of modules and the module type that are part of the MG/Carrier. Module index. For more information about the Modules table, refer to The Modules Table on page 77.

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

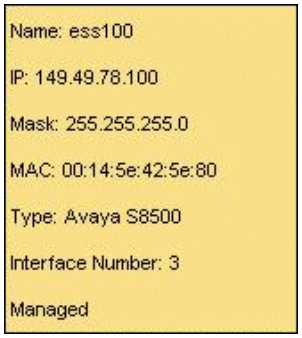
The Status Bar provides information about the Avaya Network Management Console session. It includes the following information:

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

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 8: 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.
- **Extension** - The extension of the device if the device is an IP phone.

- **Management Status** - The device's management status. This can be either **Managed** or **Unmanaged**.

Tooltips for Carriers provide the following information:

- **Building** - The building in which the carrier is physically located.
- **Floor** - The floor on which the carrier is physically located.
- **Room** - The room in which the carrier is physically located.

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

Requesting Write Permission

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

- 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 43.

All functionality is supported 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
- Setting CM Server Parameters

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 Avaya Secure Access 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.

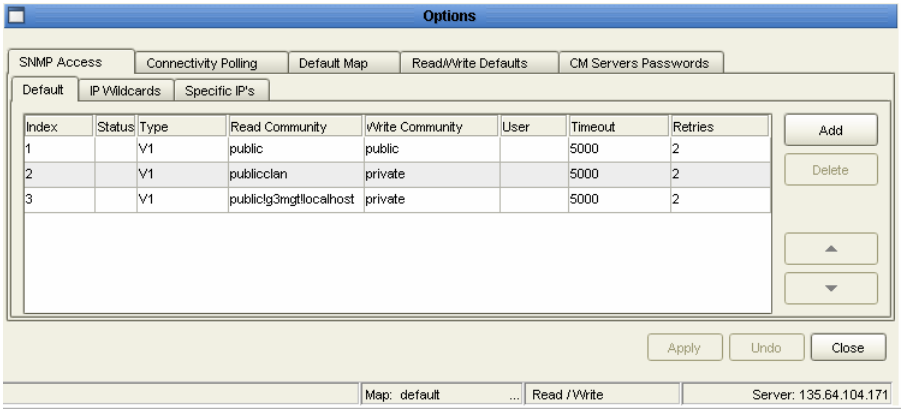
Default SNMP Access Parameters

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 Options dialog box. The Default page appears.

Figure 9: 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** from the `Type` drop-down list.
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` drop-down list. The user name must be defined in the Secure Access Administration application. For more information, refer to the *Avaya Secure Access Administration User 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 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:

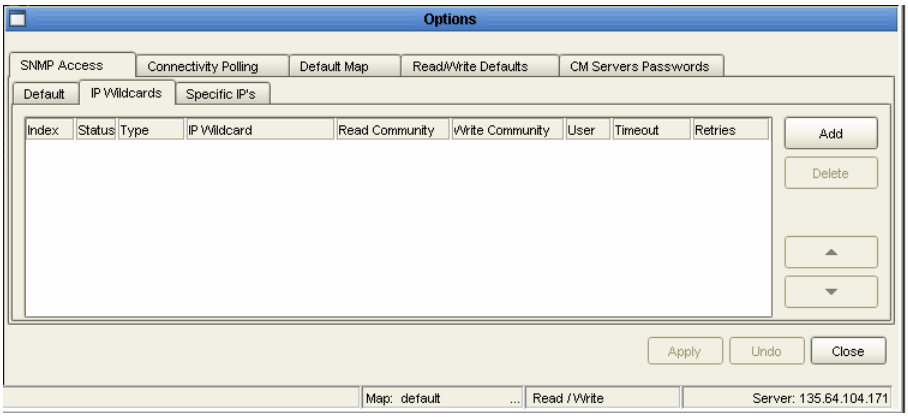
1. Select a range.
2. Click **Delete**.
3. Click **Apply**. The range is deleted from the Default table.

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 10: 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** from the `Type` drop-down list.
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` drop-down list. The user name must be defined in the Secure Access Administration application. For more information, refer to the *Avaya Secure Access Administration User 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 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.

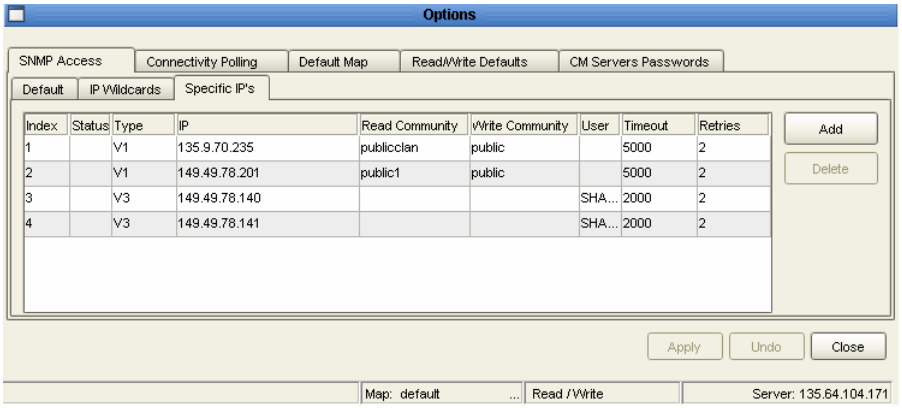
To remove a range from the IP Wildcards table:

1. Select a range.
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 Options dialog box. The Specific IP's page appears.

Figure 11: 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 from the `Type` drop-down list.
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 drop-down list. The user name must be defined in the Secure Access Administration application. For more information, refer to the *Avaya Secure Access Administration User 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.

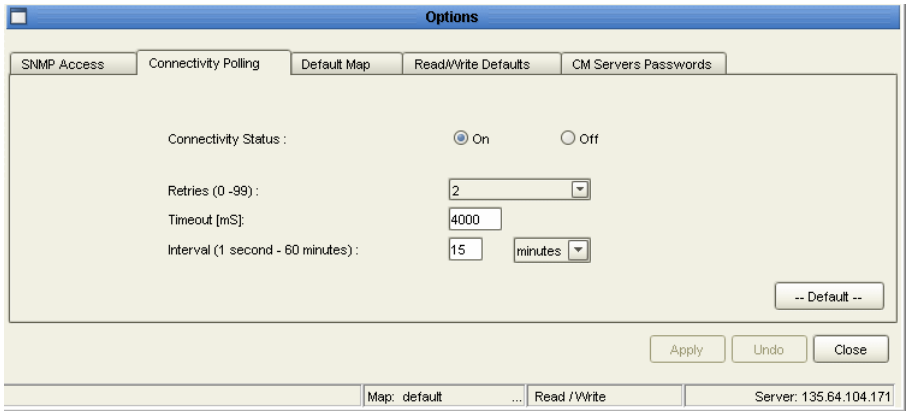
Setting Connectivity Polling Parameters

Connectivity polling parameters determine whether Avaya Network Management Server 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 unsuccessfully PINGs 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 Options dialog box. The Connectivity Polling page appears.

Figure 12: Options Dialog Box - Connectivity Polling Page



2. Select a Connectivity Status. **On** means that devices are PINGed. **Off** means that devices are not PINGed.
3. Enter a number in the `Retries` field. This is the number of times Avaya Network Management Server unsuccessfully PINGs 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 waits 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.

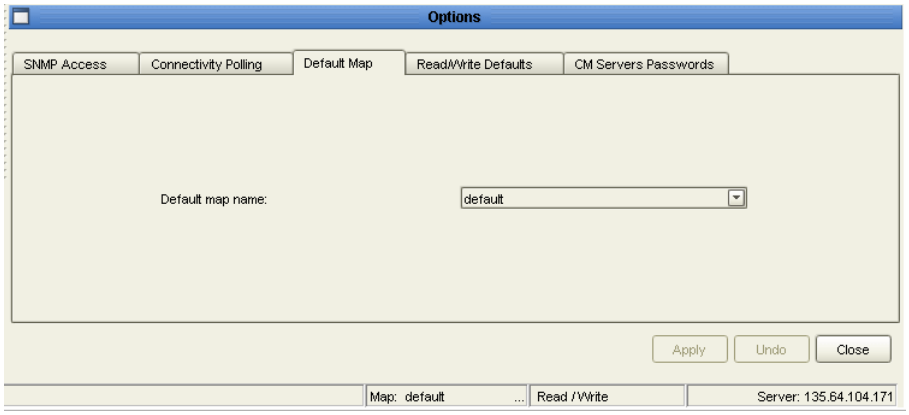
Selecting a Default Map

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 Options dialog box. The Default Map page appears.

Figure 13: Options Dialog Box - Default Map Page



2. Select a Network Map from the **Default map name** drop-down list.
3. Click **Apply**. The selected map is now the default Network Map.

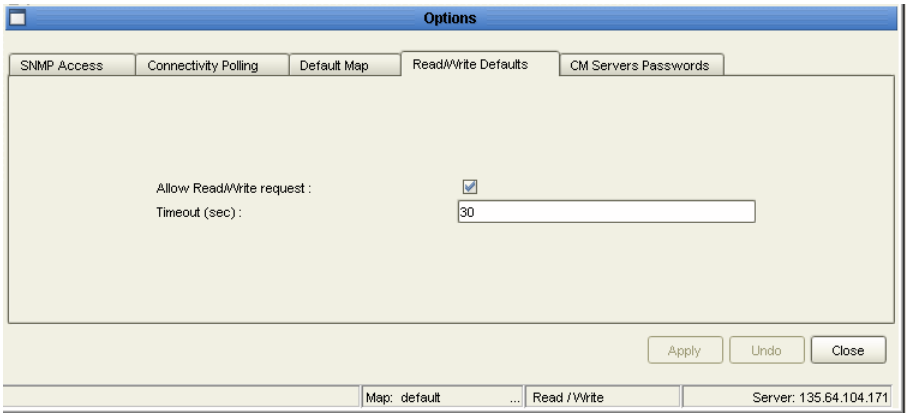
Setting Read/Write Defaults

The Read/Write Defaults page of the 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 Options dialog box. The Read/Write Defaults page appears.

Figure 14: Options Dialog Box - Read/Write Defaults Page



2. Click the **Allow Read/Write request** checkbox to enable a user to request read/write permission. If this option 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**.

Setting CM Server Parameters

The CM Servers Passwords page of the Options dialog box enables you to set the login parameters to connect to CM servers in your network.

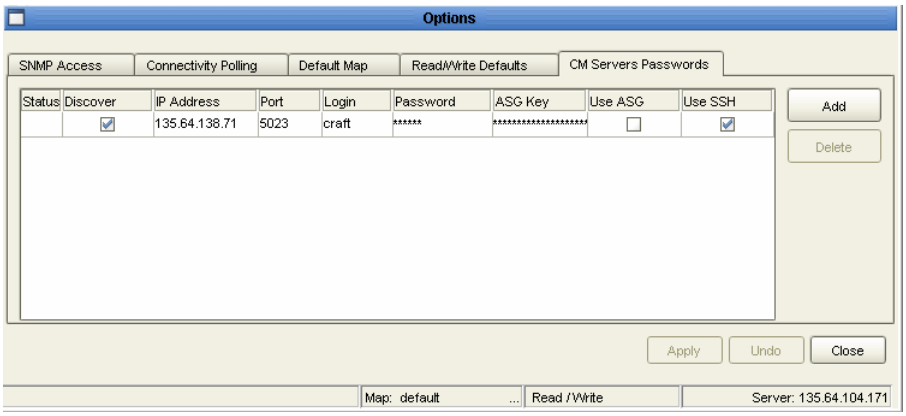
Note:

To discover analog, digital or IP phones, you must add the relevant CM Login parameters to the table.

To set CM server login parameters:

1. Click the **CM Servers Passwords** tab at the top of the Options dialog box. The CM Servers Passwords page appears.

Figure 15: Options Dialog Box - CM Server Passwords Page



2. Click **Add** to add a new CM server with which you wish to connect.
3. Click **Discover** to add the CM server to the list of devices Network Management Console attempts to discover.
4. Enter the IP address of the CM server.
5. Enter the login ID and password to access the CM server.
6. Enter the ASG key, if ASG encrypted login is used.
7. Select the encrypted login method. Possible values are **ASG** and **SSH**.
8. Click **Apply**.

Note:

The ASG key is a 20-character octal code, the 19th character of which must be either 0, 2, 4, or 6, and the 20th character of which must be 0.

Configured CM servers are queried for associated IP phone information (user name and extension). To view this information:

- Place your mouse over the discovered IP phone and view the tooltip.

  Or

- Click any branch of the Network View Tree containing an IP phone.

  Or

- View the connection dialog.

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

Chapter 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 how to use 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 VoIP system view, which includes the voice elements in a data network, and the relationships between VoIP registered endpoints, 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 VoIP 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 VoIP 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 VoIP System View - A description of the hierarchy and elements of the VoIP 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:

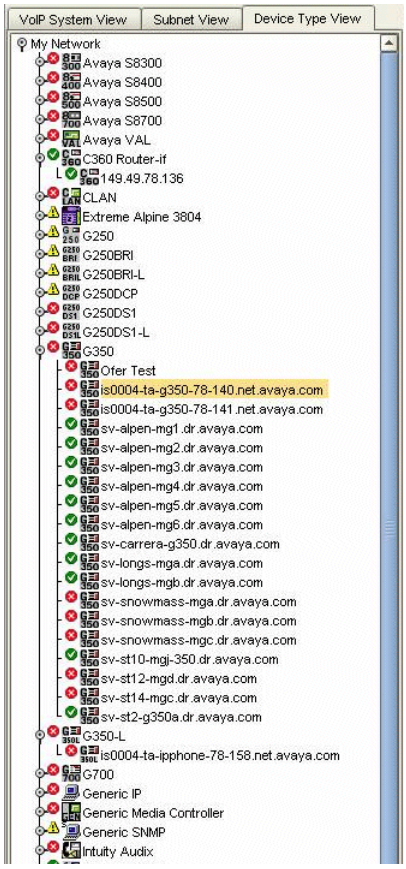
- **My Network** - Represents the entire network tree. When selected, all subnets appear in the Network Table.
- **Subnets** - Represents the subnets in the network. When selected, all devices with IP addresses in the selected subnet appear in the Network Table.
- **Devices** - Each device is labeled with the logical name or IP address of the device. When 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 the following levels:

- **My Network** - Represents the entire network tree. When selected, all supported device types in the network appear in the Network Table.
- **Device Types** - Represents all supported device types that appear in the network. When selected, all devices of the selected type appear in the Network Table.
- **Devices** - Represents the devices in the network. When selected, the device's interfaces appear in the Network Table.

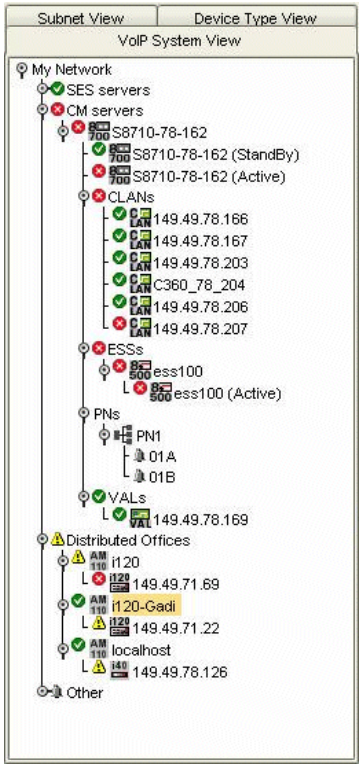
Figure 16: Device Type View



The VoIP System View

The VoIP System View tree shows a hierarchical view of the voice devices in the network. The VoIP System View tree is updated every time you run Discovery.

Figure 17: VoIP System View



The root of the VoIP System View tree is **My Network**. It represents all voice devices in the network. The root splits into several branches including **SES Servers** (SIP Enablement Services Servers), **CM Servers** (Communication Manager Media Servers), **Distributed Office** and **Other**.

The **SES Servers** branch splits based SIP Enablement Services Servers. Each discovered SES Server displays its own branch. Clicking on an SES Server branch displays all discovered SIP series IP phones associated with the SES Server.

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 duplex S8700 Communication Manager Media Servers (CM's), the tree displays the Virtual server. Under the virtual server, the active server is listed first, followed by the standby server. For simplex servers, including the S8500, S8400, S8300, and simplex S8700s, only the active server is listed.

At this level, the tree also displays the following devices:

- CLANs - Displays the CLANs related to the CM. For each CLAN, all related Media Gateways (MGs) are listed under the MG branch. When you click a CLAN, all IP phones associated with the CLAN are displayed in the Registered Endpoints Table.
- VAL boards - Displays the VAL Boards related to the CM.
- Port Networks (PNs) - Displays the PNs that are controlled by the CM. Carriers that are part of the selected PN are listed under that PN.
- Enterprise Survivability Servers (ESSs) - Displays the ESSs for the CM. If the ESS controls some of the PNs in the tree (because they lost connectivity with the CM), these PNs appear directly under the ESS, rather than under the CM.
- Local Survivable Processors (LSPs) - Display the LSPs for the CM.
- Voice Adjuncts - Displays Voice Adjuncts for the CM.
- Media Gateways (MGs) - Only appear for CMs, if the CM is running in processor ethernet mode. When you click an MG, all IP phones physically connected to the MG are displayed in the Port Connections Table.
- PNs - Displays the PNs that are controlled by the CM. Under each PN, the list of cabinets associated with the selected PN are displayed, showing the cabinet number and letter for each device.

The **Distributed Office** branch lists all the distributed office AM110 servers. Under each server, the gateway physically connected to the server (either i40 or i120) is displayed. If you click the AM110 server, all phones controlled by that server are displayed in the registered endpoints table. If you click the gateway listed under the AM110 server, a list of ports associated with the gateway are displayed in the Port Connections Table.

The **IP Office** branch displays all IP Office devices. It supports the following types of devices: IP406V2, IP412, Small Office 4T+4A+8DS, Small Office 2T+4A, and Small Office 4T+8A.

The **Other** branch splits into three. The **S8100** branch displays S8100 Devices in the network. The **Unaffiliated** branch displays a list of MGs, whose affiliation with a Communication Manager Media Server cannot be determined. If you click an MG, IP phones physically connected to the MG are displayed in the Port Connections Table. The **Remote Controller** branch displays all MGs for which the controller could be found, but the controller’s association with the CM could not be determined.

Note:

To refresh the Port Connections or Endpoints table for connections or endpoints attached to a specific device, right click on that device in the tree and select **Refresh Connections**.

Custom Views

Avaya Network Management Console enables 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

Note:

Copy, Cut, and Paste functions are allowed in Custom Views only.

Creating Custom Views

To create a custom view:

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

Figure 18: New View Dialog Box

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

   Note:

   View names cannot contain periods.

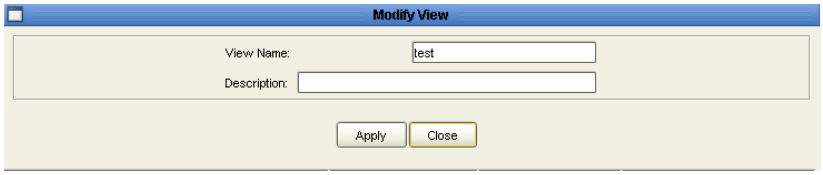
3. Enter a description of the view in the `Description` field.
4. Click **Apply**. The view is added to Avaya Network Management Console with the top level `My Network`. All devices in the network are added to a branch labeled `Unassigned`.

Modifying Custom Views

To modify a custom view:

1. Click the View Tab (refer to The VoIP System View on page 50) associated with the custom view you want to modify.
2. Select **Edit > Modify View**. The Modify View dialog box opens.

Figure 19: Modify 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 (refer to The VoIP System View on page 50) 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.

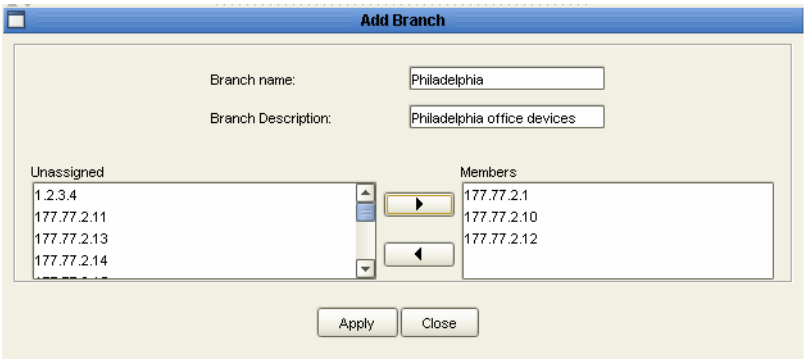
Adding Branches in Custom Views

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

Figure 20: 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:
   - Select the devices you want to add to the branch in the `Unassigned` list and click ▸. The devices appear in the `Members` list.
   - Select the devices you want to remove from the branch in the `Members` list and click ◂. The selected 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:

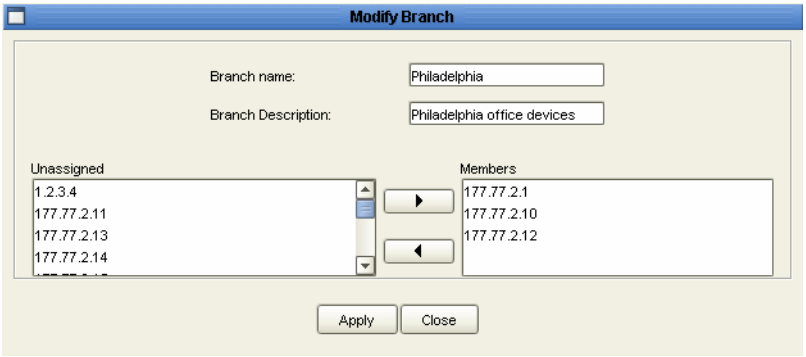
1. Select the branch you want to modify in the Network Tree.

   Note:

   An `Unassigned` branch cannot be modified.

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

Figure 21: 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 54.
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.

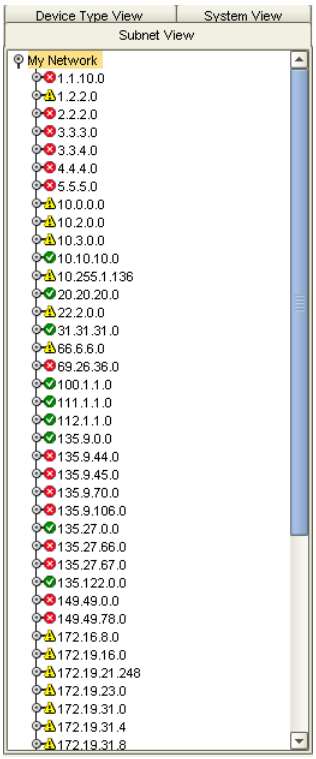
2. Select **Edit > Delete**. A confirmation dialog box opens.
3. Click **Yes**. The branch is deleted, and all its devices appear in the `Unassigned` list.

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 22: 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.

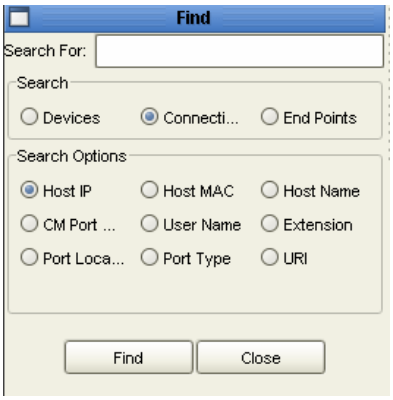
To search the Network Map:

1. Click  .

   Or

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

Figure 23: Find Dialog Box



2. Select a device.
3. Select a `Search` (Devices, Connections, or Endpoints).
4. Select one of the `Search Options`.
5. Enter the device's name (or part of it), IP address, or MAC address in the `Search For` field.
6. 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 **Close**.

Chapter 5: Launching Applications

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

- Launching Device Applications - Instructions for launching device-specific applications from Avaya Network Management Console.
- Launching Network-wide Applications - Instructions for 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 for launching the following device specific applications from Avaya Network Management Console:

- Device Manager
- IP Office Manager
- IP Office System Status
- Telnet
- Web Session
- PING
- Avaya Site Administration
- Avaya MultiSite Administration
- Avaya Fault and Performance Manager
- Avaya Voice Announcement Manager
- Extreme EPICenter
- Polycom GMS

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.

   Or

   Right-click the device and select **Device Manager** from the menu that appears.

   Note:

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

IP Office Manager

IP Office Manager is the device manager for the IP Office devices. It enables you to view and edit an IP Office device's configuration.

To launch the IP Office Manager:

1. Select the device you want to view in the Network Tree.
2. Double-click on the IP Office device. NMC will launch the IP Office Manager.\

   Note:

   IP Office Manager requires a login ID. Ensure the IP Office device has been assigned to an IP Office user in Security Access Administration (SAA) before launching IP Office Manager.

IP Office System Status

IP Office System Status enables you to log into the selected IP Office system automatically without re-entering your login and password.

To launch IP Office System Status:

Select **Tools > IP Office System Status**.

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.

   Or

   Right-click the device and select **Telnet** from the menu that appears.

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:

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

Or

Right-click the device and select **Web Session** from the menu that appears.

Or

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

PING

The PING application enables you to PING devices from within the 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.

   Or

   Right-click the device and select **Ping** from the menu that appears.

Avaya Site Administration

Avaya Site Administration (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 recognizes 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 > Voice Applications > 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 > Voice Applications > 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 > Voice Applications > 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 > Voice Applications > 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 > Voice Applications > 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 > Voice Applications > Avaya Fault and Performance Manager**. Avaya Fault and Performance Manager opens on the selected device.

Avaya Voice Announcement Manager

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

Note:

Avaya Voice Announcement Manager is part of Avaya Integrated Management.

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

To launch Avaya Voice Announcement Manager on an appropriate Voice Announcement board:

1. Select an appropriate Voice Announcement board.
2. Select **Tools > Voice Applications > Avaya Voice Announcement Manager**.

   Or

   Double-click an appropriate managed device. **Avaya Voice Announcement Manager** opens on the selected device.

Extreme EPICenter

Extreme EPICenter is a device management tool used to manage Extreme switches connected to your network. Currently supported switches are:

- Extreme Alpine 3802
- Extreme Alpine 3804
- Extreme Alpine 3808
- Extreme Black Diamond 6800
- Extreme Black Diamond 6804
- Extreme Black Diamond 6808
- Extreme Black Diamond 6816
- Extreme BlackDiamond 10808
- Extreme BlackDiamond 12802
- Extreme BlackDiamond 12804
- Extreme BlackDiamond 8806
- Extreme BlackDiamond 8810

- Extreme Summit 200 stack
- Extreme Summit 200-24
- Extreme Summit 200-48
- Extreme Summit 300-24 POE
- Extreme Summit 300-48
- Extreme Summit 400-24f
- Extreme Summit 400-24p
- Extreme Summit 400-24t
- Extreme Summit 400-48t
- Extreme Summit 450-24t
- Extreme Summit 450-24x
- Extreme Summit Stack
- Extreme Summit X250-24x
- Extreme Summit X250e-24p
- Extreme Summit X250e-24t
- Extreme Summit X250e-48p
- Extreme Summit X250e-48t
- Extreme Summit X450a-24tDC
- Extreme Summit X450a-24x
- Extreme Summit X450a-24xDC
- Extreme Summit X450a-48tDC
- Extreme Summit X450e-48p
- Extreme Summit1
- Extreme Summit1iSX
- Extreme Summit1iTX
- Extreme Summit2
- Extreme Summit24
- Extreme Summit24e2SX
- Extreme Summit24e2TX
- Extreme Summit24e3
- Extreme Summit3
- Extreme Summit4

- Extreme Summit48
- Extreme Summit48i
- Extreme Summit48si
- Extreme Summit4fx
- Extreme Summit5i
- Extreme Summit5iLX
- Extreme Summit5iTX
- Extreme Summit7iSX
- Extreme Summit7iTX
- Extreme SummitPx1
- Extreme SummitX450a-24t
- Extreme SummitX450a-48t
- Extreme SummitX450e-24p

To launch Extreme EPICenter on a supported Extreme switch:

1. Select a supported Extreme switch.
2. Select **Tools > Extreme EPICenter**.

   Or

   Double-click a supported Extreme switch. Extreme EPICenter opens for the selected switch.

   Note:

   When you launch Extreme EPICenter from Avaya Network Management Console, the Avaya Management Login dialog box opens. If you enter a username that matches a username configured on the Extreme device, you receive the administrative rights assigned to the username on the device. If you enter a username that does not match a username on the Extreme device, you receive the administrative rights assigned to the username in Avaya Network Management.

Polycom GMS

Network Management Console supports Polycom GMS for managing Polycom video conferencing gateways connected to your network. The following Polycom gateways are supported:

- VSX 3000
- VSX 7000
- VCU 25
- VCU 50
- VCU 100
- MGC 100
- MGC 100 Plus
- MGC 25
- MGC 25 Plus
- MGC 50
- MGC 50 Plus
- RMX 200

To launch Polycom GMS on a supported Polycom gateway:

1. Select a supported Polycom gateway.
2. Select **Tools > Polycom GMS**.

   The Server-based Polycom GMS application opens.

   Or

   Double-click a supported Polycom gateway. The embedded Web interface of Polycom GMS opens for the selected gateway.

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.

Applications include:

- Avaya Provisioning and Installation Manager for Gateways
- Avaya Provisioning and Installation Manager for IPO Devices
- Distributed Office Central Manager
- Avaya Software Update Manager
- Avaya Configuration Manager
- Avaya SMON Manager
- Avaya easy Management
- G860 EMS Client

Note:

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

Chapter 6: Avaya Network Management Console Tables

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

- The Network Table - A detailed description of the information in the Network Table.
- Viewing and Searching the Tables - A detailed description of the Avaya Network Management Console Table toolbars and instructions on how to filter and display the information they contain.
- Viewing and Searching the Tables - A detailed description of the information in the Alarms Table.
- The Modules Table - A detailed description of the information in the Modules Table.
- Managing Objects - Instructions on how to manage and unmanage objects in the Network Table.
- Manually Adding Devices - Instructions on how to add devices to the Network Table.
- 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 Table.
- The Port Connections Table - A detailed description of the information in the Connections Table.
- The Registered Endpoints Table - A detailed description of the information in the Registered Endpoints Table.

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 4: Network Table - Subnets

Field	Description
Interface Status	The status of the device with the highest severity level in the subnet.
Name	IP address of the subnet.
No. of Devices	The number of devices that have an interface in this 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: Network Table - Device Types

Field	Description
Interface Status	The status of the device with the highest severity level in the group of devices for the same device type.
Name	The device type.
No. of Devices	The number of devices from this type.

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

Table 6: Network Table - Devices

Field	Description
Interface Status	The status of the device.
Name	The Best Name of the device known to Avaya Network Management Console.
IP address	The IP address of the device.
Subnet Mask	The subnet mask of the device's IP address.
Phone Extension	The phone extension of the device.
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 7: Network Table - Interfaces

Field	Description
Interface Status	The status of the interface.
IP Address	The IP address 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

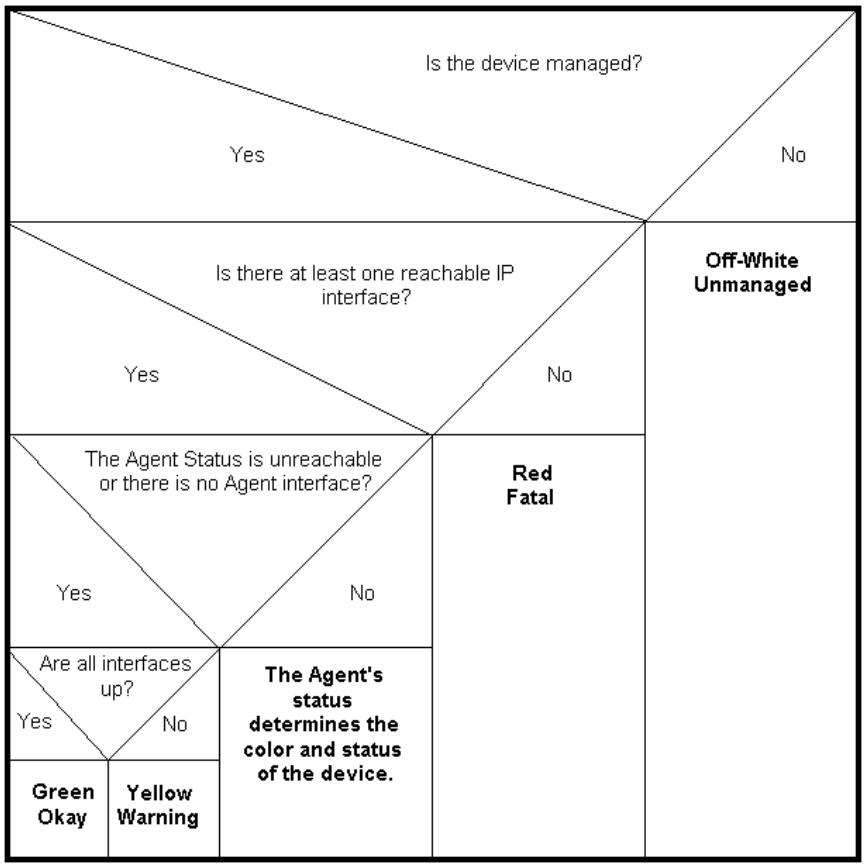
Devices and interfaces viewed in the Network Table are colored based on their status. The following table provides a list of colors and the statuses they represent.

Table 8: 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 24: Device Coloring Method



Viewing and Searching the Tables

The table toolbar and search functions are common to the Network table and Dialog area of the Avaya Network Management Console. This area includes the Alarms table, Modules table, Interfaces table, Registered Endpoints table, and the Port Connections table.

The table below describes the toolbar buttons for the Alarms, Modules and Interfaces tables and the Port Connections/Registered Endpoints Tables:

Table 9: Table Toolbar Buttons

Button	Description
	Saves the table to a .csv file.
	Opens the Select Columns list, which enables you to select the columns you want to view in the table.
	Scrolls back through the pages in the table, when there are multiple pages of data. There is a maximum of 1000 entries per page.
	Scrolls forward through the pages in the table, when there are multiple pages. There is a maximum of 1000 entries per page.
	Opens the filter function, which enables you to enter criteria for which to search in the table.
	Applies filter criteria specified in the filter row.

Choosing Table Parameters to Display

You can choose which parameters to display in a table.

To select the parameters you wish to view:

1. Click  . A list of available parameters appears.
2. Select the parameters that you wish to display in the Table. The display is updated automatically as soon as the column is selected.

Filtering the Tables

You can filter the information displayed in a table to display only the criteria you want to include.

To filter the information displayed in a Table:

1. Select the view in which you want to work or the information that you want to display in the relevant table.
2. Click 

. A new row appears in the Table, highlighted in blue.
3. In the new row, enter the filter criteria in the column you want to search. You can enter information in more than one field to narrow your search.
4. Click 

to apply changes.

The Alarms Table

The Alarms Table displays all alarms raised for the devices in the Network Tree. The Alarms Table enables you to see the status of IP Office devices and AM110 devices listed in the tree and any problems associated with them.The Network Management Console queries the network for alarm updates every 30 minutes and displays the results in the Alarms Table. A unique identifier and the severity level of the alarm are displayed for each alarm.

If a trap is received by the Avaya Network Management Server, the Network Management Console immediately queries the device that sent the trap. The Alarms Table is updated immediately, regardless of the time elapsed since the last query was performed.

To view the Alarms Table, click the Alarms Tab in the Network Table. Double-click on an alarm to open the Event Manager focused on the alarm definition. The alarm description can be customized in the event manager in the same way that a trap description can be edited. To customize the alarm description, refer to The Event Configuration User Interface.

You can filter the alarms table by category, severity level, or description. For more information on filtering the alarms table and the alarms table toolbar, refer to Viewing and Searching the Tables.

Alarms Table Parameters

The following table lists the fields that can be found in the Alarms Table:

Table 10: Alarms Table Parameters

Parameter	Description
Severity	An icon representing the severity of the alarm: ●  - Info ●  - Warning ●  - Minor ●  - Major ●  - Critical
Category	The category of the alarm.
Start Time	The time the alarm was reported.
Description	A description of the alarm.

The Modules Table

The Modules Table displays the modules associated with the gateways listed in the Network Tree. The Modules Tab is enabled for i120 and i40 devices only. For information on viewing the Modules table and the Modules table toolbar, refer to Viewing and Searching the Tables.

Modules Table Parameters

The following table lists the fields that can be found in the Modules Table:

Table 11: Modules Table Parameters

Parameter	Description
Module Index	Location of the module inside the box.
Module Type	Type of module.

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 object**. The selected object is unmanaged.

To manage an unmanaged object:

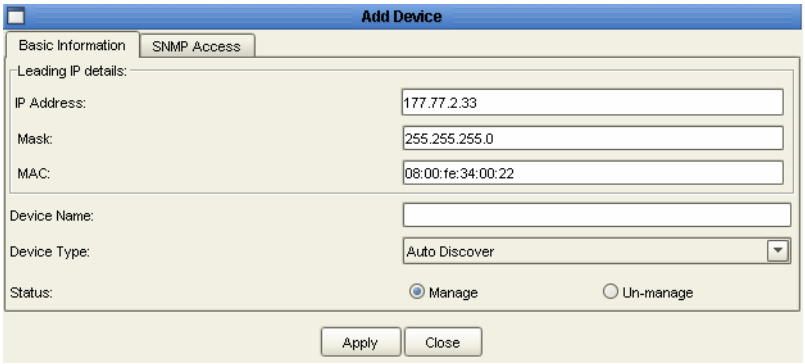
1. Select the object in the Network Table.
2. Select **Edit > Manage object**. The selected object is managed.

Manually Adding Devices

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

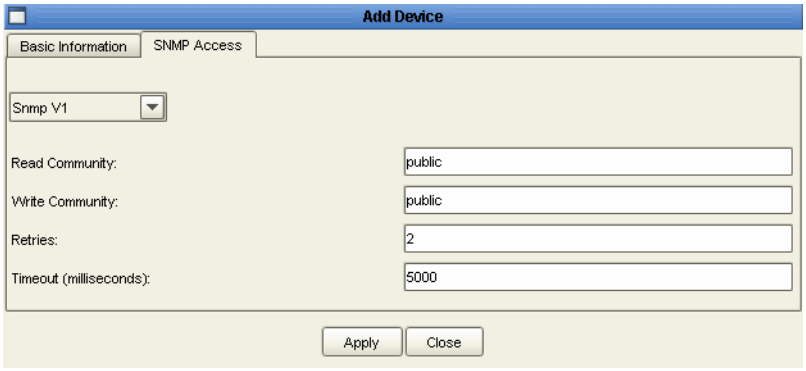
1. Select **File > New > Device**. The Add Device dialog box opens to the Basic Information tab.

Figure 25: Add Device Dialog Box - Basic Information Tab



2. Enter the device's parameters in the Add Device dialog box.
3. To edit the device's SNMP parameters, click the **SNMP Access** tab.

Figure 26: Add Device Dialog Box - SNMP Access Tab



4. Enter the SNMP parameters.
5. Click **Apply**. The device is added to the Network Map.

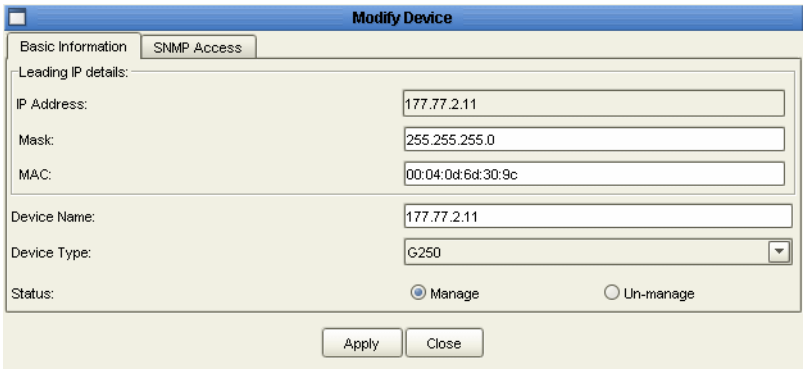
For information on the fields in the Add Device dialog box, refer to Device Parameters on page 80.

Modifying Devices

To modify basic information or SNMP parameters for a device in the current Network Map:

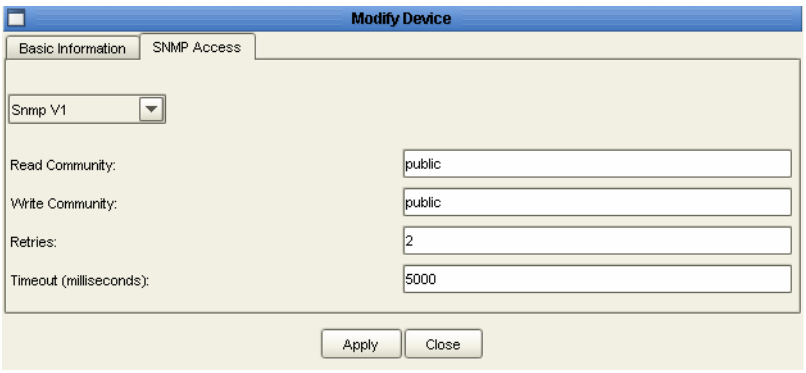
1. Select a device.
2. Select **Edit > Modify**. The Modify Device dialog box opens with the selected device's parameters.

Figure 27: Modify Device Dialog Box - Basic Information



3. Modify the parameters in the Add Device dialog box.
4. To edit the device's SNMP parameters, click the **SNMP Access** tab.

Figure 28: Modify Device Dialog Box - SNMP Access Tab



5. Modify 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 80.

Device Parameters

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

Table 12: Device Parameters

Parameter	Description
IP Address	IP address of the device.
Mask	The IP subnet mask.
MAC	The MAC address of the agent.
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 Avaya Secure Access Administration application. Only applicable for SNMP protocol V3.
	1 of 2

Table 12: Device Parameters (continued)

Parameter	Description
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.
	2 of 2

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 object**. A confirmation dialog box appears.
3. Click **Yes**. The selected device is deleted from the Network Map.

The Port Connections Table

The Port Connections Table provides information about ports on a selected device and the host devices connected to those ports. This information enables you to understand the details of network topology, and keep track of inventory for devices such as IP phones.

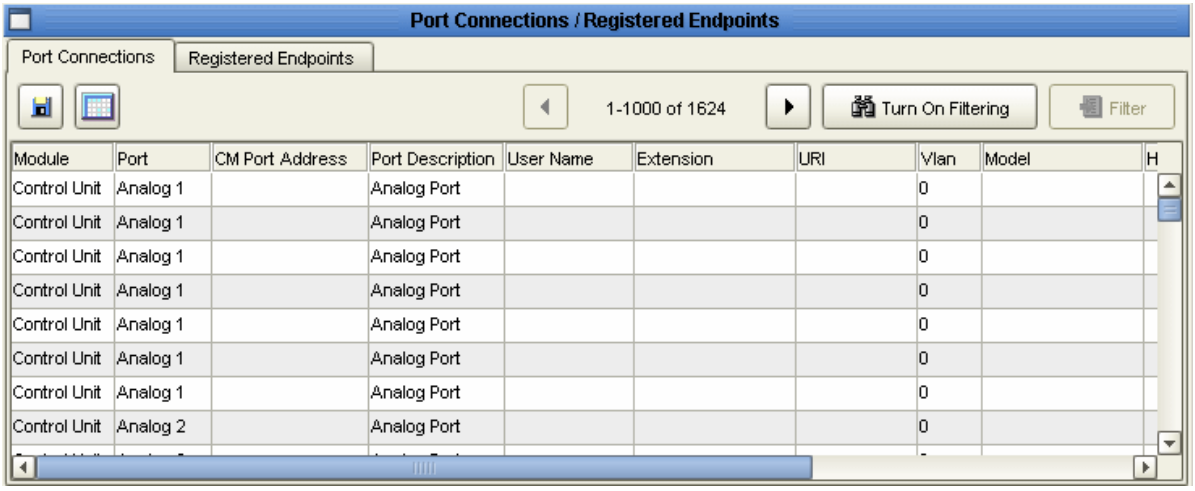
To open the Port Connections Table:

1. Open the Find dialog box (refer to Searching the Tree on page 57).
2. In the Search area, select **Connections**.
3. In the Search Options area, select the desired option to target a device.
4. Click **Find**. The Port Connections/Registered Endpoints dialog box appears and displays the Port Connections Table for the selected device.

   Note:

   You can also view the Port Connections table for a device by selecting that device and then clicking **View>Connections/Endpoints**.

Figure 29: Port Connections Table



You can choose the parameters displayed in the Port Connections table and filter the results of your search. For more information on viewing and filtering the Port Connections table and a description of the Port Connections toolbar, refer to Viewing and Searching the Tables.

Port Connections Table Parameters

The following are the fields in the Port Connections Table and their descriptions:

Table 13: Port Connections Table Parameters

Parameter	Description
Module	The module or slot number.
Port	The port name or number.
CM Port Address	The CM port address.
Port Description	The type of port.
User Name	The User Name for the selected phone.
Extension	The phone extension number. Available for connected phones only.
URI	The SIP URI. Available for connected phones only.
Vlan	The Vlan for devices supported by the port selected.
	1 of 2

Table 13: Port Connections Table Parameters (continued)

Parameter	Description
Model	The model of the phone connected to the selected device.
Host IP	The IP address of the connected host.
Host Name	The name of the connected IP host, if available. If the connection is a link to another switch, the name value is **Backbone**.
Host MAC	The MAC address of the connected host.
	2 of 2

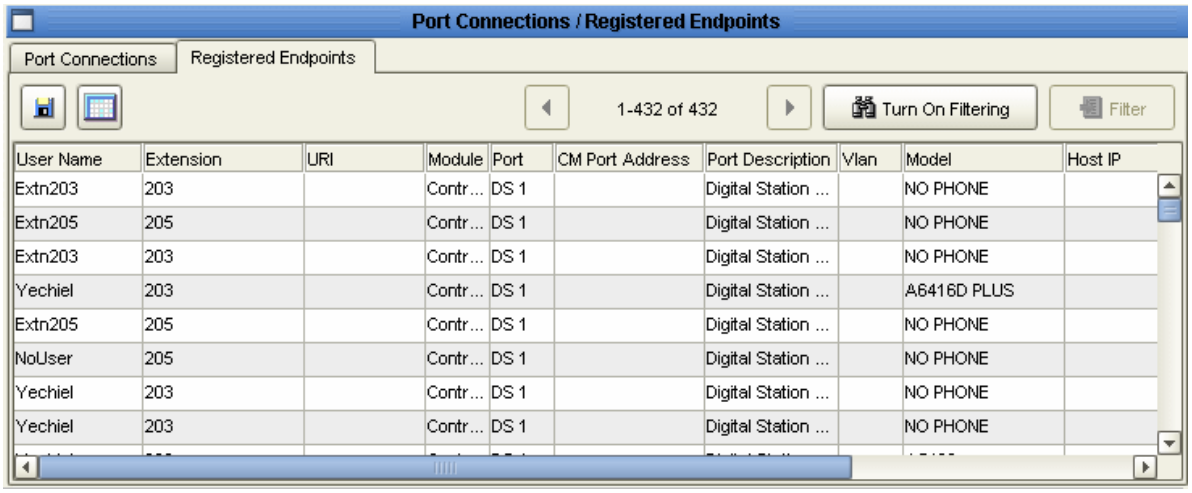
The Registered Endpoints Table

The Registered Endpoints Table displays details about the phones controlled by the selected node in the tree.

To open the Registered Endpoints Table:

1. Open the Find dialog box (refer to Searching the Tree on page 57).
2. In the Search area, select **Endpoints**.
3. In the Search Options area, select the desired option to target a device.
4. Click **Find**. The Port Connections/Registered Endpoints dialog box appears and displays the Registered Endpoints Table for the selected device.

Figure 30: Registered Endpoints Table



You can choose the parameters displayed in the Registered Endpoints table and filter the results of your search. For more information on viewing and filtering the Registered Endpoints table and a description of the Registered Endpoints toolbar, refer to Viewing and Searching the Tables.

Registered Endpoints Table Parameters

The following are the fields in the Registered Endpoints Table and their descriptions:

Table 14: Registered Endpoints Table Parameters

Parameter	Description
User Name	The User Name for the selected phone.
Extension	The phone extension number. Available for connected phones only.
URI	The SIP URI. Available for connected phones only.
Module	The module or slot number.
Port	The port name or number.
CM Port Address	The IP address of the CM port.
	1 of 2

Table 14: Registered Endpoints Table Parameters (continued)

Parameter	Description
Port Description	The description of the port as provided by the CM.
Vlan	The Vlan for devices supported by the port selected.
Model	The type of phone connected to the selected device.
Host IP	The IP address of the connected host.
Host Name	The name of the connected IP host, if available. If the connection is a link to another switch, the name value is **Backbone**.
Host MAC	The MAC address of the connected host.
	2 of 2

The Inventory Table

The Inventory Table provides information for all ports/endpoints and their associated devices over multiple devices on the network. The Inventory Filter enables you to search the Inventory Table and to refine the information displayed.

To open the Inventory Table:

- Select **View > Inventory.** The Inventory Table opens. Click the appropriate tab.

Figure 31: Inventory Table - Ports Tab

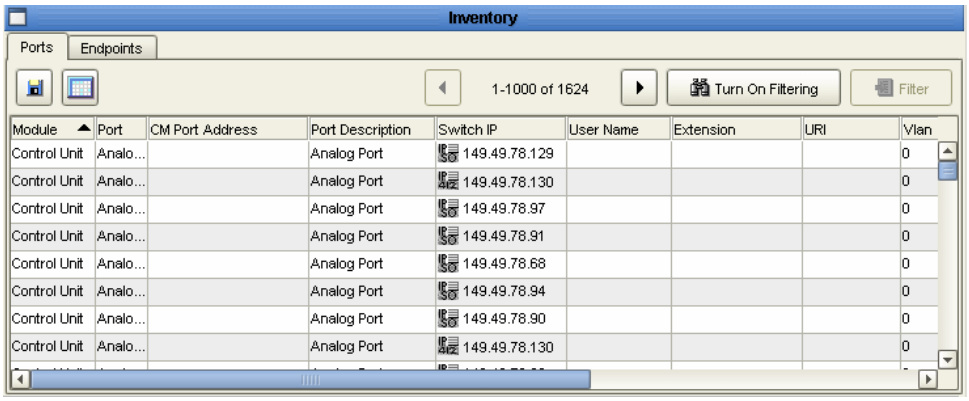
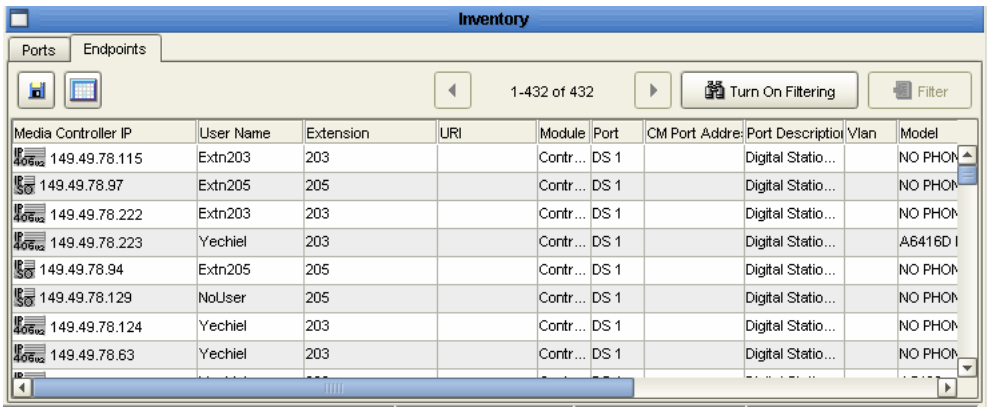


Figure 32: Inventory Table - Endpoints Tab



Inventory Table Toolbar

The table below describes the buttons on the Inventory Table:

Table 15: Inventory Table Toolbar Buttons

Button	Description
	Saves the Inventory Table to a .csv file.
	Opens the Select Columns list, which enables you to select which columns to view in the Inventory Table.
	Scrolls back through the Inventory pages when there are multiple page entries. There is a maximum of 1000 entries per page.
	Scrolls forward through the Inventory pages when there are multiple page entries. There is a maximum of 1000 entries per page.
	Opens the filter function, which enables you to enter criteria for which to search in the Inventory Table.
	Applies filter criteria specified in the filter row. This button only appears on the toolbar after the filter button has been selected.

Inventory Table Parameters

The following are the fields in the Ports tab of the Inventory Table and their descriptions:

Table 16: Ports Tab - Inventory Table Parameters

Parameter	Description
Module	Select a specific module on the device for which to view connections, or view connections for all modules on the device. This parameter is displayed by default.
Port	The port where the connection resides. This parameter is displayed by default.
CM Port Address	The IP address of the CM port.
Port Description	The description of the port as provided by the CM.
Switch IP	The IP address associated with the port. This parameter is displayed by default.
User Name	The User Name for the selected phone. This parameter is displayed by default.
Extension	The extension number, for connected IP phones only. This parameter is displayed by default.
URI	The SIP URI. Available for connected phones only.
Vlan	The Vlan for devices supported by the port selected.
Model	The model of the phone connected to the selected device. This parameter is displayed by default.
Host IP	The IP address of the connected host. This parameter is displayed by default.
Host Name	The name of the connected host, if available. If the connection is a link to another switch, the name value is **Backbone**.
Host MAC	The MAC address of the connected host.

The following are the fields in the Endpoints tab of the Inventory Table and their descriptions:

Table 17: Endpoints Tab - Inventory Table Parameters

Parameter	Description
Media Controller	The media controller for the selected endpoint.
User Name	The User Name for the selected phone. This parameter is displayed by default.
Extension	The extension number, for connected IP phones only. This parameter is displayed by default.
URI	The SIP URI. Available for connected phones only.
Module	Select a specific module on the device for which to view connections, or view connections for all modules on the device. This parameter is displayed by default.
Port	The port where the connection resides. This parameter is displayed by default.
CM Port Address	The IP address of the CM port.
Port Description	The description of the port as provided by the CM.
Vlan	The Vlan for devices supported by the port selected.
Model	The model of the phone connected to the selected device. This parameter is displayed by default.
Host IP	The IP address of the connected host. This parameter is displayed by default.
Host Name	The name of the connected host, if available. If the connection is a link to another switch, the name value is **Backbone**.
Host MAC	The MAC address of the connected host.

Inventory Table Filter

To filter the inventory table:

1. Click  . A new row appears in the Inventory Table, highlighted in blue.
2. In the new row, enter the filter criteria in the column you want to search. Search by substring only. You can enter more than one substring.
3. Click  to display search results.

Choosing Inventory Table Parameters to Display

You can choose which parameters to display in the Inventory Table.

To select the parameters you wish to view:

1. Click  . A list of available parameters appears.

Select the parameters that you wish to display in the Inventory Table. The display is updated automatically as soon as the column is selected.

Chapter 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 database enables you to store information about the devices found in a Network Map. You can create a number of Network Maps and save them in the database. 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 Postgres database.

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 95.

Managing Network Maps

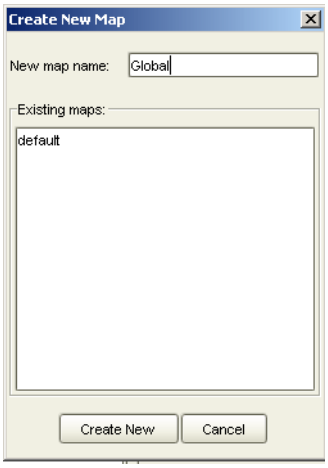
The following sections provide instructions for creating, opening, saving, and printing Network Maps.

Creating a Network Map

To create a new Network Map:

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

Figure 33: Create New Map Dialog Box



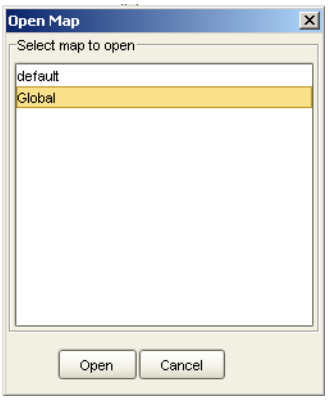
2. Enter a name for the file in the `New map name` field.
3. Click **OK**. A new Network Map is created.
4. Add subnets and devices to the Network Map using one of the following methods:
   - **Discovery** - For more information, refer to Discovering Subnets and Nodes on page 122.
   - **Manual Entry** - For more information, refer to Manually Adding Devices on page 78.
   - **Importing** - For more information, refer to Importing Devices into the Network Map on page 95.

Opening a Network Map

To open a Network Map:

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

Figure 34: Open Map Dialog Box



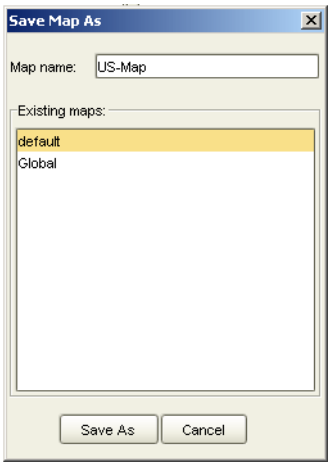
2. Select a Network Map from the list.
3. Click **Open**. The selected Network Map opens.

Saving a Network Map to a Different Name

To save a Network Map to a different name:

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

Figure 35: 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,D
ays2,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,Ve
nus,,,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,Laz
y23,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 96.

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

1. Select **File > Import map**. 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 a CSV file for use with external applications, such as Microsoft Excel. For information on the structure of CSV files of exported Network Maps, refer to CSV File Structure on page 96.

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 18: CSV 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 Secure Access Administration application. Only applicable for SNMP protocol V3.
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.

Chapter 8: Configuration Wizard

This chapter provides information and instructions for using the Configuration Wizard. It includes the following sections:

- Configuration Wizard Overview - An overview of the Configuration Wizard.
- Using the Configuration Wizard Screens - Detailed descriptions of the screens in the Configuration Wizard.

Configuration Wizard Overview

The Configuration Wizard appears at the end of the Network Management Console installation process. The Configuration Wizard enables you to configure the Communication Manager Media Servers (CM) and the Network Management Console to properly discover the network.

Using the Configuration Wizard Screens

This section provides detailed information on each of the screens within the Configuration Wizard. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Configuration Wizard without making any changes, close the wizard.

The Configuration Wizard consists of the following screens:

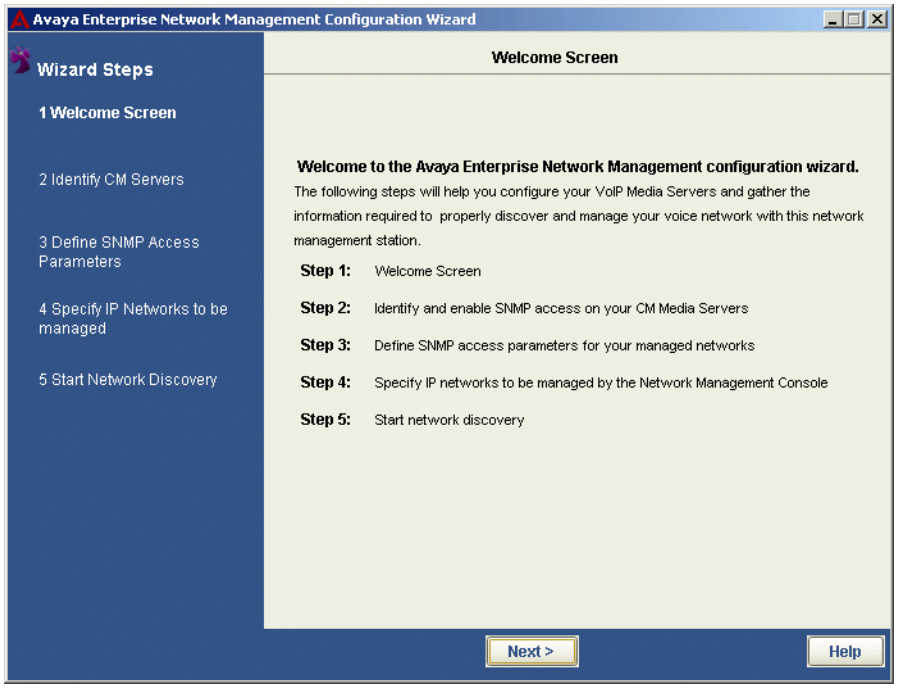
- Step 1 - Welcome Screen
- Step 2 - Identify CM Servers
  - Add/Edit CM Servers
  - Create or Add SNMPv3 User
  - Server Certificate Verification
  - Provide SNMPv3 Parameters
- Step 3 - Define SNMP Access Parameters
  - Configure User SNMP Parameters
- Step 4 - Specify IP Networks to be Managed
  - Configure Subnet Details
- Step 5 - Start Network Discovery

The following sections describe each of the Configuration Wizard screens.

Step 1 - Welcome Screen

The Configuration Wizard provides a simple, step-by-step method for configuring CM Servers and for properly discovering and managing your voice network with the Network Management Console. The steps of this method are described on the Welcome screen.

Figure 36: Step 1 - Welcome Screen

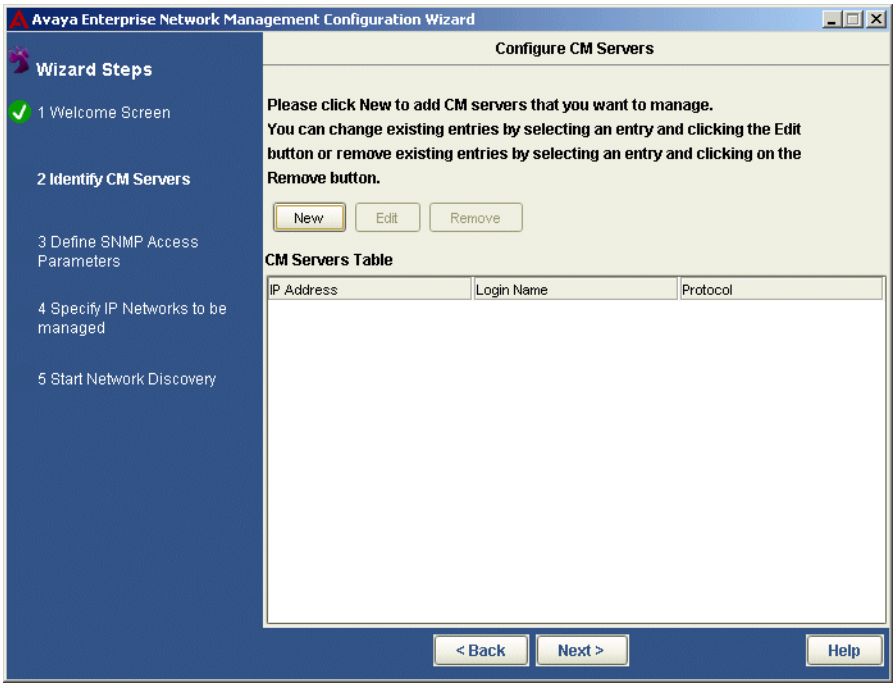


To continue, click **Next**. The Configuration Wizard continues with Step 2 - Identify CM Servers.

Step 2 - Identify CM Servers

The wizard enables you to add, edit, and remove CM Servers from the CM Servers Table. All configured CM Servers are listed in the CM Servers table.

Figure 37: Identify CM Servers Screen



To add a CM to the CM Servers Table:

- Click **New**. The Configuration Wizard continues with the Add/Edit CM Servers screen.

To edit the parameters for an existing CM Server:

1. Select the CM Server from the CM Servers Table.
2. Click **Edit**. The Configuration Wizard continues with the Add/Edit CM Servers screen.

To delete an existing CM Server:

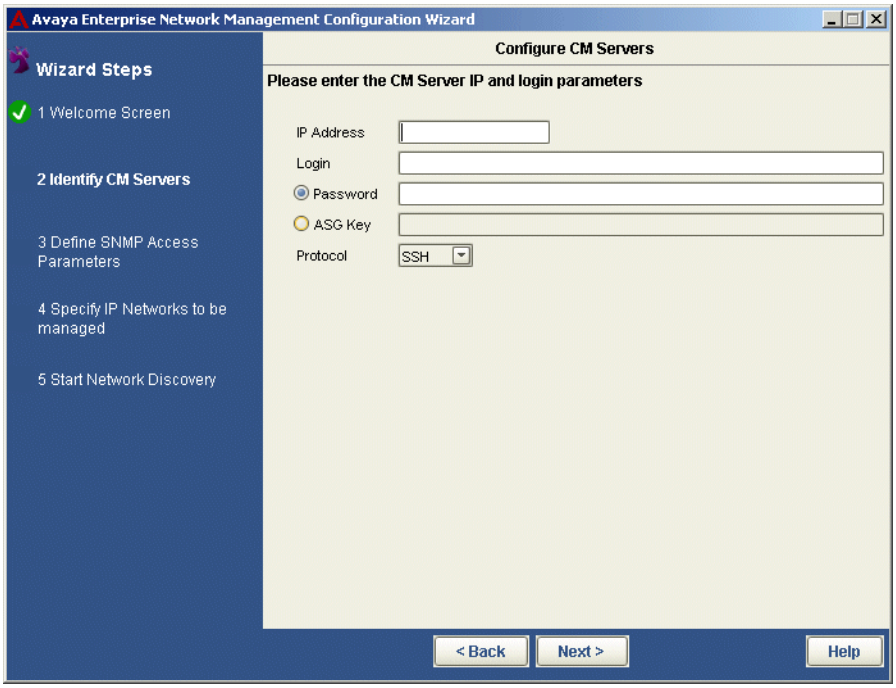
1. Select the CM Server from the CM Servers Table.
2. Click **Remove**. The selected CM Server is removed from the CM Servers Table.

To continue, click **Next**. The Configuration Wizard continues with Step 3 - Define SNMP Access Parameters.

Add/Edit CM Servers

The Configuration Wizard enables you to add parameters for a new CM Server or edit the parameters for an existing CM Server.

Figure 38: Add/Edit CM Servers Screen



To add/edit the parameters for a CM Server:

1. Enter the IP Address of the CM Server.
2. Enter the login name as configured on the CM Server.
3. Specify whether the CM Server uses a password or ASG Key for login, and enter the string.

   Note:

   The ASG key is a 20-character octal code, the 19th character of which must be either 0, 2, 4, or 6, and the 20th character of which must be 0.

4. Select the protocol for communication with the CM Server. The protocols available are: SSH and Telnet.

   Note:

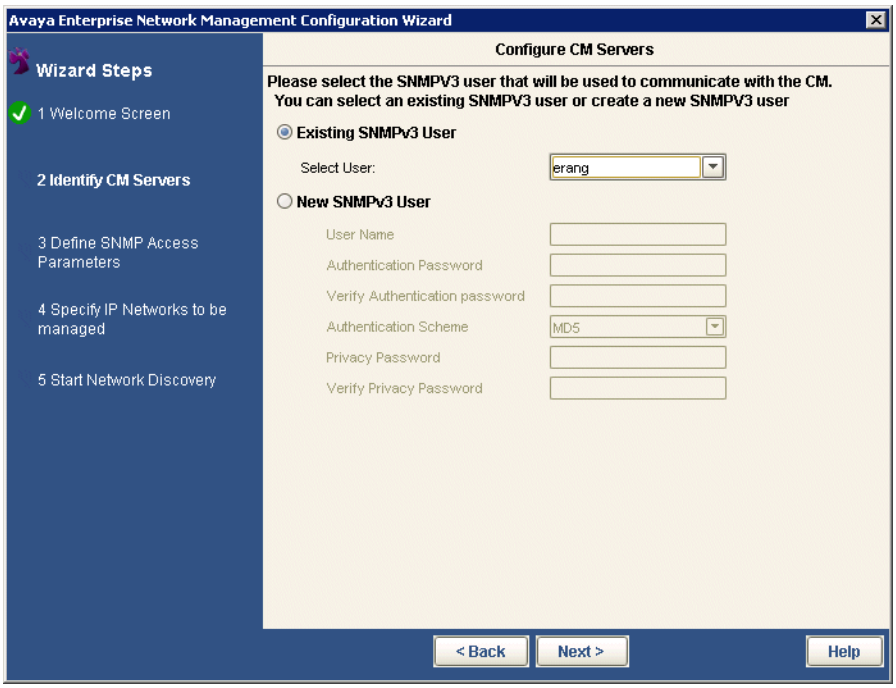
   Before accessing the CM server using passwords, the user must verify the CM server certificate. To ensure that this is the CM server you want to manage, verify that the public key is identical to the public key of the CM server certificate.

To continue, click **Next**. The Configuration Wizard continues with the Create or Add SNMPv3 User screen.

Create or Add SNMPv3 User

The Configuration Wizard enables you to select the SNMPv3 user that is used to communicate with the CM server. You can use an existing SNMPv3 user or create a new SNMPv3 user.

Figure 39: SNMpv3 User Screen



To use an existing SNMPv3 user:

1. Select the **Existing SNMPv3 User** option.
2. Select the user from the `Select User` drop-down list.

To create a new SNMPv3 user with which to communicate with the CM:

1. Select the **New SNMPv3 User** option.
2. Enter the user name for the new SNMPv3 user.
3. Enter the SNMPv3 authentication password, and enter it again to verify the password.

   Note:

   The authentication scheme supported by the CM is displayed. This field is read-only.

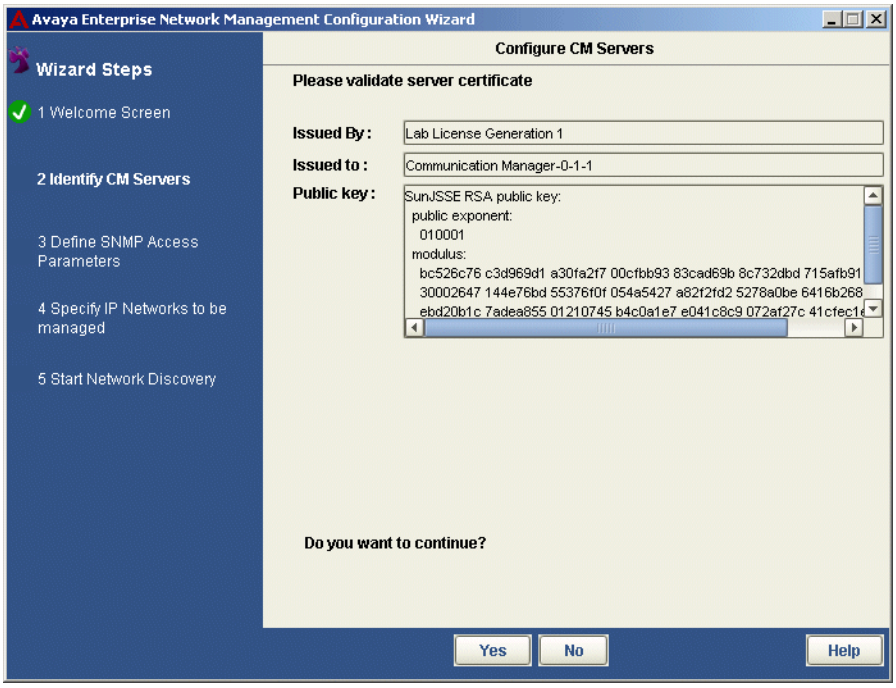
4. Enter the SNMPv3 privacy password and enter it again to verify it.

To continue, click **Next**. The Configuration Wizard continues with the Server Certificate Verification screen.

Server Certificate Verification

The Configuration Wizard enables you to verify the CM Server certificate.

Figure 40: Server Certificate Verification Screen



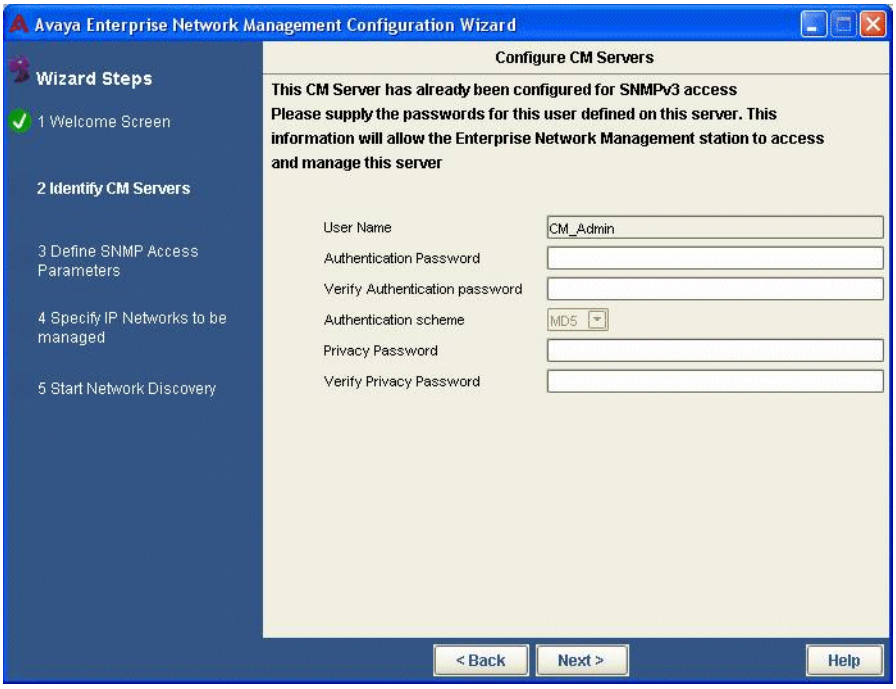
When you have finished reviewing the certificate, click **Yes**. The Configuration Wizard continues with Step 2 - Identify CM Servers.

Click **No** to return to the Add/Edit CM Servers screen and enter a different IP for the requested CM Server.

Provide SNMPv3 Parameters

The Configuration Wizard detects when a specified CM Server has a different SNMPv3 user name and password than those entered in the installation wizard. The Configuration Wizard informs you of this and provides you with the SNMPv3 user name configured on the specified CM Server. You can then enter the proper password to allow the Network Management Console to manage this server.

Figure 41: Provide SNMPv3 Parameters Screen



To enter the user parameters defined for a CM Server:

1. Enter and verify the SNMPv3 authentication password for the user name returned for this CM Server.

   Note:

   The authentication scheme supported by the CM is displayed. This field is read-only.

2. Enter and verify the SNMPv3 privacy password used to access this CM Server.
3. Click **Next**. The Configuration Wizard continues with the Server Certificate Verification screen.

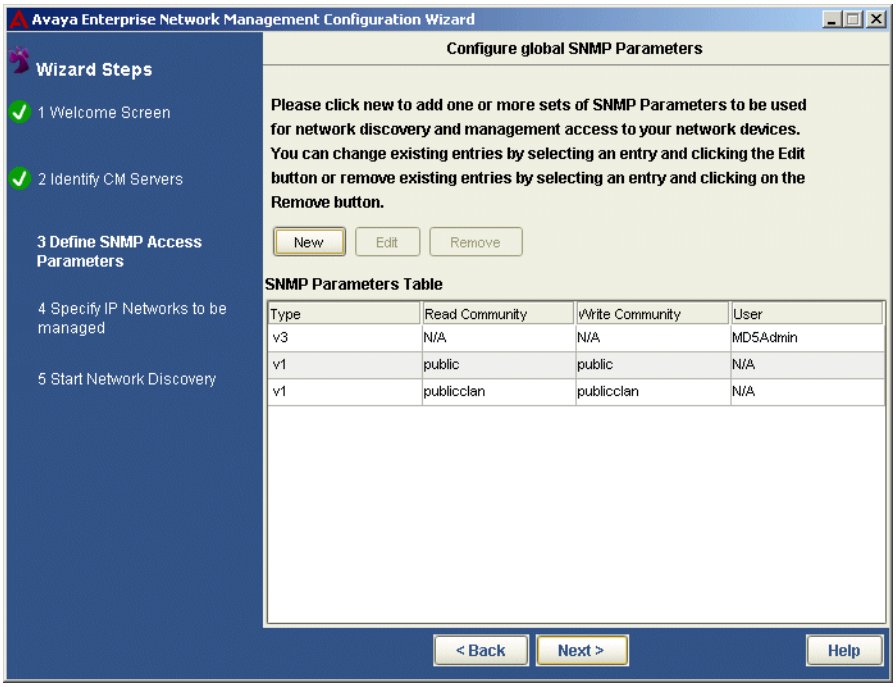
Step 3 - Define SNMP Access Parameters

The Configuration Wizard enables you to manage SNMP parameters used for network discovery and management access to the devices in your network.

Note:

These parameters can be modified later using the Options dialog box in the Network Management Console.

Figure 42: Define SNMP Access Parameters Screen



To add an SNMP parameters set to the SNMP Parameters Table:

- Click **New**. The Configuration Wizard continues with the Configure User SNMP Parameters screen.

To edit the parameters for an existing SNMP set:

1. Select the SNMP parameters set you want to edit from the SNMP Parameters Table.
2. Click **Edit**. The Configuration Wizard continues with the Configure User SNMP Parameters screen.

To remove an existing SNMP parameters set:

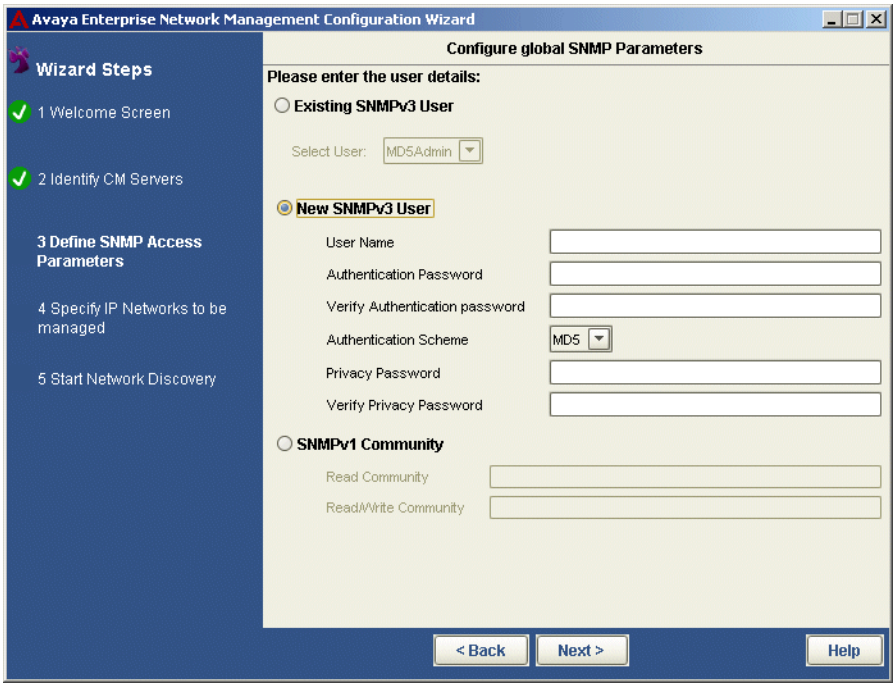
1. Select the SNMP parameters set from the SNMP Parameters Table.
2. Click **Remove**. The selected CM Server is removed from the CM Servers Table.

To continue, click **Next**. The Configuration Wizard continues with Step 4 - Specify IP Networks to be Managed.

Configure User SNMP Parameters

The Configuration Wizard enables you to manage SNMP user parameters used for accessing the new and existing devices in your network.

Figure 43: Configure User SNMP Parameters Screen



To edit the parameters for an existing SNMPv3 user:

1. Select the **Existing SNMPv3 User** option.
2. Select the user from the `Select User` drop-down list.

To add a new SNMPv3 user:

1. Select the **New SNMPv3 User** option.
2. Enter the user name for the new SNMPv3 user.
3. Enter the SNMPv3 authentication password for the new user and enter it again to verify the password.

   Note:

   The authentication scheme supported by the CM is displayed. This field is read-only.
4. Enter the SNMPv3 privacy password and enter it again to verify it.

To add an SNMPv1 community:

1. Enter the read community.
2. Enter the read/write community.

To continue, click **Next**. The Configuration Wizard returns to Step 3 - Define SNMP Access Parameters to enable you to manage other SNMP parameters.

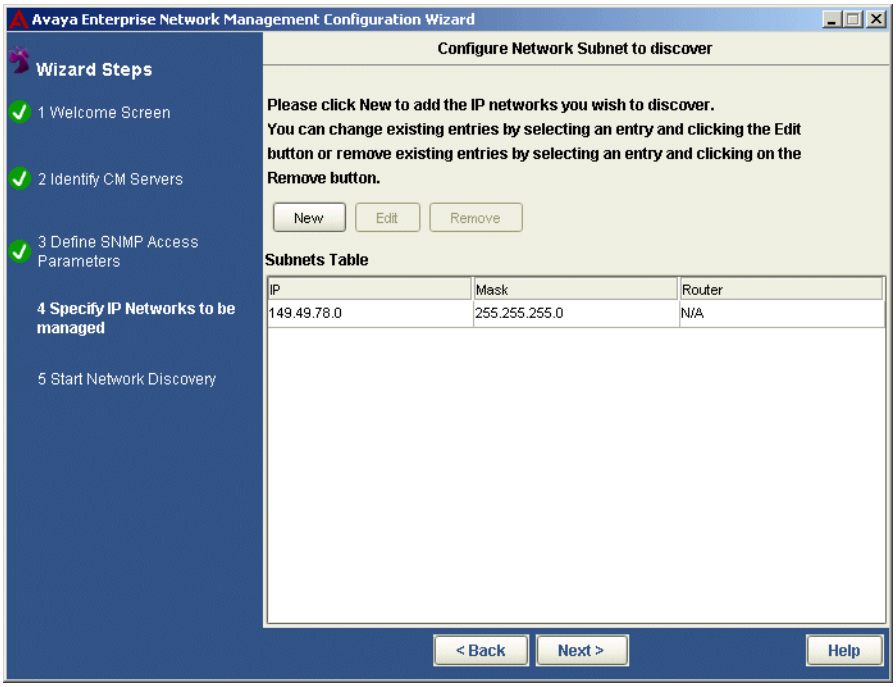
Step 4 - Specify IP Networks to be Managed

The Configuration Wizard enables you to manage the IP networks you want to discover and their parameters.

Note:

These parameters can be modified later using the IP Discovery dialog box in the Network Management Console.

Figure 44: Specify IP Networks to be Managed Screen



To add a network to the Subnets Table:

- Click **New**. The Configuration Wizard continues with the Configure Subnet Details screen.

To edit the parameters for an existing network:

1. Select the IP of the network from the Subnets Table.

2. Click **Edit**. The Configuration Wizard continues with the Configure Subnet Details screen.

To remove an existing network:

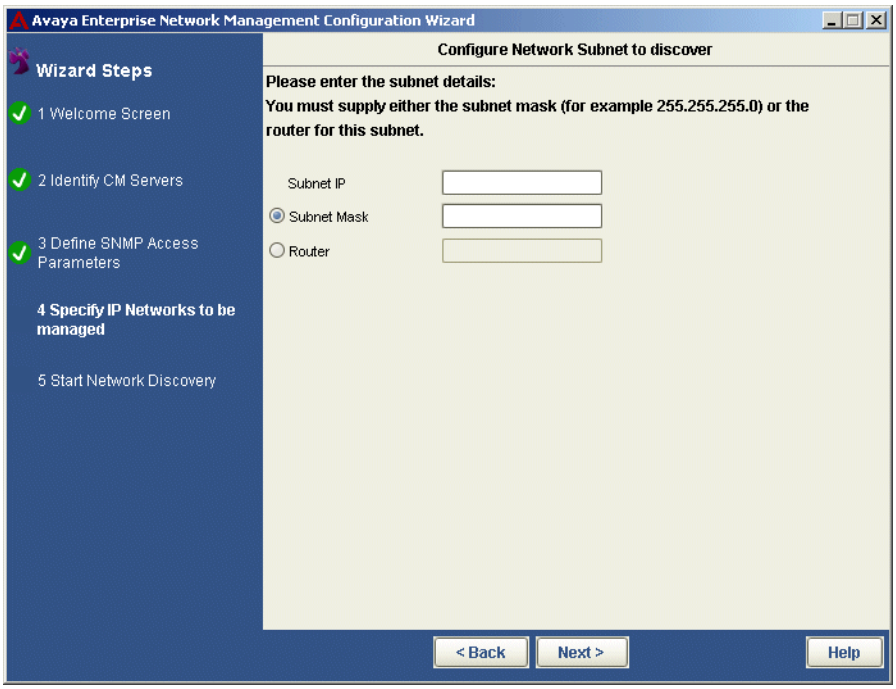
1. Select the IP of the network from the Subnets Table.
2. Click **Remove**. The selected IP of the network is removed from the Subnets Table.

To continue, click **Next**. The Configuration Wizard continues with Step 5 - Start Network Discovery.

Configure Subnet Details

The Configuration Wizard enables you to configure the subnet mask or router for the specified subnet.

Figure 45: Configure Subnet Details Screen



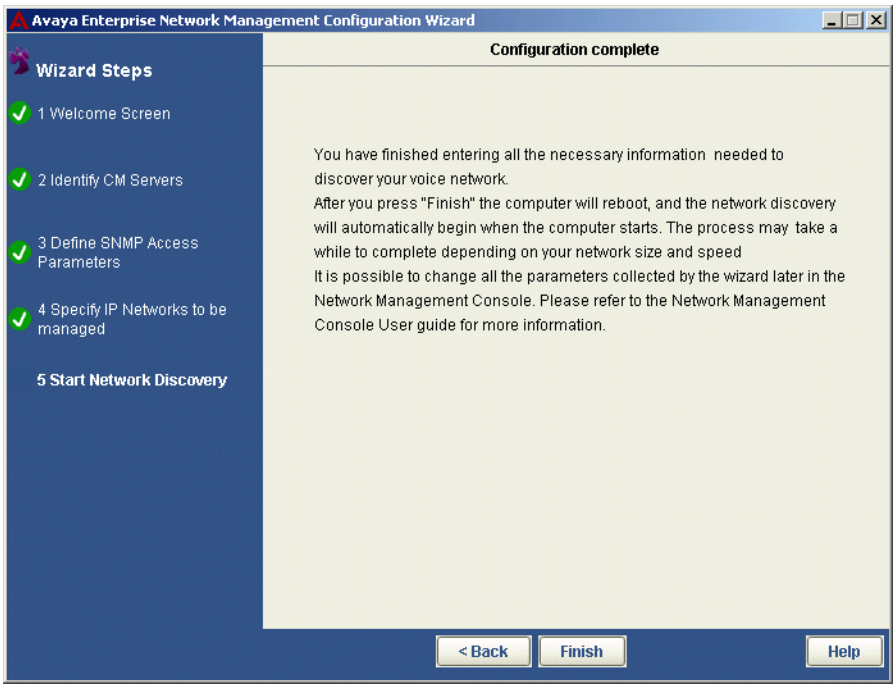
To add/edit the parameters for a subnet:

1. Enter an IP address for the new subnet. When editing a subnet, this field displays the IP address of the subnet you are editing.
2. Select whether you want to provide the subnet mask or router for this subnet, and enter the mask or router IP address.
3. Click **Next**. The Configuration Wizard returns to Step 4 - Specify IP Networks to be Managed to enable you to manage other subnets.

Step 5 - Start Network Discovery

The Configuration Wizard verifies that the configuration for running the Discovery process in your voice network is complete. You are then informed that the computer reboots after you click **Finish**, following which the Discovery process runs automatically.

Figure 46: Configuration Complete Screen



To make any changes to the configuration parameters:

1. Click **Back** until you reach the screen you want.
2. Change the relevant parameters.
3. Click **Next** until you reach the Configuration complete screen.

To end the configuration process, click **Finish**. The computer reboots and the configuration is incorporated in the Network Management Console.

Note:

All parameters may be modified later using the Network Management Console.

Chapter 9: 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

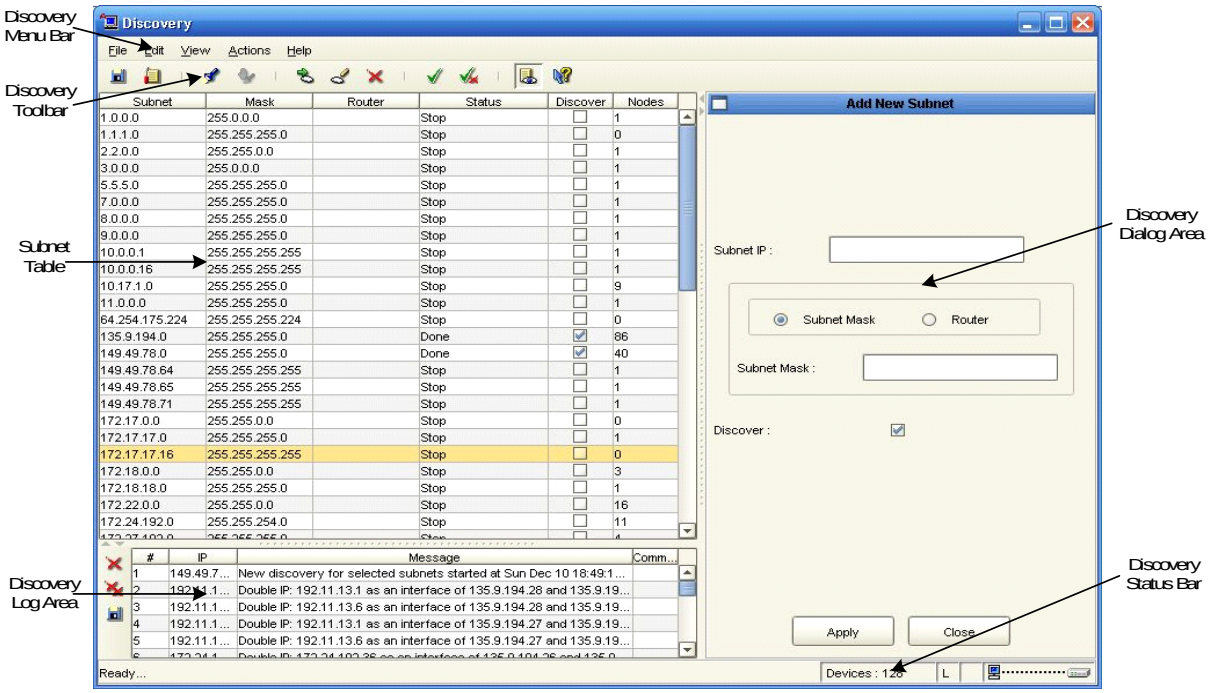
To open the Discovery window:

Click  .

Or

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

Figure 47: 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 19: 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**

1 of 2

Table 19: Discovery Toolbar (continued)

Button	Description	Menu Item
	Unchecks the `Discover` field for the selected subnet.	**Edit > Unselect**
	Opens the Discovery Log.	**View > Discovery Log**
	Opens context-sensitive help.	**Help > Help On**
		2 of 2

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 20: 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. • Selected: Discovery will search for nodes on this subnet. • Cleared: 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 128.
- **Changes Found** - If Discovery found subnets and/or nodes that are not in the current database, the letter ‘D’ appears in the Status Bar.

Closing the Discovery Window

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

Chapter 10: 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.
- Using the Discovery Scheduler - Instructions on how to schedule routine Network Discovery.
- 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.

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

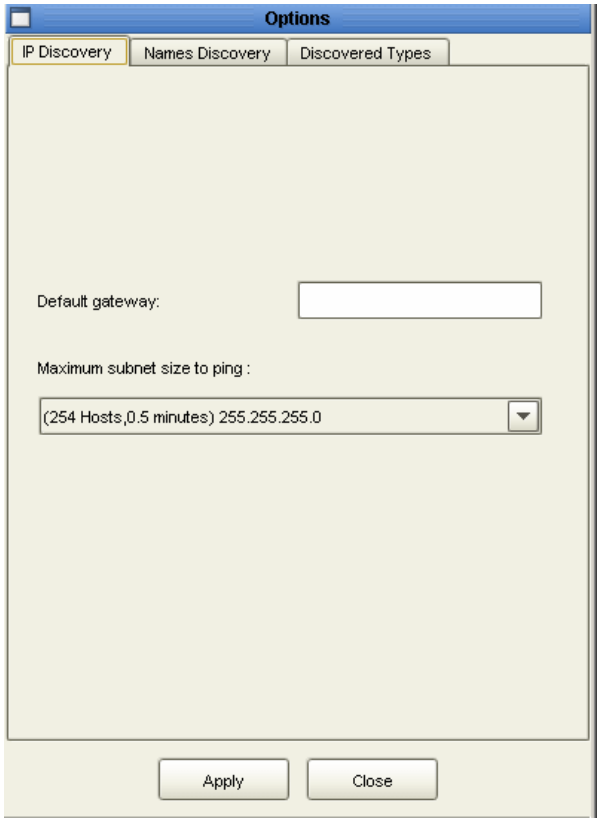
Select **File > Options** in the Discovery menu bar. The Discovery Options dialog box opens.

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 48: 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 21: IP Discovery Options

Field Name	Description
Default gateway	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 49: 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 22: Names Discovery Options

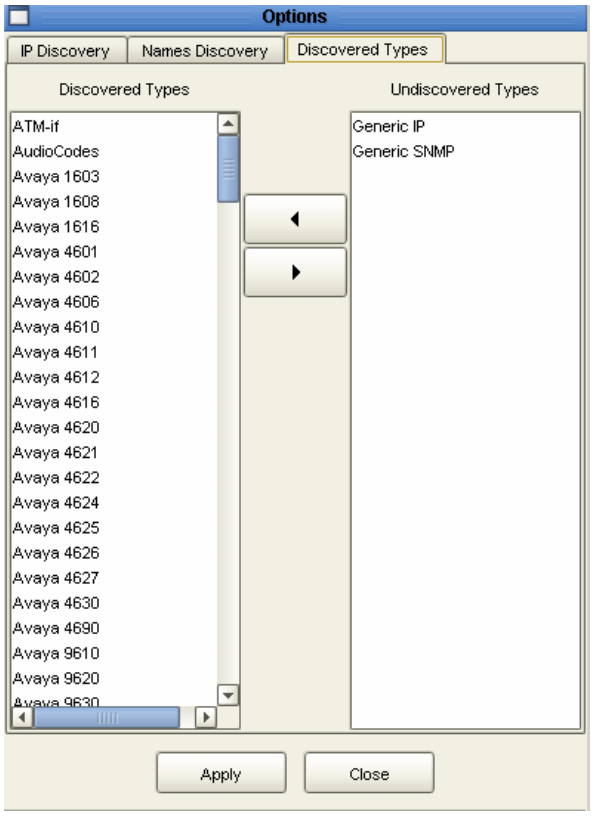
Field Name	Description
Update names for existing entries	This determines whether Discovery updates the names for nodes already listed in the Network Map. Possible states are: ● **Update** - Discovery updates the names of all discovered nodes. User defined names are replaced by the best name discovered. ● **Don't Update** - The names of existing entries in the Network Map are not replaced.
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 50: 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 lists. Only devices in the `Discovered Types` list will be found by Discovery. Devices listed in the `Undiscovered Types` list 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.

Note:

Avaya Network Management Console supports discovery of the following Avaya IP phones: Avaya 4601, Avaya 4610, Avaya 4690.

Note:

Avaya Network Management Console supports discovery of the following Extreme switches: Alpine 3804, Alpine 3808, Black Diamond 6804, Black Diamond 6808, Summit 200-24, Summit 200-48, Summit 300-24, Summit 300-48, Summit 400-48t.

Note:

Avaya Network Management Console supports discovery of Avaya SES servers.

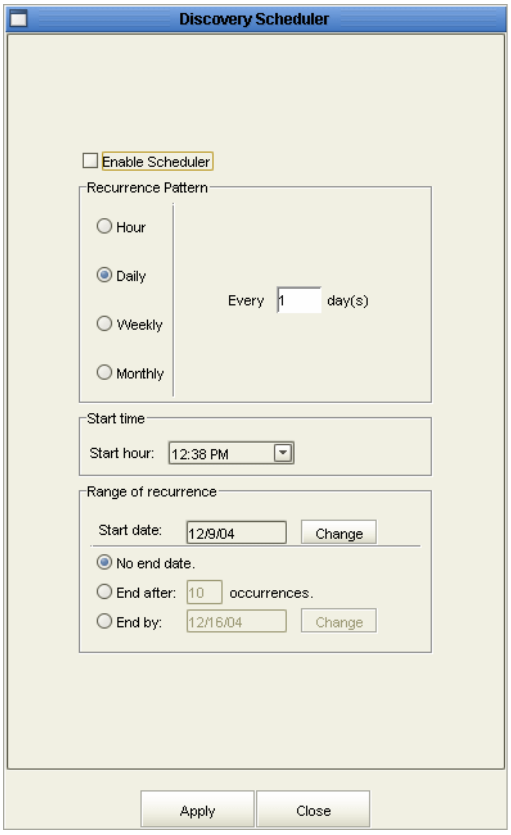
Using the Discovery Scheduler

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 51: Discovery Scheduler Dialog Box



2. Configure the Discovery Scheduler options.
3. Click **Apply**. Discovery Scheduler parameters are configured.

Note:

Certain operations of Network Management Console are disabled at different stages while Network Discovery is running.

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

Table 23: 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 113.

Problems during Discovery are reported in the Discovery Log. For more information, refer to Using the Discovery Log on page 128.

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:

Select **Actions > Start Network Discovery** in the Discovery menu bar. The Discovery process begins.

Or

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.

The progress of the discovery process is shown in the status bar of the user interface.

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 contains a list of the subnets discovered in your network.

To save changes you make in the Discovery Subnets Table:

Click  .

Or

Select **File > Save changes**.

Discovering Nodes on Specific Subnets

To select subnets upon which Discovery will search for nodes:

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

   Or

   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 selected.

   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 124.

To unselect subnets upon which Discovery will search for nodes:

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

   Or

   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 cleared.

To start Discovery on the subnets whose **Discover** checkbox is selected:

Click  in the Discovery toolbar.

Or

Select **Actions > Start Network Discovery** in the Discovery menu bar. The Discovery process begins searching for nodes on the subnets whose **Discover** checkbox is selected. The progress of the Discovery process is shown in the Status Bar of the user interface.

To stop the Discovery:

1. Click **Stop**. A confirmation dialog box opens.
2. 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 save changes you make in the Discovery Subnets Table:

Click  .

Or

Select **File > Save changes**.

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 New Subnet dialog box opens.

Figure 52: Add New Subnet Dialog Box

2. Enter the subnet parameters in the dialog box. For information on the fields in the Add New Subnet dialog box, refer to Subnet Parameters on page 127.
3. Click **Apply**. The subnet is added to the current Network Map.

To save changes you make in the Discovery Subnets Table:

Click .

Or

Select **File > Save changes**.

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.

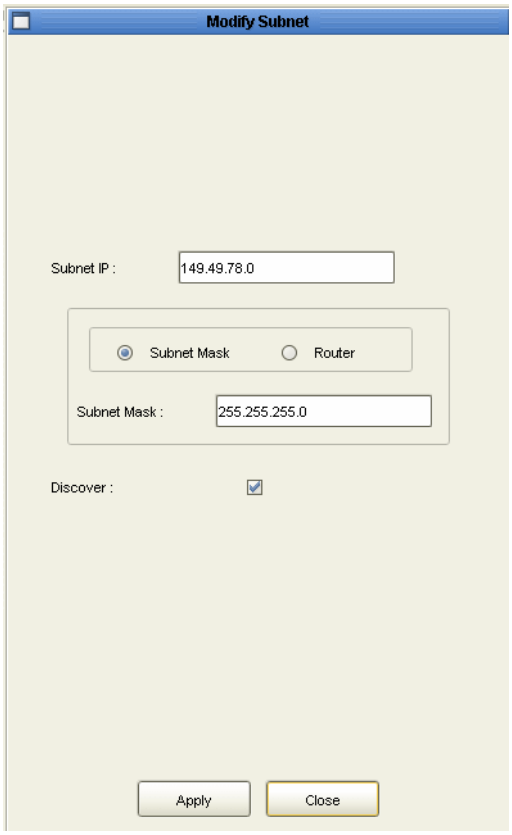
   Or

   Double-click the selected subnet.

   Or

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

Figure 53: Modify Subnet Dialog Box



3. Modify the parameters in the dialog box. For information on the fields in the Modify Subnet dialog box, refer to Subnet Parameters on page 127.
4. Click **Apply**. The subnet is modified in the current Network View.

To save changes you make in the Discovery Subnets Table:

Click  .

Or

Select **File > Save changes**.

Subnet Parameters

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

Table 24: Subnet Parameters

Parameter	Description
Subnet IP	IP address of the subnet.
Subnet Mask/ Router	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. • **Router** - The subnet's router is used for the subnet. You must enter the router's IP address in the `Router` field.
Subnet Mask	The IP of the subnet mask.
Router	The IP address of the subnet's router.
Discover	If selected, Discovery will 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 bolded in the Discovery Log.

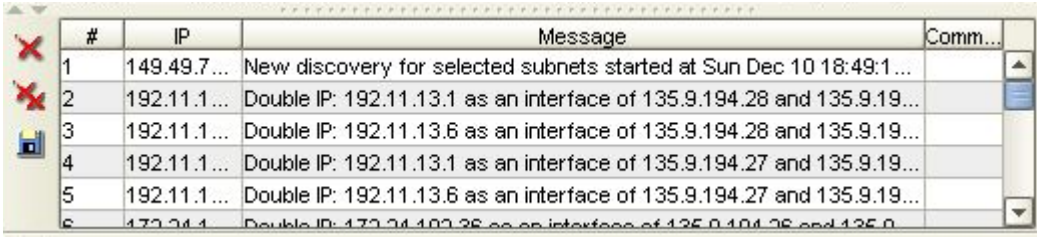
To view the Discovery Log:

Click  in the Discovery toolbar.

Or

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

Figure 54: Discovery Log



You can perform the following actions from the Discovery Log:

- 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 enables 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 55: 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 25: 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 Secure Access Administration application. Only applicable for SNMP protocol V3.
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 selecting 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.

Chapter 11: 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 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 the following windows:

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

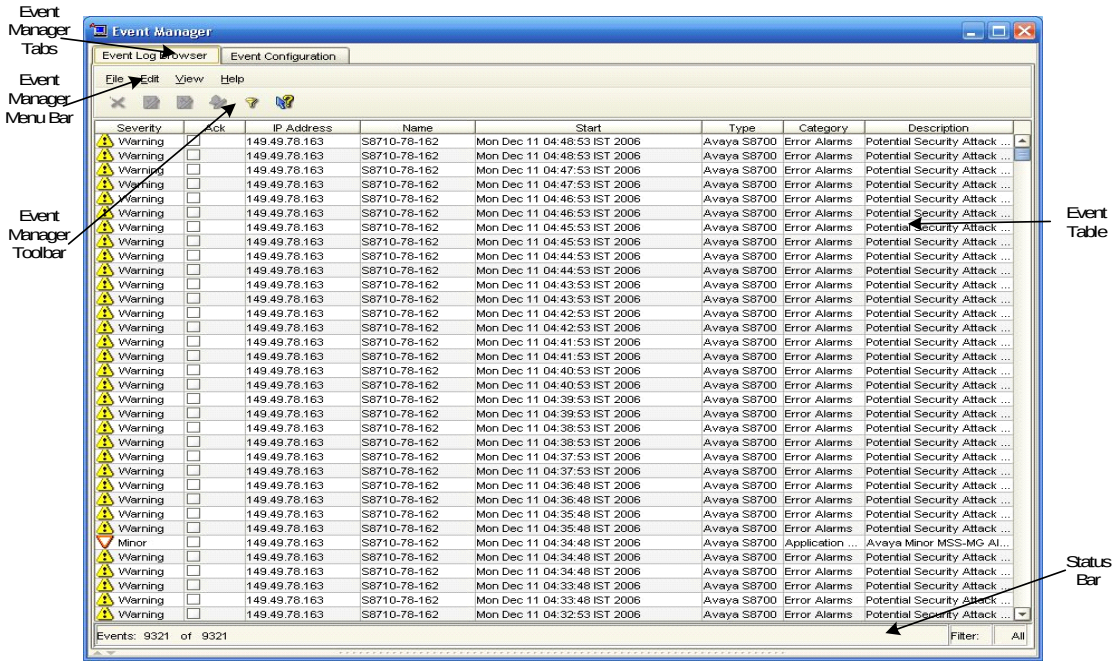
Use the Tabs at the top of the Event Manager to switch between the Event Log Browser and Event Configuration windows. The Action List window can only be viewed from the Event Configuration window.

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 56: 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 26: 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**

1 of 2

Table 26: Event Log Browser Toolbar (continued)

Button	Description	Menu Item
	Filters the information in the trap log by the criteria you select.	
	Opens context-sensitive help.	**Help > Help On**
		2 of 2

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. 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 140.

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 27: 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.
	1 of 2

Table 27: Trap Table Fields (continued)

Field	Description
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 140.
	2 of 2

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

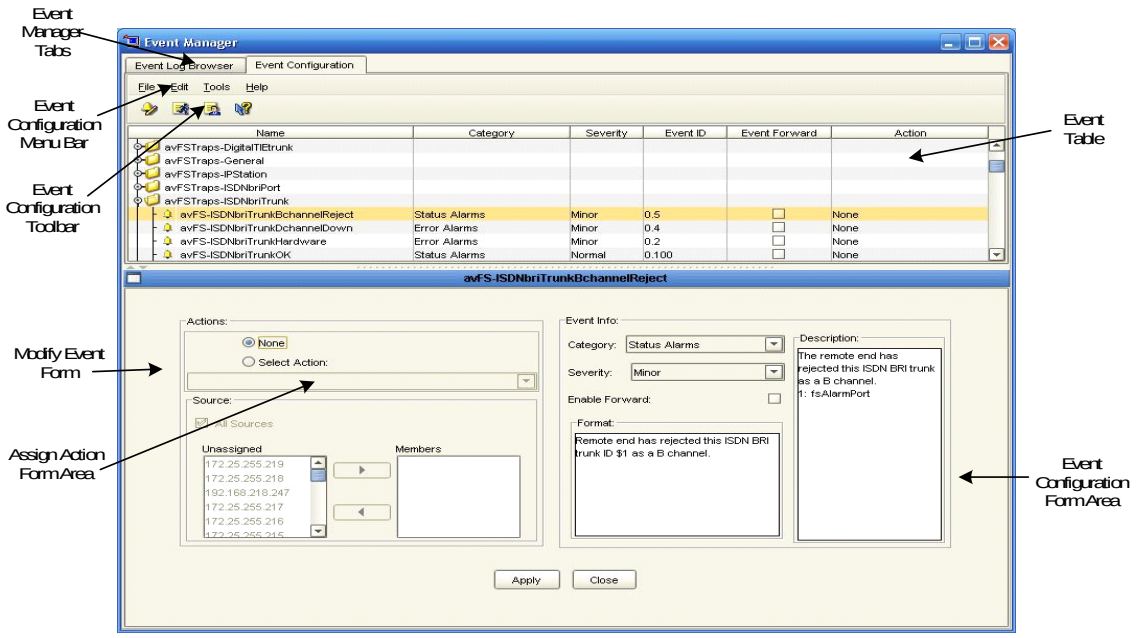
The Event Log Browser's Status Line displays the number of traps in the Event Log Browser. This number includes traps that are not currently displayed in the Trap Table. In addition, the Status Line displays the current filtering options.

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 57: 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 28: 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 29: Event Table Fields

Field	Description
Name	The name of the event or event category.
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.
	1 of 2

Table 29: Event Table Fields (continued)

Field	Description
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.
	2 of 2

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 30: 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 drop-down list is assigned to the selected event.
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** list 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 31: 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.
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).
	1 of 2

Table 31: Event Configuration Form Fields (continued)

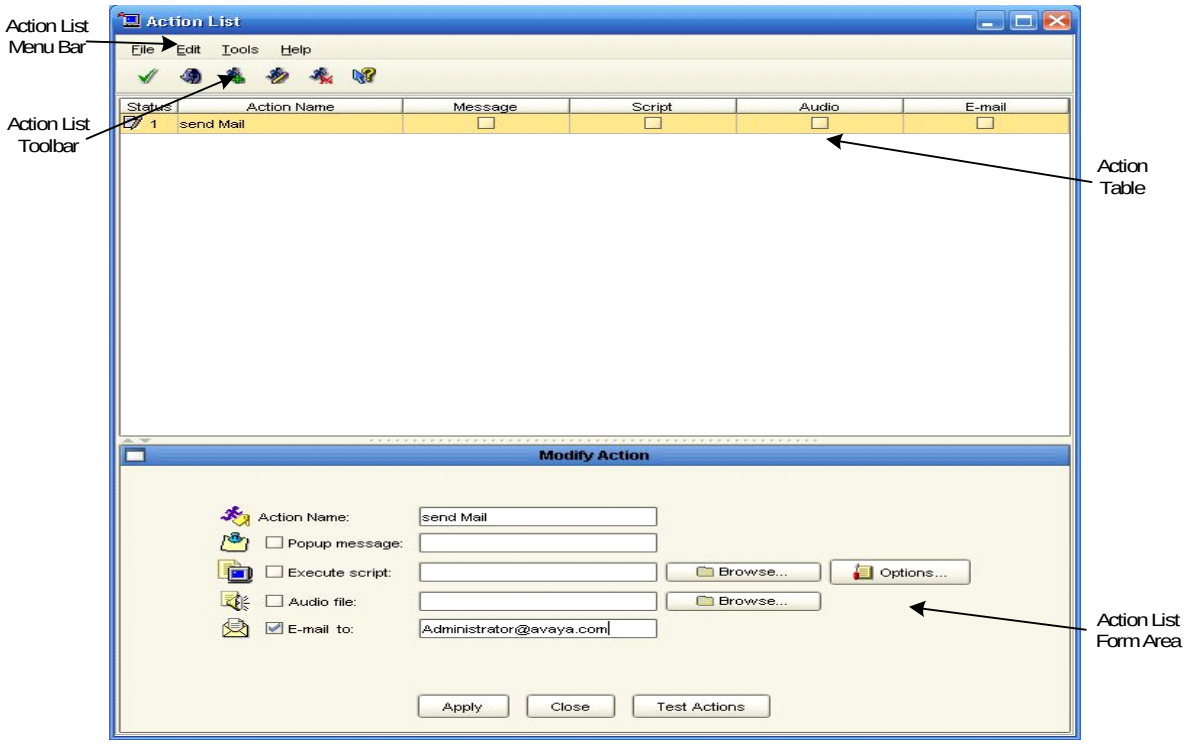
Field	Description
Description	A detailed description of the selected event. This information does not appear in the Event Log Browser.
	2 of 2

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 58: 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 32: 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 33: 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 45.
Action Name	The user defined name of the action.
Message	If selected, the action includes a pop-up message.
	1 of 2

Table 33: Action Table Fields (continued)

Field	Description
Script	If selected, the action includes running a script.
Audio	If selected, the action includes an audible message.
E-mail	If selected, the action includes sending an e-mail.
	2 of 2

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 155.

Closing the Event Manager

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

Chapter 12: Managing Events

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

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

Managing Events

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

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

For more information on the Event Manager user interface, refer to The Event Manager User Interface on page 134.

Event Log Options

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

Note:

By default, when the Event Log holds 10,000 events, the oldest 1,000 events are discarded.

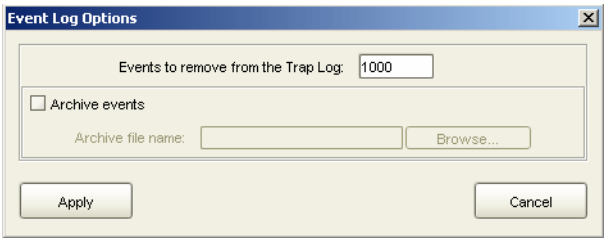
Note:

Archived events are appended to the event archive.

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

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

Figure 59: Event Log Options Dialog Box



2. Enter a number between 1 and 9999 in the `Events to remove from the event Log` field. This is the number of events to be deleted when there are 10,000 events in the Event Log.
3. If you want the deleted events saved to an archive, click the **Archive events** checkbox.
   - 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

   1. Click **Browse**. A file browser dialog box opens.
   2. Browse to the directory in which you want to save the archive.
   3. Enter a file name in the `File name` field.
   4. Select a file type from the `Files of type` drop-down list. Available file types are CSV (comma separated value) and XML.

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

   Note:

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

Filtering Events

By default, all events in the Event Log Browser are displayed in the Event Table. However, you can filter events by severity level, category, source, device type, or acknowledgment status. When you filter the Event Table, events 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 Category
- Filtering by IP Address
- Filtering by Device Type
- Filtering by Acknowledged
- Viewing All Events

Note:

You can only filter by one criterion at a time.

Filtering by Severity Level

To only view events of a given severity level:

1. Click  . The cursor changes to a hand.
2. Click on the `Severity` column of an event with the desired severity. Only events with the selected severity are displayed in the Event Table.

Or

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

Figure 60: Severity Filter Dialog Box

2. Click the checkboxes next to the severity levels of the events you want displayed in the Event Table.
3. Click **Apply**. Only events of the selected severity levels are displayed in the Event Table.

Filtering by Category

To only view events from a specific category:

1. Click  . The cursor changes to a hand.
2. Click the `Category` column of an event from the desired device. Only events from the selected category are displayed in the Event Table.

Or

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

Figure 61: Category Filter Dialog Box

2. Select the category of the devices from which you want to view events from the listbox.
3. Click **Apply**. Only events from the selected category are displayed in the Event Table.

Filtering by IP Address

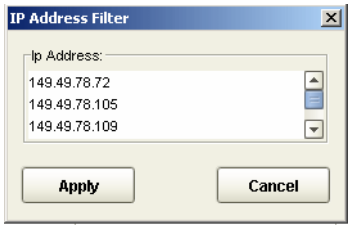
To view only events from a specific IP address:

1. Click . The cursor changes to a hand.
2. Click on the `From` column of an event from the desired device. Only events from the selected IP address are displayed in the Event Table.

Or

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

Figure 62: IP Address Filter Dialog Box



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

Filtering by Device Type

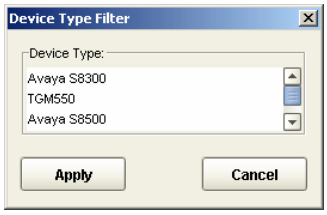
To only view events from a specific device type:

1. Click . The cursor changes to a hand.
2. Click the `Device Type` column of an event from the desired device type. Only events from devices of the selected device type are displayed in the event Table.

Or

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

Figure 63: Device Type Filter Dialog Box



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

Filtering by Acknowledged

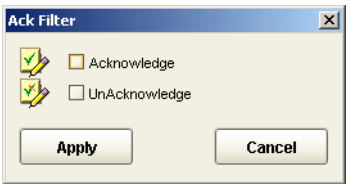
To filter events by the `Acknowledged` field:

1. Click  . The cursor changes to a hand.
2. Click the `Ack` column of an event with the desired Acknowledgement. Only events with the same value in the `Acknowledged` field are displayed in the Events Table.

Or

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

Figure 64: Acknowledged Filter Dialog Box



2. Click the checkboxes next to the Acknowledgement statuses of the events you want displayed in the Event Table.
3. Click **Apply**. Only events with the selected Acknowledgement statuses are displayed in the Event Table.

Viewing All Events

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

Acknowledging Events

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

To acknowledge an event:

1. Select an event.
   - To select multiple events, press **CTRL** while selecting additional events.
   - To select all events, select **Edit > Select All**.

2. Click  .

   Or

   Select **Edit > Acknowledge**.

   Or

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

To remove the acknowledge mark from a event:

1. Select an event.
   - To select multiple events, press **CTRL** while selecting additional events.
   - To select all events, select **Edit > Select All**.
2. Click  .

   Or

   Select **Edit > UnAcknowledge**.

   Or

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

Deleting Events

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

To delete an event:

1. Select an event.
   - To select multiple events, press **CTRL** while selecting additional events.
   - To select all events, select **Edit > Select All**.
2. Click  .

   Or

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

Editing Severity Levels

You can change the severity level of selected events. This is useful when a event 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 event's source being a monitored port, or any other cause.

To edit the severity level of a event:

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

   Or

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

Saving the Event Table

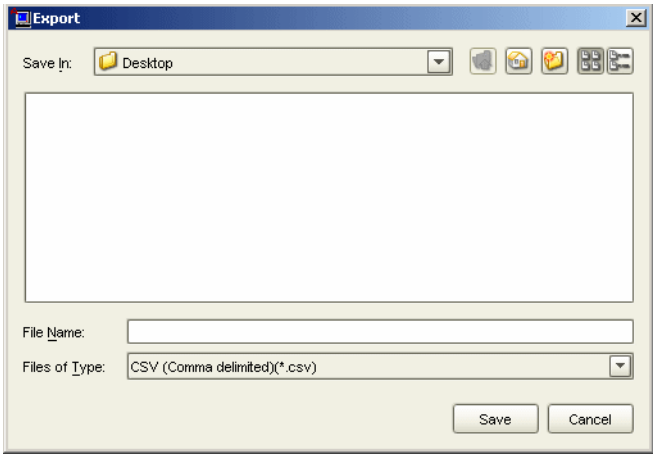
The Event Table can be saved to a file. The file can be in one of the following formats:

- **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 Event Table to a file:

1. Click **File > Export**. The Export dialog box opens.

Figure 65: 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` drop-down list.
5. Click **Save**. The event Table is saved to the specified file.

Defining Actions

This section provides instructions for defining actions and includes the following sections:

- Actions Overview - An overview of event 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 142.

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 events. For more information on assigning actions to events, refer to Configuring Events on page 159.

The Action Table includes a list of all configured actions.

Adding Actions

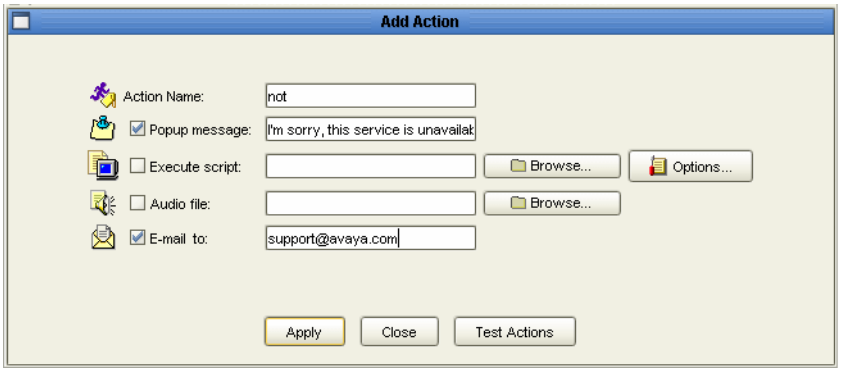
To add an action to the Action List:

1. Click  .

   Or

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

Figure 66: 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 155.
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

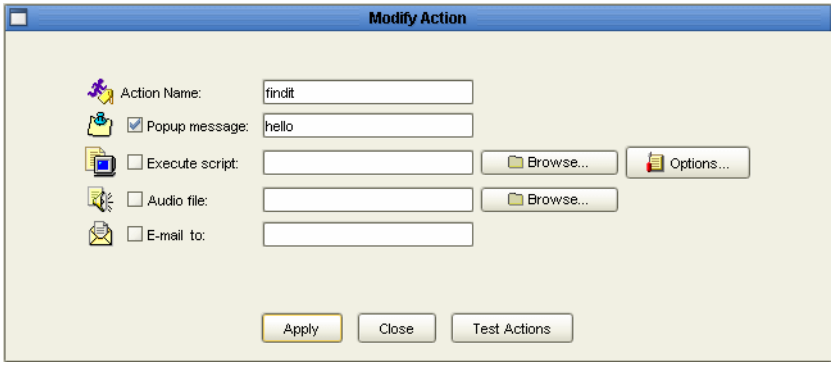
To modify an action in the Action List:

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

   Or

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

Figure 67: 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 155.
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 34: 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 the standard file browser to find the script file. For more information on scripts, refer to Action Scripts on page 156.

Table 34: Action Fields (continued)

Field	Description
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 the standard file browser to find the audio file. For more information on audio files, refer to Action Audio Files on page 157.
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. You can include more than one email address, each separated by a semicolon.

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 35: Command Line Parameters

Parameter	Variable	Description
IP Address	**$A**	The IP address of the device from which the event was sent.
SysOId + n	**$e**	The SysOId of the device followed by **.***n* for predefined events, or **0.***n* for vendor specific events, where *n* is the event 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

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

Figure 68: Script Parameters Dialog Box

2. Click 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 69: 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 events. 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 138.

Assigning Actions to Events

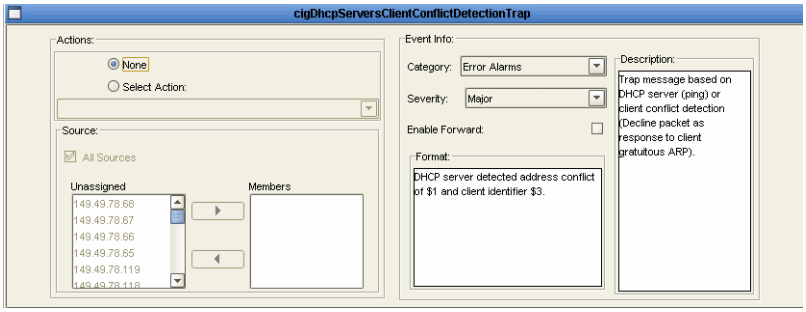
To assign an action to an event:

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 70: 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 drop-down list. For more information on defining actions, refer to Defining Actions on page 153.

6. Select source devices for the action. The Event Action is defined for only the devices in the `Members` drop-down list for all devices.

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

   - To add individual devices to the `Members` list, select a device in the `Unassigned` list and click  . The selected devices are moved to the `Members` list.
   - To remove individual devices from the `Members` list, select a device in the `Members` list and click  . The selected devices are moved to the `Unassigned` list.

   Note:

   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.

7. Select a category from the `Category` drop-down list.
8. Select a severity from the `Severity` drop-down list.
9. If you want to enable event forwarding for the event, click 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 event recipients on the device level. Instead, events from multiple devices can be forwarded to a single network device from which the events 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:

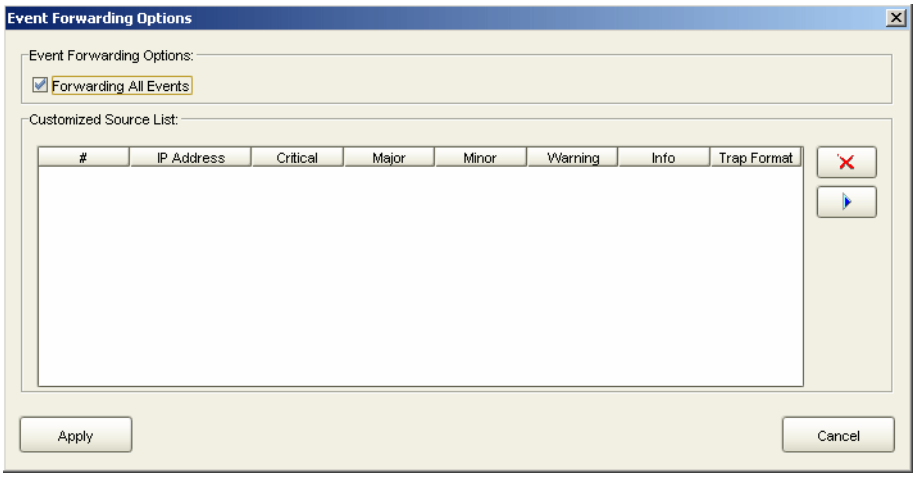
To open the Event Forwarding Options dialog box:

Click  .

Or

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

Figure 71: 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, click the **Forwarding All Events** checkbox.
   - To forward only specific events, clear 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 158.
2. Select the severity level of the alarm: **Critical**, **Major**, **Minor**, **Warning**, **Info**. You can select any number of levels.
3. Select the event Format: **SNMPv1 event**, **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 and port, separated by a colon, of a device to which you want to forward network events. The default port for SNMPv1 is 162, and for Syslog is 514.
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`.

Appendix 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 View 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 36: Avaya Network Management Console - File Menu

Item	Description
New	Creates a new Network Object - Map, View, Branch, or Device.
Open map	Opens a Network Object.
Save map	Saves a Network Object to a new name.
Import map	Imports device information from a CSV file into the current Network Map.
Export map	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.
Logout	Ends the current user's session.
Exit	Closes Avaya Network Management Console.

Avaya Network Management Console Edit Menu

Table 37: Avaya Network Management Console - Edit Menu

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

Table 37: Avaya Network Management Console - Edit Menu (continued)

Item	Description
Unmanage object	Unmanages a currently managed Network Object.
Find	Opens the Find dialog box.

Avaya Network Management Console View Menu

Table 38: Avaya Network Management Console - View Menu

Item	Description
Connections/Endpoints	Opens the Port Connections/Registered Endpoints log.
Inventory	Opens the Inventory log.
Tooltip	Toggles the display of device tooltips.

Avaya Network Management Console Actions Menu

Table 39: Avaya Network Management Console - Actions Menu

Item	Description
Avaya Secure Access Administration	Opens the Security Access Administrator (SAA).
Avaya User Administration	Opens Avaya User Administration.
Change Password	Opens the Change Password dialog box.
Event Manager	Opens the Event Log Browser.
IP Discovery	Opens the Discovery window.
Network Discovery Wizard	Opens the Network Discovery Wizard.
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 40: 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 MultiSite Administration -** Launches Avaya MultiSite Administration. • **Avaya Fault and Performance Manager -** Launches Avaya Fault and Performance Manager. • **Avaya Voice Announcement Manager -** Launches Avaya Voice Announcement Manager.
Avaya Software Update Manager	Launches Avaya Software Update Manager.
Avaya Provisioning and Installation Manager	Launches Avaya Provisioning and Installation Manager for Gateways.
Avaya Provisioning and Installation Manager for IPO Devices	Launches Avaya Provisioning and Installation Manager for IP Office Devices.
Avaya SMON Manager	Launches Avaya SMON Manager.
Avaya Device Manager	Launches the Device Manager for the selected device.
Avaya Network Configuration Manager	Launches Avaya Network Configuration Manager.
Polycom GPS	Launches Polycom GPS for the selected Polycom device.
Extreme EPICenter	Launches Extreme EPICenter for the selected Extreme device.
IP Office Manager	Launches IP Office Manager.
Avaya Distributed Office Central Manager	Launches Avaya Distributed Office Central Manager.
Avaya easy Management	Launches Avaya easy Management.

Table 40: Avaya Network Management Console - Tools Menu (continued)

Item	Description
IP Office System Status	Launches IP Office system status.
G860 EMS Client	Launches G860 EMS client.
Web	Launches a Web session to the selected Avaya P330 or Avaya P580/P882 Device.
Telnet	Launches a Telnet session to the selected device.
Ping	PINGs the selected device.

Avaya Network Management Console Help Menu

Table 41: 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 42: Discovery - File Menu

Item	Description
Save changes	Saves the updated Network Map with the results of the latest Discovery to the database.
Options	Opens the Discovery options dialog box.
Exit	Closes the Discovery window.

Discovery Edit Menu

Table 43: Discovery - Edit Menu

Item	Description
Add	Opens the Add Subnet dialog box.
Modify	Opens the Modify Subnet dialog box.
Select	Selects the `Discover` field for the selected subnets.
Unselect	Clears 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 44: Discovery - View Menu

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

Discovery Actions Menu

Table 45: Discovery - Actions Menu

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

Discovery Help Menu

Table 46: Discovery - Help Menu

Item	Description
Contents	Opens the on-line help to the first topic.
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 47: 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 48: Event Log Browser - Edit Menu

Item	Description
Delete	Deletes the selected traps.
Acknowledge	Acknowledges the selected traps.
UnAcknowledge	Unacknowledges the selected traps.
Modify Event	Opens the Modify Event dialog box.
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.

Table 48: Event Log Browser - Edit Menu (continued)

Item	Description
Change Severity > Change severity to Warning	Changes the severity of the selected traps to Warning.
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.

Event Log Browser View Menu

Table 49: Event Log Browser - View Menu

Item	Description
Filter > Severity Filter	Opens the Severity Filter dialog box.
Filter > Category Filter	Opens the Category 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.
Filter > New Traps on top	Displays the newest traps at the top of the list in the Event Log Browser table.

Event Log Browser Help Menu

Table 50: 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 51: Event Configuration - File Menu

Item	Description
Exit	Closes the Event Log.

Event Configuration Edit Menu

Table 52: Event Configuration - Edit Menu

Item	Description
Modify Event	Opens the Modify Event dialog box.

Event Configuration Tools Menu

Table 53: 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 54: 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 55: Action List - File Menu

Item	Description
Exit	Closes the Action List.

Action List Edit Menu

Table 56: 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 57: Action List - Tools Menu

Item	Description
Options	Opens the Action List Options dialog box.

Action List Help Menu

Table 58: Action List - Help Menu

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

Index

A

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W