Maintenance and Troubleshooting for Avaya Aura™ Communication Manager Branch

03-602029
Issue 4
November 2009

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 support information, please see the following complete documents: *Avaya Support Notices for Hardware Documentation*, document number 03-600759, and *Avaya Support Notices for Software Documentation*, document number 03-600758.

To locate the document on our Web site, 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

Chapter 1: Introduction

Maintenance and Troubleshooting for Avaya Aura™ Communication Manager Branch contains the maintenance and troubleshooting functions that Communication Manager Branch customers consider to be the most important and are performed most frequently. Along with maintaining and troubleshooting, this book also provides procedures for testing and replacing system components.

This book is not intended to solve all the Communication Manager Branch problems. If the limits of the procedures found in this book have been reached and the problem has not been resolved, the problem should be escalated to a higher level of technical support.

This book provides troubleshooting and maintenance information for the Branch Central Manager and the Avaya Branch Device Manager applications as well as the information on how to troubleshoot hardware problems. If the information is contained in the online help, the reader is pointed to the appropriate location. If the information is not available in the online help, then it will be addressed in this book.

Audience

This book is intended to be used by the following audience:

- Self-maintaining customers
- Service personnel

Access to Branch Device Manager

This chapter explains how to access Branch Device Manger by using a LAN connection, Network Management Console, and the WAN/Services port on the front of the Communication Manager Branch platform.

Accessing Branch Device Manager through the LAN

After the Communication Manager Branch is connected to the LAN, use the following steps to access Branch Device Manager:

1. Open a browser on your computer.
2. Type the IP address of the Communication Manager Branch system and press **Enter**.

   A Branch Device Manager logon screen appears.

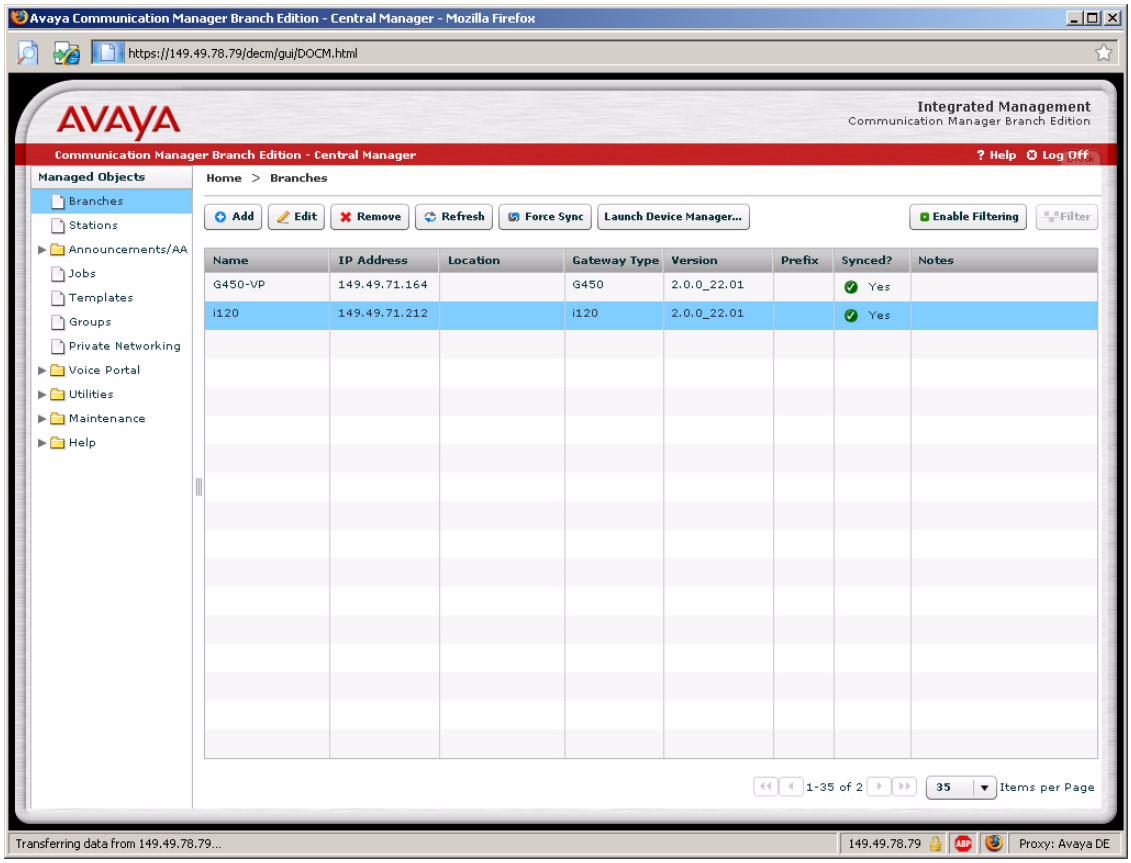
   - The default user name is administrator
   - The default password is password
3. If the Branch Device Manager logon screen does not appear:
   - Use Packet Internet Groper (PING) to check network connectivity:
     a. If the system does not respond to the PING, contact your support organization.
     b. If the system does respond to the PING but you still cannot access Branch Device Manager, check your Web proxy settings.

Accessing Branch Device Manager through Branch Central Manager

You can access the Branch Device Manager for a specific branch from Branch Central Manager as follows:

1. Open Branch Central Manager.
2. Open the **Managed Objects > Branches** page.
   - The following screen opens:

Figure 1: Branch Central Manager Branches page

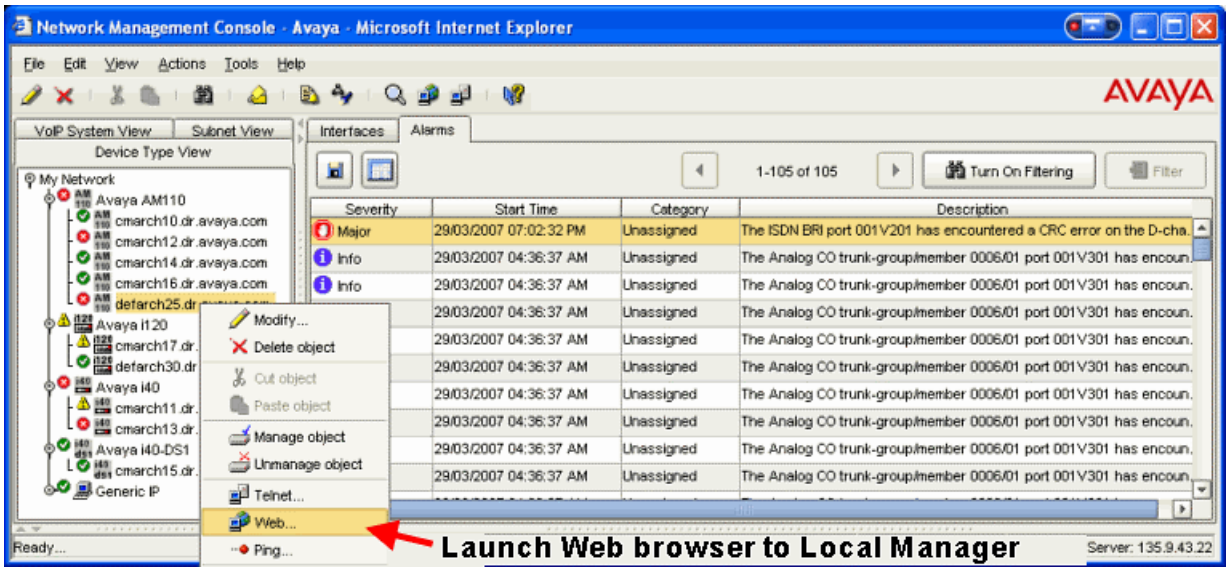


3. Select the branch from the list.
4. Click **Launch Branch Device Manager...**
   - The Branch Device Manager log-in screen opens.

Accessing Branch Device Manager through Avaya Network Management Console

Avaya Network Management Console is an optional tool that allows you to view the Communication Manager Branch systems in your network and provides a platform from which you can launch the Branch Device Manager interface.

Figure 2: Network Management Console



For more information on Network Management Console, see *IM Network Management Console User Guide,* 14-300169 at http://support.avaya.com.

Accessing Branch Device Manager through the Services port

DHCP Method

The Communication Manager Branch DHCP server automatically assigns 192.11.13.5 to a PC plugged into the WAN/Services port on the front of the Communication Manager Branch. A standard CAT 5 Ethernet cable is used for the connection. Once connected you can access Branch Device Manager by typing 192.11.13.6 in the address field of a browser window. If the Branch Device Manager screen does not appear:

- Check the health status of the Communication Manager Branch by looking at the LEDs. There are two LEDs on the Communication Manager Branch:
  - The ALM LED: The ALM LED lights red when a problem with the Communication Manager Branch has been detected or when the Communication Manager Branch is performing a reset.

- The CPU LED: The CPU LED lights a steady green when the Communication Manager Branch is operational. The CPU LED blinks on and off when the Communication Manager Branch is performing a reset.

If the CPU LED does not have a steady green light and/or the ALM LED is red, reboot the Communication Manager Branch using the reset button. For more information on rebooting the Communication Manager Branch, see Rebooting Communication Manager Branch on page 243. If rebooting the Communication Manager Branch does not correct the problem, call your system administrator or your support organization for assistance.

If your PC does not automatically get the 192.11.13.5 IP address, you must manually configure your PC using the instructions provided in the rest of this chapter.

Manual method

Use this section to manually configure your laptop before connecting to the Services port.

Network settings

Important:

Make a record of any IP addresses, DNS servers, or WINS entries that you change when you configure your computer.

The network settings must be configured as follows:

- TCP/IP properties - set the laptop's TCP/IP properties as follows:
  - IP address: **192.11.13.5**
  - Subnet mask: **255.255.255.252**
- Browser settings – configure the browser for a direct connection to the Internet. Do *not* use proxies.
- Server address – access the Communication Manager Branch using the URL http://192.11.13.6.

Note:

Do not configure a default gateway.

The names of the dialog boxes and buttons vary depending on the operating systems and the browser releases. If you need assistance in locating the correct place to enter this information, you can use the help system on your PC.

Setting TCP/IP properties in Windows

TCP/IP administration varies among Windows systems as described in this section.

Procedure to check your version of Windows

Use the following steps to check your version of Windows:

1. On your laptop, double-click the **My Computer** icon. The **My Computer** window opens.
2. Click **Help** on the My Computer window's tool bar.

   The Help menu opens and displays the version of Windows installed on your laptop.
3. Depending on your operating system, follow the instructions in one of the two following procedures.

To change TCP/IP properties and network settings (Windows 2000 and XP):

Use the following steps to change the TCP/IP properties and network settings:

1. Right-click **My Network Places** on your desktop or under the Start menu in XP.
2. Select **Properties** to display the **Network and Dial-up Connections** window.

   Windows should have automatically detected the Ethernet card in your system and created a LAN connection for you. More than one connection can appear.
3. Right-click the correct **Local Area Connection** from the list in the window.
4. Select **Properties** to display the Local Area Connection Properties dialog box.
5. Select **Internet Protocol (TCP/IP)**.
6. Click the **Properties** button. The Internet Protocol (TCP/IP) Properties screen appears.
7. On the General tab, select the radio button **Use the following IP address**. Enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

   Note:

   Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.
8. Disable DNS service as follows**:**
   a. Click the radio button labeled **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
   b. Click the **Advanced** button at the bottom of the screen. The Advanced TCP/IP Settings screen appears.

c. Click the **DNS** tab. Verify that the DNS server is not administered (the address field should be blank).

9. Disable WINS Resolution as follows:

   a. Click the **WINS** tab. Make sure WINS is not administered (the address field should be blank).

   b. Click **OK**. If warned about an empty primary WINS address, click **Yes** to continue.

10. Click **OK** twice to accept the address information and close the TCP/IP and Local Area Connection Properties dialog boxes.

11. Reboot the system if directed to do so.

    After you have made these changes to your computer's network configuration information, the Network and Dial-up Connections window shows the status of the Local Area Connection:

    - Enabled appears when the laptop's Ethernet cable is connected to the server.
    - Disabled or unplugged appears if the NIC is not connected to anything.

To change TCP/IP properties (Windows 95, 98, NT 4.0, and ME)

Use the following steps to change TCP/IP properties:

1. Access your computer's network information. On your desktop:
   - *Windows 95, 98, and NT:* Right-click **Network Neighborhood**.
   - *Windows ME:* Right-click **My Network Places**.
2. Select **Properties** to display the Network dialog box.
3. Locate the TCP/IP properties as follows:
   - *Windows 95, 98, and ME:* On the **Configuration** tab, scroll through the installed network components list to the TCP/IP part of the devices list. Select the TCP/IP device that corresponds to your Ethernet card.
   - *Windows NT:* On the Protocols tab, select **TCP/IP** in the installed network components list.
4. Select **Properties**.
5. In the TCP/IP Properties box, click the **IP Address** tab.
6. Click the radio button to **Specify an IP address**, and enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

   Note:

   Record any IP addresses, DNS settings, or WINS entries that you change. You may need to restore them later to connect to another network.

7. Disable DNS service as follows:

- *Windows 95, 98, and ME:* Click the **DNS Configuration** tab. Verify that the **Disable DNS** radio button is selected.
- *Windows NT:* Click the **DNS** tab.
  - If any IP addresses appear under DNS Service Search Order, make a note of them in case you need to restore them later.
  - Select each IP address in turn and click the **Remove** button.

8. Disable WINS Resolution as follows:
   - *Windows 95, 98, and ME:* Click the **WINS Configuration** tab. Verify that the **Disable WINS Resolution** radio button is selected.
   - *Windows NT:* Click the **WINS Address** tab.
     - If any IP addresses appear for the Primary and Secondary WINS servers, make a note of them in case you need to restore them later.
     - Clear each server entry.
     - Clear the check box for **Enable DNS for WINS Resolution**.
9. Click OK twice to accept the address information and close the Network dialog box.
10. Reboot the system if directed to do so.

Procedure to disable/bypass proxy servers in browser

If you are connecting a laptop directly to the WAN/Services port on the Communication Manager Branch, you must either disable or bypass proxy servers as described below.

Note:

Microsoft Internet Explorer (IE) browser is recommended.

1. Open Internet Explorer.
2. Verify that you have a direct connection with no proxies as follows:
3. Select **Tools > Internet Options**.
4. Click the **Connections** tab.
5. Click the **LAN Settings** button.
6. If **Use a proxy server for your LAN** is not selected, no change is necessary; click **Cancel** to exit.
7. If **Use a proxy server for your LAN** is selected, you can:
   - Deselect it and click **OK** to exit;
   - Or, you can leave it selected and configure your browser to bypass the proxy server whenever you are connected to the WAN/Services port as follows:

- Click **Advanced.**
- Type **192.11.13.6** in the Exceptions box. If there are other entries in this box, add to the list of entries and separate entries with a “;”.
- Click **OK** to exit.

Connect the laptop to Services port on the Communication Manager Branch

You can use either a standard CAT5 Ethernet cable or a crossover cable to connect the laptop to the Ethernet WAN/Services port. If you use a crossover cable:

- Crossover cables come in various lengths and are commercially available.
- For crossover cable pinout connections, see Table 1. Crossover of the transmit and the receive pairs is required.

Table 1: Crossover cable pinout chart

Pin to Communication Manager Branch WAN/Services port	connects to	Pin to laptop's Ethernet card
8		8
7		7
6		2
5		5
4		4
3		1
2		6
1		3

To connect your laptop to the WAN/Services port:

1. Connect one end of the cable to the laptop and the other end to the ETH WAN or Ethernet Services/WAN port on the front of the Communication Manager Branch platform. For the Services port location, see Figure 3, Figure 4 and Figure 5.

Figure 3: Communication Manager Branch i40 front panel

Figure 4: Communication Manager Branch i120 front panel

Figure 5: Communication Manager Branch G450 Media Gateway front panel

Figure notes:

1. **Services port**

2. If your laptop is configured with the correct network settings, open a browser and type **192.11.13.6** in the browser's address or location field**.** The Branch Device Manager logon screen appears.

Station Problems

This chapter contains information on troubleshooting stations and possible resolutions to station problems.

Basic station troubleshooting guidelines

Use the following guidelines to troubleshoot problems on a Communication Manager Branch station:

1. Identity and record if the problem is on:
   - One station;
   - Or all stations of one type;
   - Or Multiple station types.

     There are four types of stations supported on Communication Manager Branch:

     - H.323
     - Digital Enhanced Cordless Telecommunications (DECT)
     - SIP
     - Analog

     If the problem is only on one station type, record the type of station. The station type is marked somewhere on the station. Some station types are marked on the underside of the station or on the base.

     Find your station in the following list of supported station types:

     - H.323
       - 4610SW
       - 4621SW
       - H323 Softphone
       - 1603
       - 1608
       - 1616
     - DECT
       - WT3701

    - WT3711
- SIP
    - 9610
    - 9620
    - 9630
    - 9640
    - 9650
    - Cisco 7940
    - Cisco 7940G
    - Cisco 7960
    - Cisco 7960G
- Analog
    - 6211
    - 6219
    - 6221
- DCP
    - 2402
    - 2410
    - 2420
- Wireless
    - 3631
    - 3641
    - 3645

2. Identify the problem: Regardless if the problem appears on only one station or multiple stations, you must obtain an understanding of what the real issue is. Table 2 and Table 3 provide examples of possible station problems and resolutions. The tables can be used to fix a problem or obtain a better understanding of the issue before calling support. The tables also contain pointers to advanced troubleshooting information for administrators and maintenance support personal.

   For single station problems, use Table 2.

   For multi-station problems, use Table 3.

Table 2: Single station problems

Station Type	Problem	Resolution
Analog	No dial tone	1. Check station wiring into the station to ensure that the station is properly connected. 2. Change the station with one of the same type. 3. Call your system administrator or support person for help. If you are the system administrator or a support person, see One station does not have dial tone on page 36.
H.323 SIP	No dial tone or lights	1. Check station wiring into the station to ensure that the station is properly connected. 2. Check the power source to ensure that the station is receiving power. In most cases, power is supplied over the Ethernet. If power is not over the Ethernet, verify that the Telephone Power Module is plugged into the power source. If you are not sure where the station gets power, contact your administrator. **Note:** If more than one station is out of service, check for mid-span power. 3. Unplug the station from the LAN jack and plug it back in. 4. Change the station with one of the same type. 5. Call your support organization. If you are the system administrator or a support person, see One station does not have dial tone on page 36.
		1 of 5

Table 2: Single station problems (continued)

Station Type	Problem	Resolution
H.323 SIP	Lights but no dial tone	The lights on the phone indicate that the station is receiving power. The loss of dial tone can be caused by many factors: 1. Hardware: a. Verify that the lights change when the handset is off-hook. b. Check the cord from the station to the handset to ensure that it is properly connected. c. Check the station for a speaker. If the speaker works, then: - Change the handset with a handset of the same type. - Change the handset cord. d. If this is a 4600 series station: - Perform the station's Test procedure: With the station on-hook, press 8 3 7 8 # (test) on the keypad. The display indicates that the test has started and reports if the test passes or fails. If nothing appears on the display and the station is receiving power, then go to the next step. e. Change the station with one of the same set type. f. If the above steps do not correct the problem, call your administrator or your support organization. 2. Loss of connectivity to Communication Manager Branch: If there is a message on the display record the message and contact the administrator or support organization. If you are a administrator or a support person, see One station does not have dial tone on page 36 or Stations do not register on page 38.
SIP	Display shows 'Attempting login failed' or 'Login failed retrying'	The network connection between the station and the SIP server was interrupted or lost. The station automatically attempts to re-register with the SIP server. Call the system administrator or a support person for help. If you are the system administrator or a support person, see: ● Checking the status of a station on Branch Device Manager on page 32 ● Stations do not register on page 38
		2 of 5

Table 2: Single station problems (continued)

Station Type	Problem	Resolution
H.323	Display shows 'Discovering'	When an H.323 station displays 'Discovering', the network connection between the station and Communication Manager Branch was interrupted or lost. The station automatically attempts to re-register with the Communication Manager Branch. Call your system administrator or a support person for help. If you are the system administrator or a support person, see: • Checking the status of a station on Branch Device Manager on page 32 • Stations do not register on page 38
H.323	Display shows 'DHCP XX seconds'	When an H.323 station displays 'DHCP XX seconds' the station is not receiving an IP address from the DHCP server. Call your system administrator or a support person for help. If you are the system administrator or a support person, see: • Checking the status of a station on Branch Device Manager on page 32 • Stations do not register on page 38
H.323 SIP	Poor voice quality	Poor voice quality is generally associated with network issues. Call the system administrator or a support person for help. If you have a 4600 series station, there is a method of viewing the network audio quality *while* you are on a call: 1. Press the Options button. 2. Select Network Audio Quality. 3. If this option is administered on the station, you see the Audio Status screen. 4. Inform a support person of any information that appears. If you are the system administrator or a support person, for more information see I have poor voice quality on page 40.
		3 of 5

Table 2: Single station problems (continued)

Station Type	Problem	Resolution
Analog	Cannot make or receive calls	• Can you make a station to station call? Making a call to another station verifies that the station is working properly and the problem is likely associated with the trunks, outside lines, or inter-branch facilities. If a station to station call works, call the system administrator or a support person. • If a station to station call does not work: 1. Check the volume of the station to ensure that you can hear when a call arrives. 2. Replace the station with one of the same type. 3. Call the system administrator or a support person. If you are the system administrator or a support person, see: • Checking the status of a station on Branch Device Manager on page 32 • Testing a station using Branch Device Manager on page 35 • Trunk or Outside Line Problems on page 61
H.323 SIP	Cannot make or receive calls	• Do you have dial tone on the station? - If not, go to No dial tone or lights on page 25 or Lights but no dial tone on page 26. • Can you make a station to station call? Making a call to another station verifies that the station is working properly and the problem is likely associated with the trunks, outside lines, or inter-branch facilities. If a station to station call works, call the system administrator or a support person. • If the station has a display, what does it say? Record the message and report it to the system administrator or a support person. • If you are the system administrator or support person, see: - Checking the status of a station on Branch Device Manager on page 32 - Testing a station using Branch Device Manager on page 35 - Trunk or Outside Line Problems on page 61
H.323 SIP analog	Voice mail	Voice mail is administered by the system administrator. For help troubleshooting voice mail problems, see Voice Mail on page 69.
		4 of 5

Table 2: Single station problems (continued)

Station Type	Problem	Resolution
H.323 SIP	Power problems	In most cases, power for the IP and SIP station power is provided by the ethernet switch and delivered over the station wiring. 1. Unplug and plug the station back in 2. Move the station to a different jack or switch-port. 3. Change the station to another station of the same type. 4. Call the system administrator or a support person. If you are the system administrator or a support person, see I don't have power on a station on page 38.
H.323 SIP	Button problems	Button assignments are administered by the system administrator. If a button assignment is incorrect call the system administrator for help.
		5 of 5

Table 3: Multi station problems

Station Type	Problem	Resolution
All	No dial tone or lights	Call the system administrator or a support person. If you are the system administrator or a support person, see I don't have dial tone on Communication Manager Branch on page 37.
H.323 SIP	Voice quality is poor	Poor voice quality is generally associated with network issues. Call the system administrator or a support person for help. If you have a 4600 series station, there is a method of viewing the network audio quality *while* you are on a call: 1. Press the Options button. 2. Select Network Audio Quality 3. If this option is administered on the station, you see the Audio Status screen. 4. Inform the system administrator or a support person of any information that appears. If you are the system administrator or a support person, see I have poor voice quality on page 40.
		1 of 3

Table 3: Multi station problems (continued)

Station Type	Problem	Resolution
All	Cannot make or receive calls	Trouble making or receiving calls is generally a problem with one or more trunks, outside lines, or an inter-branch facility. Call the system administrator or a support person. If you are the system administrator or a support person, you can status, busy out, release busy, and test most outside lines and trunks using the following information: • Status screens and available functions for outside lines and trunks on page 61 • Busy a group or a group member using Branch Device Manager on page 64 • Release the busy of a trunk or outside line group using Branch Device Manager on page 65 • Testing a trunk group using Branch Device Manager on page 63 • Testing a outside line using Branch Device Manager on page 63
SIP	Display shows 'Attempting login failed' or 'Login failed retrying'	The network connection between the station and the SIP server was interrupted or lost. The station automatically attempts to re-register with the SIP server. Call the system administrator or a support person for help. If you are the system administrator or a support person, see: • Checking the status of a station on Branch Device Manager on page 32 • Stations do not register on page 38
H.323 SIP	Displays says 'Discovering' or Stations do not register	An H.323 or SIP stations show a message in the display when it cannot register. The message gives an indication of what the registration problem is. For example, an H.323 station can display: • 'Discovering' when there is a problem with the IP connectivity between the station and Communication Manager Branch. • 'DHCP XX seconds' when the station is not receiving an IP address from the DHCP server. Call the system administrator or a support person for help. If you are the system administrator or a support person, see: • Checking the status of a station on Branch Device Manager on page 32 • Stations do not register on page 38
DECT	DECT stations do not register	DECT station information can be found in the *Avaya IP DECT Installation, Administration, and Maintenance* book (16-601625).
		2 of 3

Table 3: Multi station problems (continued)

Station Type	Problem	Resolution
H.323 SIP	Display problems	Identify the issue with the display. For example: • Is the display blank or operational? • Is the language correct? Call the system administrator or a support person. If you are the system administrator or a system support person, see: • Checking the status of a station on Branch Device Manager on page 32 • Checking the administration of a station using Branch Device Manager on page 34 • A station displays the wrong language on page 38
All	Voice mail problems	Voice mail is administered by the system administrator. For help testing and troubleshooting voice mail, see Voice Mail on page 69.
H.323 SIP	Power problems	In most cases, power for the H.323 and SIP stations is provided over the Ethernet wires. If you are the system administrator or a support person verify: • If the stations are plugged directly into Communication Manager Branch. If they are then reboot Communication Manager Branch or check the power from the AC outlet to Communication Manager Branch. To reboot Communication Manager Branch, see Rebooting Communication Manager Branch on page 243. • If the stations are connected directly into the Ethernet switch, check the switch to verify that it is running properly. • Check the mid-span power unit. 1. In Communication Manager Branch go to: **Maintenance and Monitoring> Platforms> Ethernet Ports** 2. Click **Search > Delivery**. A unit should be showing electrical flow.
		3 of 3

Advanced station troubleshooting using Branch Device Manager

This section provides advanced station troubleshooting information for the system administrator or a support person who has access to Branch Device Manager and has knowledge about data and telephony.

Checking the status of a station on Branch Device Manager

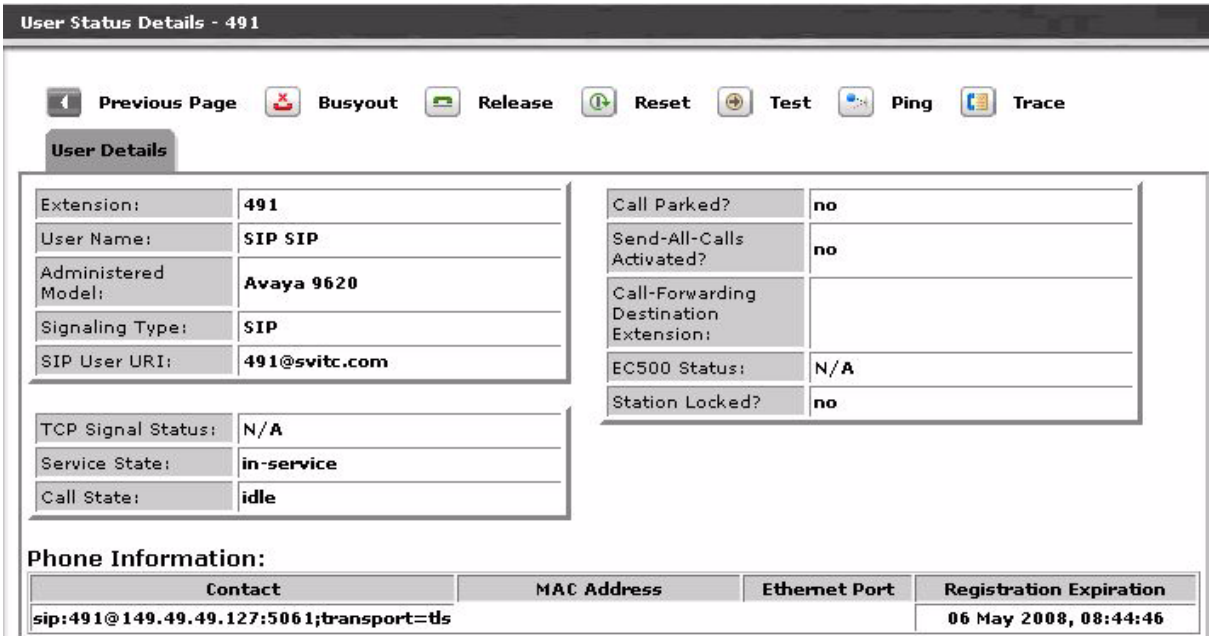
The first step in station troubleshooting is to find out more about the station using the **User Status** screen. The **User Status** screen (Figure 6) displays important station information and station status. For example, 'in service' appears in the **Status** column if the station is registered.

In addition to displaying the current station status, the **User Status** screen also provides the following functions:

- Busyout: Removes the station from service. For more information, see Busy a station using Branch Device Manager on page 34.
- Release: Removes the busy and restores the station to service. For more information, see Release a station busy using Branch Device Manager on page 35.
- Reset: Reboots the station.
- Test: Tests the station. For more information, see Testing a station using Branch Device Manager on page 35.
- Ping: Verifies network connectivity to the station. For more information on the PING command, see Network Diagnostics on page 101.
- Trace: Displays path information (ping, codex, jitter and other parameters).

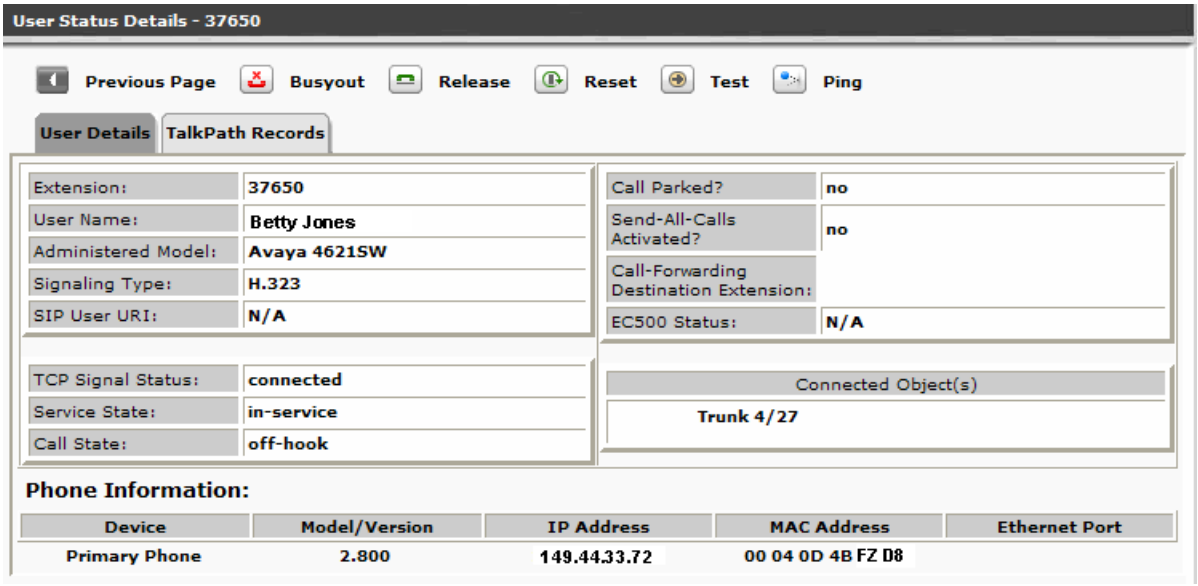
To display the **User Status** screen, click **Users** under Maintenance and Monitoring > Telephony.

Figure 6: User Status screen



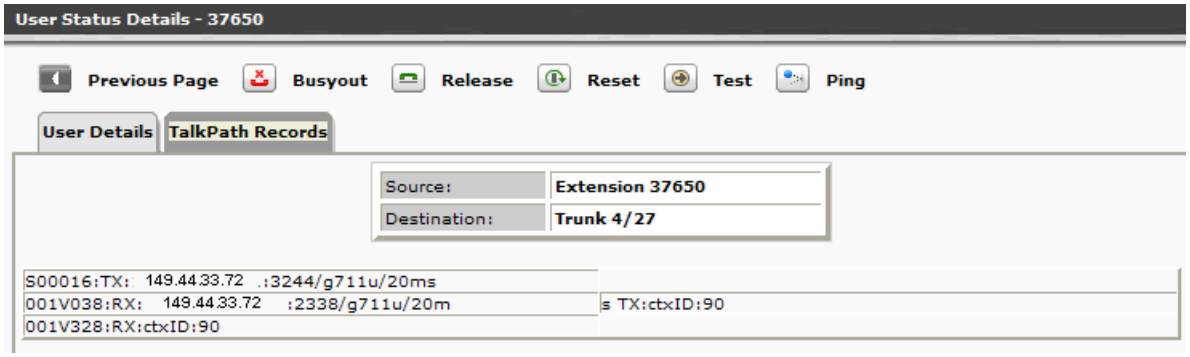
Additional details about the station can be obtained by clicking any column of data associated with the station. A **User Status Details** screen appears as shown in example Figure 7.

Figure 7: User Status Details screen



If a station's status is off-hook, information about the connection appears in the Connected Object(s) box. Additional information about the connection can be obtained by clicking the TalkPath Records tab as shown in Figure 8.

Figure 8: TalkPath Records tab



For more information on both the **User Status** and the **User Status Details** screen, see Branch Device Manager online help.

Checking the administration of a station using Branch Device Manager

To see how a station was administered, click **Users** under Configuration. The **Users** screen provides information that can help in resolving a station trouble. For example:

- Verifying the station type: Under the Stations tab, check the **Set Type** field.
- Station display is incorrect: Under the General tab, check the **Display Name** and the **Preferred Language** field.
- Voice mail is not working:
  a. Under the Voicemail tab, verify that there is a check mark next to 'User has a voicemail mailbox on this system'.
  b. Check the mailbox type. For more information on what the different types mean, see Verifying voice mail administration on page 69.
  c. If voice mail administration appears to be correct, see Voice Mail on page 69. Under the Station tab, verify that Voicemail appears in the **Coverage** field.
- Port information: Under the Station tab, record the port from the Port field.
- Button assignment: Under the Buttons tab, verify the button assignment and the ringing type for the station.

For more information on the columns and fields within the **Users** screen, see the Branch Device Manager online help.

Busy a station using Branch Device Manager

When you busy a station, you remove it from service. A busied station looks different based on the station type. For example, a busied analog station will not have dial tone while a busied SIP or IP station will be unregistered. You may want to busy a station that is causing problems, make the station inactive to users, or attempt to fix a problem by busying out a station and then releasing it.

To busy a station:

1. Log onto Branch Device Manager and click **Users** under Maintenance and Monitoring > Telephony.
2. Click the box next to the station you want to busy.
3. Click **Busyout Checked** from the selection on the top of the screen

   A **Maintenance Operation Results** screen appears displaying the status of the station.

For more information on the columns and fields in the **Users Status** screen, see the Branch Device Manager online help.

Release a station busy using Branch Device Manager

A system administrator or support person can release a station busy once the reason for placing the station in a busy condition has passed.

To release a station:

1. Log onto Branch Device Manager and click **Users** under Maintenance and Monitoring > Telephony.
2. Click the box next to the station you want to release.
3. Click **Release Checked** from the selection on the top of the screen.

   A **Maintenance Operation Results** screen appears displaying the status of the station.

For more information on the columns and fields within the **User Status** screen, see the Branch Device Manager online help.

Testing a station using Branch Device Manager

When you select a station to be tested, Branch Device Manager runs multiple tests against the station. As each test passes or fails, the system displays details that help you troubleshoot the problem. The number and kind of test can change depending on the type of station being tested.

To test a station:

1. Log onto Branch Device Manager and click **Users** under Maintenance and Monitoring > Telephony.
2. Click the box next to the station you want to test.
3. Click **Test Selected** from the selection on the top of the screen. A number of tests execute against the station. The name of the test and the test results are displayed. For more information on the errors and help with resolutions, see Maintenance Tests on page 139.

For more information on the columns and fields within the **User Status** screen, see the Branch Device Manager online help.

One station does not have dial tone

Use the following steps to troubleshoot and fix a station with no dial tone:

1. Check the status of the station, see Checking the status of a station on Branch Device Manager on page 32.
   - If the station is in a busy state, release it (see, Release a station busy using Branch Device Manager on page 35).
   - Busy the station, then release it (see Busy a station using Branch Device Manager on page 34 and Release a station busy using Branch Device Manager on page 35).
   - For SIP or H.323 stations: If the station is not registered or if there is a loss of communication to Communication Manager Branch, there will be a message that displays on the station. For more information, see:
     - SIP stations:
       - 9600 series SIP stations: *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (16-601943) at http://support.avaya.com.
     - 4600 series stations:
       - *4600 Series IP Telephone Installation Guide* (555-233-128) at http://support.avaya.com.
       - *4600 Series IP Telephone LAN Administrator Guide* (555-233-507) at http://support.avaya.com.
     - 1600 series IP station:
       - *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide* (16-601438) at http://support.avaya.com.
2. Check the administration of the station (see Checking the administration of a station using Branch Device Manager on page 34):
   - Verify that the administered station type is the same as the one that was installed.
3. Test the station: To test a station, use the steps in Testing a station using Branch Device Manager on page 35. If the station does not pass a test, check the list of error codes in Maintenance Tests on page 139 for possible resolutions.

I don’t have dial tone on Communication Manager Branch

Use the following steps to troubleshoot a system that does not have dial tone.

CO Phones

1. Try accessing Branch Device Manager through the LAN. If you are at the location of the problem and you cannot access the Branch Device Manager through the LAN, try accessing Branch Device Manager through the Services port on the front of the Communication Manager Branch. Follow the instructions at Accessing Branch Device Manager through the Services port on page 15. If you still cannot access Branch Device Manager, reboot the system using the steps outlined in Rebooting Communication Manager Branch on page 243.
2. If you can access Branch Device Manager, verify that the loss of dial tone is not related to a registration issue. To verify if the stations are registered, log onto Branch Device Manager and click **Users** under Maintenance and Monitoring > Telephony. The **User Status** screen appears. The **Status** column displays ’in service’ if the stations are registered.
3. Check the **Status** field in the **System Summary** screen for active alarms. The **System Summary** screen can be found under Maintenance and Monitoring > System Status. If ’Active Alarms’ appears in the **Status** field, display the active alarms by clicking Maintenance and Monitoring > Alarms. A list of the active alarms display in the **Display Active Alarms** screen. For more information on alarms, see Alarms.

Analog Phones

1. Switch the phone and cable.
2. Check the user status and ensure that the line is in service.
3. Try accessing Branch Device Manager through the LAN. If you are at the location of the problem and you cannot access the Branch Device Manager through the LAN, try accessing Branch Device Manager through the Services port on the front of the Communication Manager Branch. Follow the instructions at Accessing Branch Device Manager through the Services port on page 15. If you still cannot access Branch Device Manager, reboot the system using the steps outlined in Rebooting Communication Manager Branch on page 243.
4. Check the **Status** field in the **System Summary** screen for active alarms. The **System Summary** screen can be found under Maintenance and Monitoring > System Status. If ’Active Alarms’ appears in the **Status** field, display the active alarms by clicking Maintenance and Monitoring > Alarms. A list of the active alarms display in the **Display Active Alarms** screen. For more information on alarms, see Alarms.

A station displays the wrong language

Use the following steps if a station displays the wrong language:

1. Log onto Branch Device Manager and click **Users** under the Configuration heading.
2. Find the station in the list of users and click the extension number.
3. Verify that the displayed language in the **Preferred Language** field. If the displayed language is not correct, select your preferred language from the drop-down list and click **Edit**.

I don’t have power on a station

For information on H.323 stations see:

- *4600 Series IP Telephone LAN Administrator Guide,* 555-233-507*,* issue 6 or greater
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide* (16-601438)

For information on SIP stations, see *Avaya one-X Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide,* 16-601943.

Stations do not register

To verify if a station is registered, click **Users** under Maintenance and Monitoring > Telephony on the Branch Device Manager interface. The **Status** column displays ’in service’ or ’not registered’ for the H.323 or SIP stations.

There can be multiple reasons for a station not to register. Avaya provides documentation for each station type to aid in troubleshooting. Once you have read the documentation that pertains to your station type, return to this document for more troubleshooting tips.

For registration help on H.323 stations, see:

- *4600 Series IP Telephone LAN Administrator Guide,* 555-233-507, Issue 6 or greater
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide,* 16-601438

For registration help on SIP stations, see *Avaya one-X Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide,* 16-601943.

The DHCP server on Communication Manager Branch

An IP station needs an IP address to register. A Dynamic Host Configuration Protocol (DHCP) server provides each IP station with a unique IP address. If the DHCP server on Communication Manager Branch is used, it is administered using the Branch Device Manager interface. If the DHCP administration is incorrect or if there is a problem with the DHCP server, the IP stations will not receive an IP address and will not be able to register with the call server.

You can verify the performance of the Communication Manager Branch DHCP server by clicking **DHCP Server** under Maintenance and Monitoring > Platform > Data Services. The **DHCP Server Bindings and Statistics** screen displays.

The **DHCP Server Bindings and Statistics** screen provides a list of assigned IP addresses and statistics about the overall performance of the DHCP server such as:

- The number of requests for IP addresses
- The number of IP stations that were declined
- The number of IP addresses that were released.

For more information on the **DHCP server Bindings and Statistics** screen, see DHCP server diagnostics on page 106.

I have poor voice quality

When troubleshooting voice quality, many factors should be considered such as equipment configuration, how the system was configured, network or environmental conditions, etc. To begin troubleshooting you must first define the problem and then identify how widespread the problem is (one or all stations). For help defining and troubleshooting the problem, see Voice Quality Issues on page 41.

Voice Quality Issues

Voice quality issues have many and varied causes. Problems may be caused by equipment configuration or administration such as low bit -rate speech coders, defective or improperly (impedance) matched hybrid trunk circuits, damaged phone equipment (microphones, loudspeakers, or earpieces), or by network or environmental conditions.

This section provides a guide to troubleshooting voice quality issues and determining which component(s) in the call topology is causing the problem.

Troubleshooting Voice Quality Issues

Troubleshooting involves determining what the user is experiencing, ensuring the equipment is up-to-date, whether the problem is reproducible or not, whether the problem is near-end or far-end, and determining if the problem is a phone or a component in the network.

1. Determine the following information from the user:
   - Call type (station-to-station, trunk)
   - What equipment is being used (phone, headset, speakerphone)
   - Whether an operation is being performed when the voice quality issue occurs (transfer, conference)
2. Make sure the system components are up-to-date with the correct software/firmware releases and hardware versions.
3. It is important that you outline the exact end-to-end route the voice signal takes through the system and across the customer network to the end network device.
4. Determine the following:
   - **If the problem involves IP telephones and is intermittent**, work with the customer to set up a network analyzer to monitor the network for 24/7 operation so that the call information is captured at the time the problem occurs. When the user experiences the problem, the trace can be stopped and the RTP analyzed. Use this data in conjunction with the network topology and call flow to determine what network element is causing the voice quality issue.
   - **If the problem occurs on trunk calls**, a trunk ID button can be programmed on the user's phone so that when the voice problem occurs, the specific trunk that is accessed can be obtained. Also, the VERIFY (also known as **busy verify**) button can be used by a third party station to listen to the conversation voice quality. Using **verify** to bridge onto a trunk might change how it sounds, and that in itself is extra data.

- **If the problem is reproducible**, establish a call with the phone experiencing the voice quality issue and note the call traversal (the path the call takes through the system) Once the call flow has been identified, all of the network components involved are known. Try to determine whether the problem is limited to specific system components by initiating new calls that traverse a fewer number of system components. For example, test if the voice quality issue can be reproduced on a station-to-station call between two phones on the same port network. Determine if the voice quality issue exists with IP to IP direct (shuffling), whether the voice quality issue only exists when calls traverse a VoIP resource, or if the problem occurs only on a trunk call.

5. Use the VoIP Monitoring Manager (VMM) (if available). VMM allows for measuring many of the problems mentioned in this section. It displays VoIP characteristics history and the properties of a VoIP session.
6. Determine the voice quality issue the user is experiencing. The following table contains a list of possible voice quality issues and how to resolve them.

Voice Quality Issue	See...
Audio contains static	Static
Audio is choppy, popping, or clicking	Clipping
Audio is choppy in both directions	Clipping during double-talk
Caller cannot hear the agent	Cannot hear agent
Caller is too loud/too soft	Caller too loud/too soft
Caller cannot hear me	Caller cannot hear me
Muffled Speech	Muffled Speech
Hollow or reverberant speech	Reverberant Speech
Synthetic, Mechanical, or Robotic Speech	Synthetic, Mechanical or Robotic Speech
Stutter	Stutter
Changes in volume during call	Speech-level Pumping
Hiss	Hiss or White Noise
Motor-boating	Motor-boating
Hum	Hum
Distorted Music-on-Hold	Distorted Music-on-Hold
Echo	Echo

Static

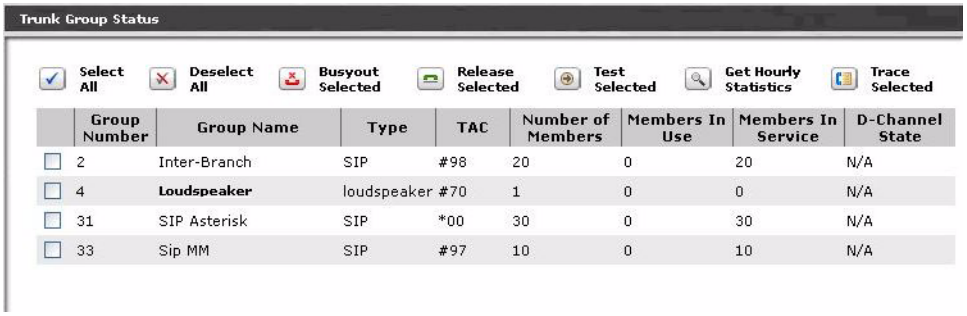
Static is an unnatural or raspy noise, similar to the sound of an AM radio when tuned to a very weak or nonexistent radio station.

Possible causes: Headset or soundcard, radio interference, lost speech packets and/or bit errors.

Recommended actions:

1. Under **Monitoring> Telephony> Trunk Group**, choose the analog trunk.
2. Select **Trace Selected**.

Figure 9: Trace Selected



3. Click **Start** and begin to talk.

   You will receive specifications on the trunk's performance.

4. Troubleshoot the Trunk as needed.

Other recommended actions:

1. Check environmental conditions. Local noise sources such as computer fans, PC speakers, noise from air conditioning, or noisy office environments can have an affect on voice quality being perceived by the user.
2. Replace the headset or soundcard with Avaya recommended hardware. See http://support.avaya.com
3. Use a network analyzer to determine if there is packet loss or bit errors.

Clipping

Clipping is speech where portions of the speech signal are not heard. This can occur when large numbers of successive speech packets are not received due to excessive network congestion.

Possible causes: Packet loss or late packet arrival, poorly performing PC hardware

Recommended actions for station to station calls:

1. Ensure the network is performing optimally. Increase network bandwidth to the PC or decrease network bandwidth usage.
2. Ensure optimal PC performance by disabling unused hardware.
3. Check the soundcard manufacturer's support site for optimization tips and updated drivers.
4. Ensure the soft phone Jitter Buffer setting is set to Automatic.
5. Amplitude clipping can be determined by running an Ethereal trace and converting the RTP stream to a .wav file and analyzing that file with a tool such as Audacity. The clipped speech signal can be observed graphically. Amplitude clipping coming from outside the customer's network is typically caused the far-end phone. If amplitude clipping is present, identify solution elements that add gain and verify each element is applying the expected amount of gain.This is common in wireless phones, where the RF-signal strength fades as the user moves within the environment.
6. Determine packet loss by using a network analyzer. Take network QoS measurements and note the values of packet loss, delay, jitter, etc.
7. Administer the DS1 echo canceller setting to a less aggressive echo canceller setting. See Echo Cancellation Levels.

Recommendations for station-to-core calls:

1. In the Communication Manager Branch, go to **Configuration> Public Networking> Trunk Group**.
2. Select the group.
3. Click the **Media Tab**.
4. Under Codec set, enable Silence Suppression.

Clipping during double-talk

Clipping during double-talk is clipping that is heard when both parties of a call talk at the same time.

Possible cause: the excessive use of echo suppression at some point within the network.

Recommended action:

1. Check the echo suppressor function of the echo cancellers in the network. Also check Echo Cancellation Levels.

Cannot hear agent

Possible causes: Headset is muted, faulty headset or soundcard, improper adjustment of microphone input.

Recommended actions:

1. Verify that the headset is not muted.
2. Turn up the microphone input level. This may require you to disable the microphone Automatic Gain Control using the Audio Tuning Wizard.
3. If the soundcard has an option for a +20 db boost, make sure it is enabled.

Caller too loud/too soft

Possible causes: Improper volume control setting, master volume and/or wave volume is set too high/low.

Recommended actions:

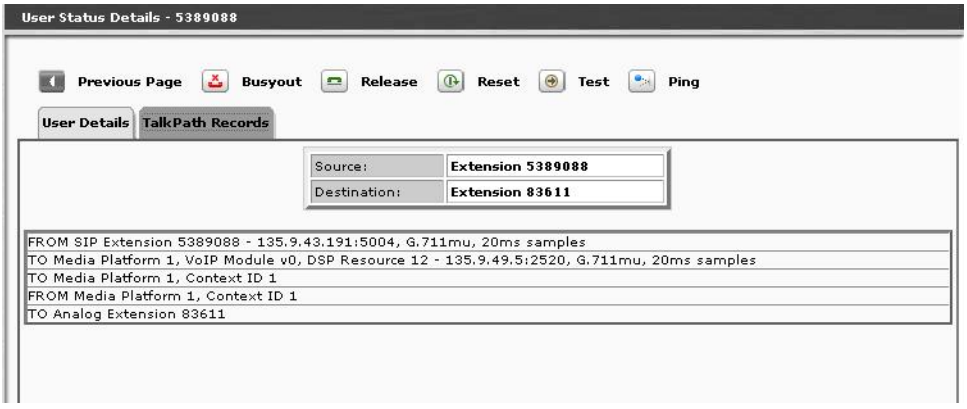
1. Check the Windows master volume and wave volume sound settings.
2. Ensure no other applications are changing PC volume settings.
3. If the caller is still too loud or too soft, the cause may be a poorly performing headset or soundcard. Adjust the amplification of the call by adjusting the Receive Gain from the Audio Options menu. Note that adjusting the gain distorts the original signal which may decrease the voice quality.

Caller cannot hear me

Possible causes: Poorly performing headset or soundcard, or one-way talk path.

Recommended actions:

1. Adjust the microphone input control.
2. Adjust the amplification of the transmission by adjusting the Transmit Gain from the Audio options menu. Note that adjusting the gain distorts the original signal which may decrease the voice quality.
3. If the problem is not the headset or soundcard, it most likely is a one-way talk path, which can be tricky to diagnose.
   a. Check the talk path Click on **User** under **Maintenance & Monitoring > Telephony**, then select the affected user. If the call is still up, click on the **Talk Path** tab.



b. Ping from one station to the other, then ping the reverse direction.

c. Look at VMM or other network monitoring tools for complaints in the network along the path that the voice is taking.

Muffled Speech

Muffled speech has an unnatural loss of high-frequency content.

Possible causes: Microphone assembly in the handset, low bit-rate speech coders.

Recommended actions:

1. Swap out the equipment to determine if this is the cause.
2. If this does not resolve the problem, set up a network analyzer to monitor the network for 24/7 operation so that the call information is captured at the time the problem occurs. When the user experiences the problem, the trace can be stopped and the RTF analyzed. Use this data in conjunction with the network topology and call flow to determine which network element is causing the problem.

Reverberant Speech

Reverberant speech sounds like the person you are listening to is speaking in a barrel or large empty room.

Possible causes: the speaker using a speakerphone, network echo.

Recommended actions:

1. For optimum speakerphone performance, make sure the phone is sufficiently clear of any shelves or clutter near the phone that could provide an echo path during speakerphone use. Hard and reflective surfaces such as metal walls and glass windows can promote reverberation when speakerphones are used and result in echo complaints from the far-end.
2. If this does not resolve the problem, see Echo.

Synthetic, Mechanical or Robotic Speech

Speech sounds monotonic and robotic. Recognizing who is speaking is often difficult.

Possible causes: Faulty or bad acting hardware (e.g., a DSP chip in a cell phone, base station, or VoIP gateway), use of a low bit-rate speech codec, packet loss or frame erasures.

Recommended actions:

1. Take network QoS measurements and note the values of packet loss, delay, and jitter.
2. Set up a network analyzer to monitor the network for 24/7 operation so that the call information is captured at the time the problem occurs. When the user experiences the problem, the trace can be stopped and the RTF analyzed. Use this data in conjunction with the network topology and call flow to determine which network element is causing the problem.

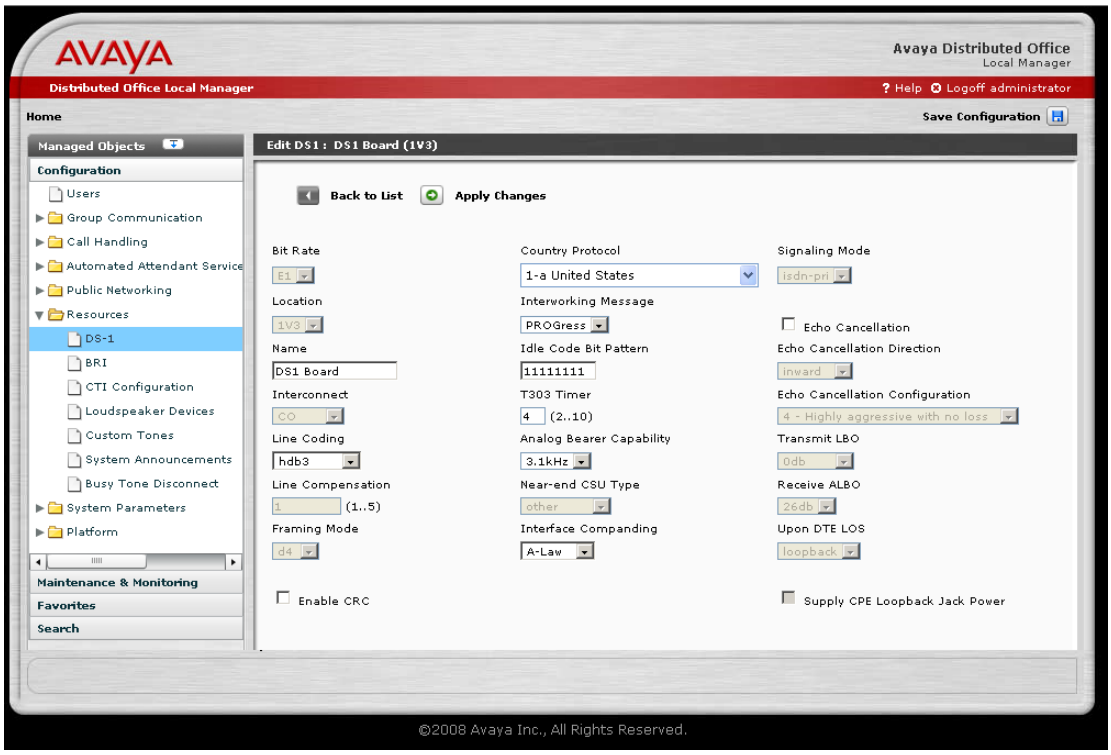
Stutter

This term is often used to describe an effect caused by the repetition of short bursts of noise or speech, such as "da-da-da-da" or "fa-fa-fa-fa".

Possible cause: one or more network elements (e.g., router or switch) is a bottleneck to the timely transmission of speech packets.

Recommended action:

1. Stutter can be traced to its origin by setting up a network analyzer to analyze the call topology and find out where the bottleneck is occurring.
2. Check the configuration/administration of the DS1 trunk under **Configuration > Resources > DS-1**, then click on the trunk.



Speech-level Pumping

Speech gets louder, softer, then louder again over the course of a call, often over a period of just several seconds.

Possible causes: Phone's Automatic Gain Control, DS1 echo canceller level.

Recommended actions:

1. Adjust the DS1 echo canceller to a less aggressive setting. See Echo Cancellation Levels.
2. If the problem still occurs, turn off the phone's Automatic Gain Control.
3. If the problem still occurs, reduce the TX gain in the 4610/4620 Settings file.
4. If the problem is not resolved, work with the customer to set up a network analyzer to monitor the network 24/7 such that when the user experiences the problem, the trace can be stopped and the data analyzed. Use this data in conjunction with the network topology and call flow to determine what network element is causing the problem.

Hiss or White Noise

Hiss or white noise is relatively natural-sounding noise containing energy at all frequencies.

Possible cause: idle-channel noise is too high.

Recommended action:

1. Typical idle-channel noise should measure approximately 15dBrnC. This can be determined using a pair of Sage 925VSTs, or a Sage 825VST with a Sage Responder.

Motor-boating

Motor-boating is a repetitive noise that is separate and distinct from the speaker's voice.

Possible cause: power-line interference at telephone endpoints.

Recommended action:

1. Check grounds and any nearby high voltage sources to determine the cause of this problem.

Hum

Possible cause: Hum noise often occurs when a source of 50 Hz or 60 Hz electrical power is located near a telephone. The power source emits an RF (radio frequency) field that induces a hum-like noise that is heard through the phone's handset/headset earpiece or speakerphone loudspeaker.

Recommended action:

1. Make sure that a 50Hz or 60Hz electrical power source is not located near the telephone.

Distorted Music-on-Hold

The possible cause of this problem could be that the entry point of the call is separated from the actual system in which the call is being put on hold. For example, if the call came in on Communication Manager Branch #1 and is then transferred to Communication Manager Branch

#2 which is across a WAN connection. The call gets put on hold in Communication Manager Branch #2.

Recommended action:

1. Switch phones to ensure that the problem is not the phone itself.
2. There could also be a problem with the codecs selected. Since the codecs used are designed to transport voice (but not music), the codecs could conflict with the music being played. However, the codecs can not be changed.

Echo

Echo, either electrical or acoustic, is a function of delay in the call path.

Possible causes: Headset or soundcard, improper adjustment of microphone input, system configuration, room acoustic levels, impedance mismatches in the telephone network at 2-to-4-wire analog-to-digital conversion points.

Recommended actions:

1. Determine the source of the echo. Test the speech back to the far-end by muting the near-end phone. If the far-end no longer complains of echo, this confirms the near-end is the source of the echo.
   - If the near-end is a speakerphone user, verify the environment setup.
   - If the near-end is a headset user, verify the amplifier settings and that the proper cords are used.
2. If the near-end is not the source of the echo, determine if the echo is on the phone or from the far-end. Take a trace on the IP phone while echo is heard.
   - If no echo is heard in the trace, the echo source is in the phone.
     a. Adjust the microphone input control.
     b. Activate the microphone Automatic Gain Control using the Audio Tuning Wizard.
     c. If the caller is still complaining that they are hearing an echo, the cause may be a poorly performing headset or soundcard. Decrease the amplification of the transmission by adjusting the Transmit Gain from the Audio Options menu. Note that adjusting the gain distorts the original signal, which may decrease the voice quality.
3. The echo source is either at the analog trunk or in the network. Terminate the trunk locally and test for echo. This will identify if the source of the echo is local or in the network.

After determining the source of the echo, determine the type of echo the user is experiencing and follow the troubleshooting steps.

Echo Source	See...
Analog Trunk - Constant echo	Constant Analog Trunk Echo
Analog Trunk - Intermittent echo	Echo Canceller Training Period
DS1 Trunk	DS1 Trunk Echo
Speakerphone	Speakerphones
Handset	Handset Echo
Headset/Headset Adapter	Headset Echo

Constant Analog Trunk Echo

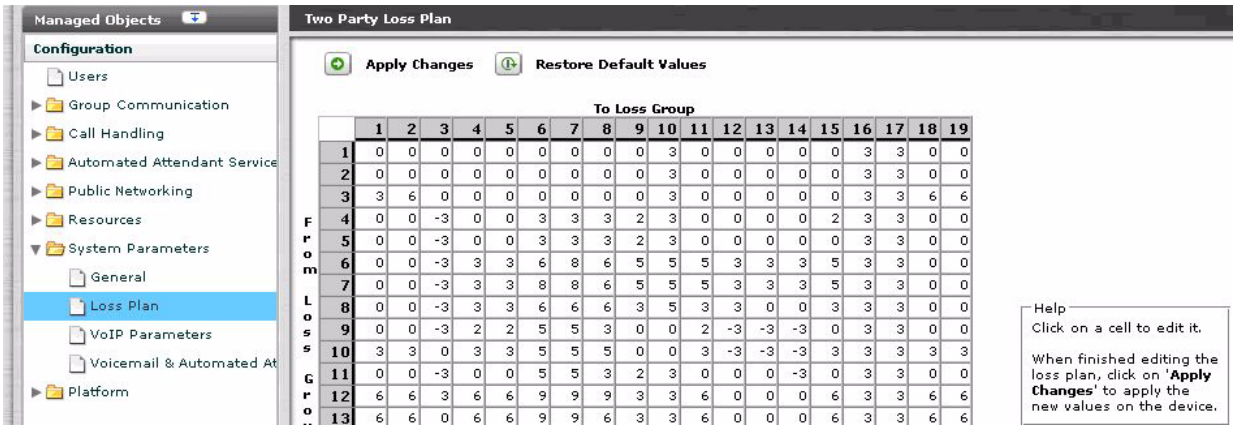
Constant echo on an analog trunk usually means the echo is beyond the specifications of the echo canceller. It can be too loud or too far away.

1. It is possible that the impedance choice of the analog trunk has been chosen incorrectly. To check the impedance of the analog trunk:
   a. Click on **Trunk Groups** under **Configuration > Public Networking** in the menu on the left side of the screen.
   b. Click on the trunk name to display information regarding the trunk
   c. Select the **Trunk Parameters** tab.
   d. Determine the best impedance choice (600 ohm vs. RC). Normally, RC is used for long loop lengths and 600 ohm for shorter loop lengths. If possible, create a new private trunk group so as not to subject the user to trial and error testing. Several calls to the same destination should be tried at each setting to get an overall reading. Note that by changing the impedance choice, you may experience temporary echo for the first call to a given trunk.
2. If problems persist, insert loss in 1 db increments until the problem is resolved. If the voice signal level coming in from the trunk is low, only introduce loss towards the analog trunk. If signal levels are balanced, insert loss in both directions. Typically, the loss group for analog trunks is 6. The loss group for inter-gateway or IP trunk connections is 18. IP phones use loss group 19. Therefor, loss should be inserted between loss groups 6 and 18, and between loss groups 6 and 19.

   To insert a loss:

   a. In the Communication Manager Branch, go to **Configuration> System Parameters> Loss Plan**.

Figure 10: Loss Plan



b. Click on a cell.

c. Edit the loss.

d. Click **Apply Changes**.

CAUTION:

Changing the loss plan can have very serious consequences for the entire network. Avaya strongly recommends that only certified Avaya technicians adjust these parameters.

e. If you want to restore the default values, click **Restore Default Values**.

3. A noisy analog trunk may cause poor performance of an echo canceller. It the analog trunk is noisy, has crosstalk or other impairments, take whatever steps possible to reduce or eliminate the noise or impairment on the trunk.
4. If the problem still persists, see Far End Echo.

Echo Canceller Training Period

The echo canceller may be having difficulty training with a given echo source or change in echo source.

1. Try all of the steps under Constant Analog Trunk Echo to attempt to decrease the volume level of the echo. This alone may result in a significant improvement.
2. Turn off call classification if the feature is not being used. Call classification can affect trunk gain and cause an extended echo training period at the early portion of the call.

   To turn off the call classification:

   a. In the Communication Manager Branch, go to **Configuration> Resources**.

b. Select the trunk type.

c. Deselect **Echo Cancellation**.

3. If analog trunks are the echo source, use MM711 HW V21 FW V61 or greater if possible. This media module has an-board echo cancellers which may alleviate the problem.

DS1 Trunk Echo

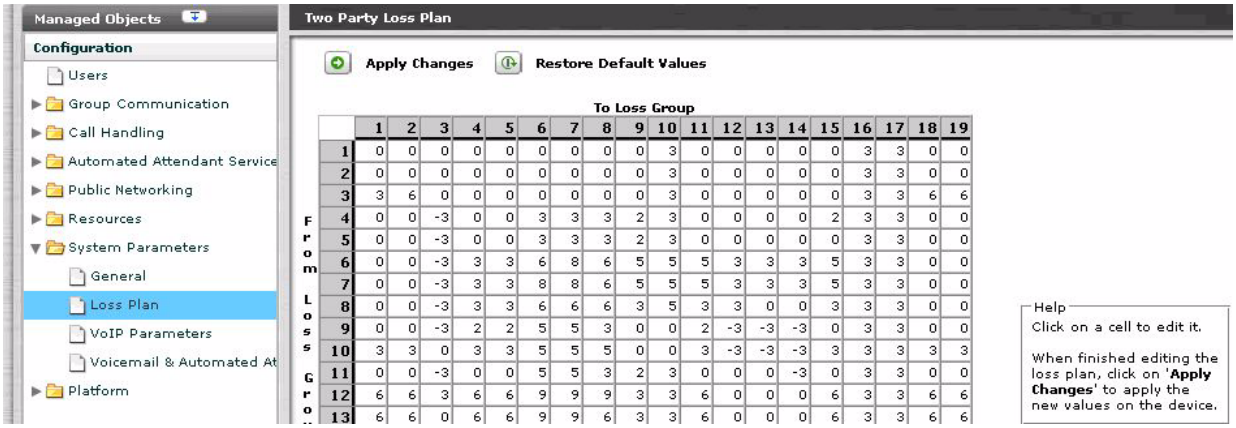
If the echo source is a DS1 trunk:

1. Verify that the DS1 echo canceller option has been turned ON. Select **DS-1** under **Configuration > Public Networking** and click on the name of the trunk. Make sure that the **Echo Cancellation** box is checked.
2. If the DS1 media module does not have an echo canceller, try upgrading to one that does and make sure that Echo Cancellation is enabled on the trunk form. See Echo Cancellation Levels for the description of the Echo Cancellation levels.
3. If possible, upgrade to the media module with the largest tail support.
4. Insert loss in 1 db increments in both directions until the problem has been resolved. The loss should be inserted between the loss group associated with the DS1 trunk and loss group 18 (IP trunks or inter-gateway), and also between the loss group associated with the DS1 trunk and loss group 19 (IP phones).

   To insert a loss:

   a. In the Communication Manager Branch, go to **Configuration> System Parameters> Loss Plan**.

Figure 11: Loss Plan



b. Click on a cell.

c. Edit the loss.

d. Click **Apply Changes**.

CAUTION:

Changing the loss plan can have very serious consequences for the entire network. Avaya strongly recommends that only certified Avaya technicians adjust these parameters.

e. If you want to restore the default values, click **Restore Default Values**.

5. If the problem still persists, the echo may be too far away for the echo canceller to handle. See Far End Echo.

Speakerphones

The actual user of the problematic speakerphone will not be the one reporting the echo. The echo will be reported by those on the other end of the call. The user of the speakerphone may not be aware of the problem.

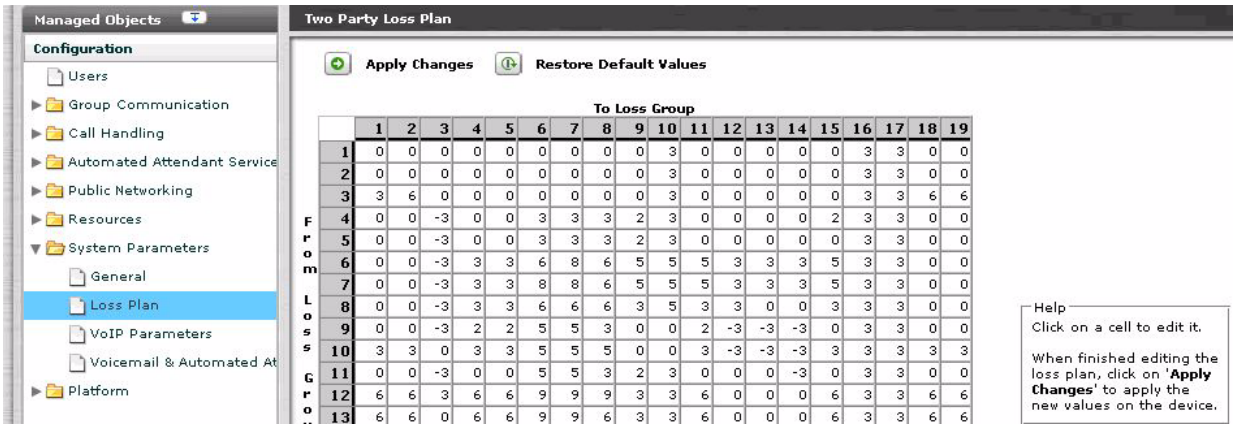
If the source of the echo has been determined to be a speakerphone:

1. If the phone causing the echo is an IP phone, upgrade it to the latest IP firmware. The IP phone itself is responsible for controlling its own echo.
2. If the problem persists, insert loss in both directions until the problem is resolved. The loss should be inserted between loss groups 2 and 19 for IP phones.

   To insert a loss:

   a. In the Communication Manager Branch, go to **Configuration> System Parameters> Loss Plan**.

Figure 12: Loss Plan



b. Click on a cell.

c. Edit the loss.

d. Click **Apply Changes**.

CAUTION:

Changing the loss plan can have very serious consequences for the entire network. Avaya strongly recommends that only certified Avaya technicians adjust these parameters.

3. If you want to restore the default values, click **Restore Default Values**.
4. For some speakerphone models, turning down the volume control of the speakerphone may cause some improvement.

Handset Echo

The actual user of the problematic handset will not be the one reporting the echo. It will be reported by those on the other end of the call. The user of the handset may not be aware of the echo.

Handset echo is usually a low-level acoustic echo caused by the direct coupling of handset speaker to handset microphone. It will be most noticeable when the phone listen volume level is set rather high on the end causing the echo.

1. If the phone causing the echo is an IP phone, upgrade to the latest IP phone firmware. The IP phone itself is responsible for controlling its own echo.
2. If possible, ask the user of the problematic handset to lower the telephone listen volume level.

Headset Echo

The actual user of the problematic headset will not be the one reporting the echo. It will be reported by those on the other end of the call. The user of the headset may not be aware of the echo.

Headset echo can be acoustic or electrical echo. In most cases, it will probably be a low-level echo and usually can be controlled.

1. If the headset causing the echo is connected to an IP phone, upgrade to the latest IP phone firmware. The IP phone itself is responsible for controlling its own echo.
2. Make sure the headset is on the list of approved IP telephones.
3. Ask the user of the problematic headset to lower the telephone listen volume level.
4. If the echo is caused by the Avaya M12 headset adaptor in handset mode, install the special patch cord provided by the manufacturer. The Avaya M12 headset, when on handset mode, can cause a very extreme loud echo when the phone listen volume is set high.

Far End Echo

Persistent echo can be caused if the echo is so far away that it exceeds the window size of the echo canceller. If possible, have the user write down the phone number being used for the call to determine where the destination is and if the problem is reproducible.

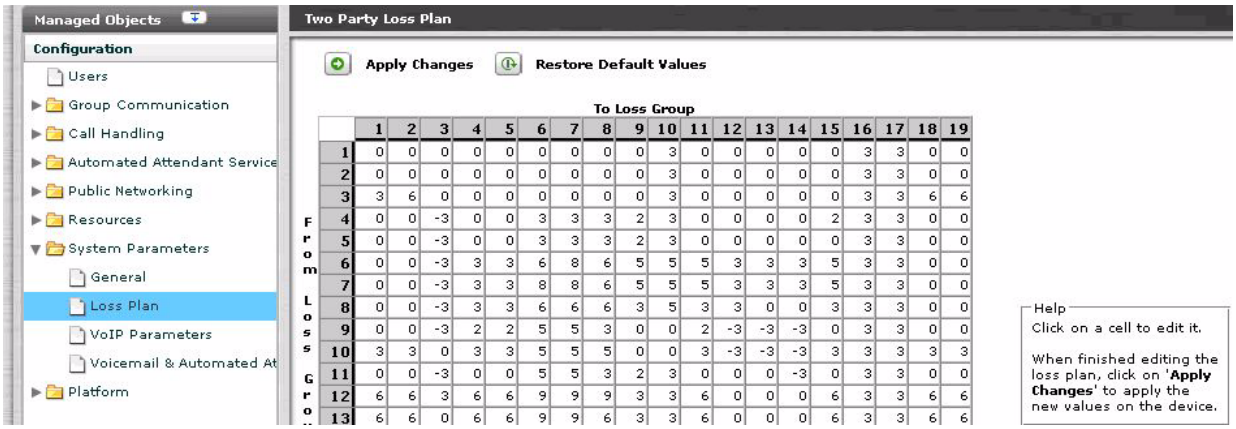
If the echo is indeed beyond the window of support for the echo canceller, the echo should occur on every call to that same phone and be persistent throughout the call for all calls to that number.

1. If a DS1 trunk is involved, upgrade to the latest media module with the largest tail support. Also make sure that the DS1 echo cancelling option has been turned on. Click on **DS-1** under **Configuration > Public Networking** in the menu on the left side of the screen. Click on the trunk name to display information regarding the trunk. Make sure the **Echo Cancellation** box is checked.
2. If the echo source is an analog trunk, try to have the customer switch to a DS1 trunk.
3. Some improvement may occur by adding loss between the relevant loss groups.
   - For DS1 trunks, insert loss in 1 db increments in both directions until the problem has been resolved. The loss should be inserted between the loss group associated with the DS1 trunk and loss group 18 (IP trunks or inter-gateway), and also between the loss group associated with the DS1 trunk and loss group 19 (IP phones).
4. For analog trunks, insert loss in 1 db increments until the problem is resolved. If the voice signal level coming in from the trunk is low, only introduce loss towards the analog trunk. If signal levels are balanced, insert loss in both directions. Typically, the loss group for analog trunks is 6. The loss group for inter-gateway or IP trunk connections is 18. IP phones use loss group 19. Therefor, loss should be inserted between loss groups 6 and 18, and between loss groups 6 and 19.

   To insert a loss:

   a. In the Communication Manager Branch, go to **Configuration> System Parameters> Loss Plan**.

Figure 13: Loss Plan



From \ To	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	3	3	0	0
2	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	3	3	0	0
3	3	6	0	0	0	0	0	0	0	3	0	0	0	0	0	3	3	6	6
4	0	0	-3	0	0	3	3	3	2	3	0	0	0	0	2	3	3	0	0
5	0	0	-3	0	0	3	3	3	2	3	0	0	0	0	0	3	3	0	0
6	0	0	-3	3	3	6	8	6	5	5	5	3	3	3	5	3	3	0	0
7	0	0	-3	3	3	8	8	6	5	5	5	3	3	3	5	3	3	0	0
8	0	0	-3	3	3	6	6	6	3	5	3	3	0	0	3	3	3	0	0
9	0	0	-3	2	2	5	5	3	0	0	2	-3	-3	-3	0	3	3	0	0
10	3	3	0	3	3	5	5	5	0	0	3	-3	-3	-3	3	3	3	3	3
11	0	0	-3	0	0	5	5	3	2	3	0	0	0	-3	0	3	3	0	0
12	6	6	3	6	6	9	9	9	3	3	6	0	0	0	6	3	3	6	6
13	6	6	0	6	6	9	9	6	3	3	6	0	0	0	6	3	3	6	6

b. Click on a cell.

c. Edit the loss.

d. Click **Apply Changes**.

CAUTION:

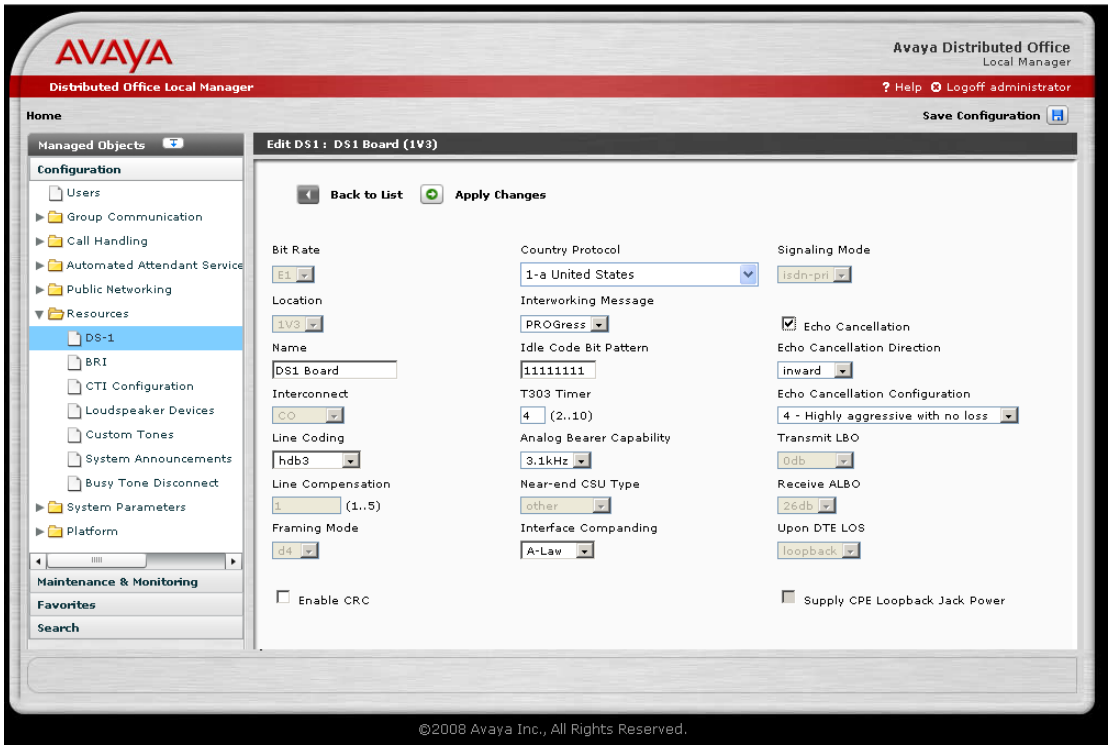
Changing the loss plan can have very serious consequences for the entire network. Avaya strongly recommends that only certified Avaya technicians adjust these parameters.

e. If you want to restore the default values, click **Restore Default Values**.

5. Report the problem to the telephone service provider. There may be a problem with the echo canceller equipment.
6. If the problem still persists, an external echo canceller may be necessary, or the customer can switch to a more reliable long distance provider.

Echo Cancellation Levels

The echo cancellation level can be determined by clicking **DS-1** under **Configuration > Public Networking** in the menu on the left side of the screen. Click on the trunk name to display information regarding the trunk.



The levels and their meanings are:

1. Highly aggressive with 6db loss
2. Aggressive and stable
3. Aggressive and very stable
4. Highly aggressive with no loss
5. Very moderate and very stable

The levels will appear only if the **Echo Cancellation** box is checked.

Trunk or Outside Line Problems

Use this chapter to help identify and fix trunk or outside lines problems.

Important:
Digital Central Office (CO) loop-start trunks and loop-start outside line groups are not supported on Distributed Office R1.1. Digital CO ground-start trunks and ground-start outside line groups are supported.

Status screens and available functions for outside lines and trunks

Displaying the status of a trunk or an outside line is the first step in troubleshooting. You can display the status of a trunk group or outside line by clicking **Trunk Groups** or **Outside Line Groups** under Maintenance and Monitoring > Telephony. The **Trunk Group Status** screen or the **Outside Line Group Status** screen appears providing information such as trunk type, number of members, number of members in use, number of members in service, and D-Channel state (if used).

From the **Outside Line Group Status** screen and the **Trunk Group Status** screen the following functions can be performed against a group or a trunk member:

- Busy: When you busy a trunk or outside line, it is removed from service. Use this function to block user access when a trunk or outside line is not functioning properly. For more information on how to busy a trunk or outside line, see Busy a group or a group member using Branch Device Manager on page 64.
- Release busy: Once the problem has been corrected, you can release the busy and allow user access. For more information on how to release a busy, see Release the busy of a trunk or outside line group using Branch Device Manager on page 65.
- Test: The number and types of tests that are executed against a trunk or outside line varies on the trunk or line type. If a test fails an error displays. The error can be used as an aid in identifying the trouble. For more information on how to test a trunk or outside line, see Testing a trunk group using Branch Device Manager on page 63.
- Get Hourly Statistics: The Trunk Group Hourly Statistics screen displays information such as total usage, maintenance usage, total seizes, etc. Use this information to regulate traffic and to identify problems.

Basic trunks or outside line troubleshooting guidelines

Use the following steps as a basic guideline to troubleshoot problems on an Communication Manager Branch trunk or outside line:

1. In the **Status** field of the **System Summary** screen, verify if there is an active alarm on the system. To display the **System Summary** screen, click **System Summary** under Maintenance and Monitoring.
2. If there is an active alarm on the system, use the **Display Active Alarms** screen to view the detailed alarm information. The Display Active Alarms screen can be found by clicking **Alarms** under Maintenance and Monitoring. For more information on Communication Manager Branch alarms, see Alarms.
3. If a trunk or outside line is alarming:
   a. Check the status of the alarming trunk or outside line in the **Trunk Group Status** screen or **Outside Line Status** screen by clicking **Trunk Groups** or **Outside Line Groups** under Maintenance and Monitoring > Telephony.

      For a trunk group, you can drill down to an individual trunk member by clicking on any column of data associated with the trunk or outside line. The state of each member displays on the **Trunk Member Status** screen.

   b. On the **Trunk Member Status** screen or the **Outside Line Groups screen**, select the trunk member or the line group that is alarming by clicking the associated box. Click **Test Selected**. A number of tests are executed. The results of the tests are displayed on the screen.

      For more information on testing a trunk, see Testing a trunk group using Branch Device Manager on page 63.

      For more information on testing an outside line group, see Testing a outside line using Branch Device Manager on page 63

      For more information on the tests that run and possible resolutions, see Maintenance Tests on page 139.
4. To test the media module associated with the alarming trunk:
   a. Click **General** under Maintenance and Monitoring > Telephony > Media Services. The **Media Services Status** screen appears.
   b. Check the box associated with the media module and then click **Test Selected**. The **Test Operation Results** screen appears.

      For more information on the tests that run and possible resolutions, see Maintenance Tests on page 139.

Testing a trunk group using Branch Device Manager

Testing a trunk group can identify a problem and can provide a resolution. All tests are done using Branch Device Manager.

Use the following steps to run a test:

1. Click **Trunk Groups** under Maintenance and Monitoring > Telephony.

   The **Trunk Group Status** screen appears.

2. Tests can be run on all the members in a group or an individual member in a group:

   - To test all the members:

     a. Click the selection box associated with the group and then click **Test Selected** from the top of the screen.

   - To test individual members:

     a. Click any column of information associated with the group.

        The **Trunk Member Status** screen appears.

     b. Select the group member by clicking the associated box.

     c. Click **Test Selected** from the top of the screen.

   A **Test Operation Results** screen appears. The Test Operation Results screen contains the name of the tests, the results of the test, error codes, and detailed information.

   For more information on the fields for the Test Operation Results screen, see the Branch Device Manager online help.

   For more information on the test, the error codes, and the possible resolutions, see Maintenance Tests on page 139.

Testing a outside line using Branch Device Manager

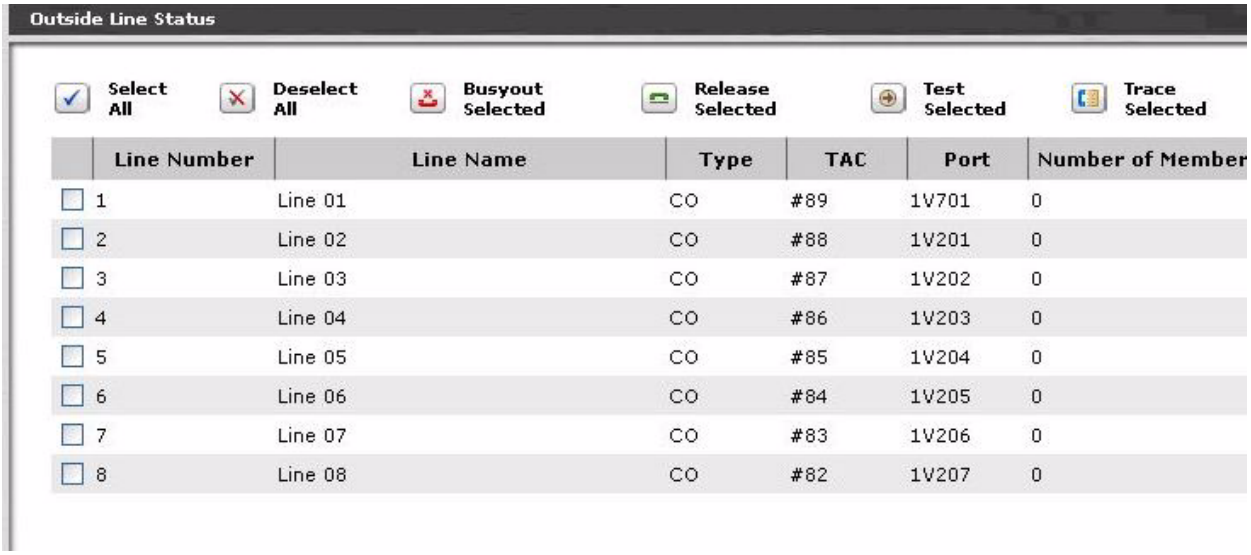
Testing an outside line can identify the problem and can provide a resolution. All tests are done using Branch Device Manager.

Use the following steps to run a test:

1. Click **Outside Line Groups** under Maintenance and Monitoring > Telephony.

   The **Trunk Line Status** screen appears as shown in example Figure 14.

Figure 14: Outside Line Status screen



The Trunk Line Status screen displays the administered outside lines, the line type, the port, and the number of stations on which the line appears (Number of Members field).

2. To test the outside line: Click the selection box associated with the group then click **Test Selected** from the top of the screen.

   A **Test Operation Results** screen appears. The Test Operation Results screen contains the name of the tests, the results of the test, error codes, and detailed information.

   For more information on the fields for the Test Operation Results screen, see the Branch Device Manager online help.

   For more information on the tests that run, the error codes, and the possible resolutions, see Maintenance Tests on page 139.

Busy a group or a group member using Branch Device Manager

If testing indicates that a group or a group member is not working properly, you can busy it using Branch Device Manager. Once busied, the group or group member will be unavailable to users.

Use the following steps to busy a trunk or an outside line:

1. Click **Trunk Groups** or **Outside Line Groups** under Maintenance and Monitoring > Telephony.

   The **Trunk Group Status** or **Outside Line Group Status** screen appears.

2. You can busy a trunk, an outside line group, or an individual member within a trunk group:
   - To busy a trunk or outside line group:
     a. Select the trunk or outside line group.
     b. Check the box associated with the group and click **Busyout Selected** from the top of the screen.

     The trunk is now out of service.
   - To busy an individual trunk member:
     a. In the **Trunk Group Status** screen, click any column of information associated with the trunk group.

        The **Trunk Member Status** screen opens.
     b. Check the box associated with the member.
     c. Click **Busyout Selected** from the top of the screen.

   A **Maintenance Operation Results** screen appears with the status of the group or group member.

   For more information on the **Trunk Groups** screen or **Outside Line Groups** screen, see the Branch Device Manager online help.

Release the busy of a trunk or outside line group using Branch Device Manager

Once the problem has been corrected on the trunk or the outside line group, you can release the busy to allow user access.

Use the following steps to release the busy of a trunk or an outside line group:

1. Click **Trunk Groups** or **Outside Line Groups** under Maintenance and Monitoring > Telephony.

   The **Trunk Group Status** or **Outside Line Group Status** screen appears.
2. You can release the busy for a trunk, an outside line group, or individual members in a trunk group:
   - To release the busy for a trunk or an outside line group:
     a. Check the box associated with the group then click **Release Checked** from the top of the screen.
   - To release the busy on an individual trunk member:

a. In the **Trunk Group Status** screen, click any column of information associated with the trunk group.

   The **Trunk Member Status** screen appears.

b. Check the box associated with the busied trunk member.

c. Click **Release Checked** from the top of the screen.

A **Maintenance Operation Results** screen appears with the status of the group or group member.

For more information on the **Trunk Groups** screen or **Outside Line Groups** screen, see the Branch Device Manager online help.

Manually testing a trunk group or outside line group

If you have a problem with a trunk, trunk group, outside line, or outside line group, you can test it manually using a station on the Communication Manager Branch system. Your station must have privileges that enable you to run a test and you must know the facility test call access code.

Note:

You cannot manually test an ISDN trunk using this procedure.

The facility test call access code allows you to select an individual trunk, trunk group, outside line, or outside line group. If the trunk or line is busied by maintenance, it will be temporarily released for the test call and then returned to a busied state after the test completes.

Note:

If the status of the trunk or outside line displays out-of-service and you receive a busy-tone when performing a manual test, contact your provider for assistance.

Note:

If you hear silence instead of dial-tone when performing a manual test, contact your provider for assistance.

Use the following steps to perform a facility test call:

1. To verify that you have privileges to run a facility test:
   - On the Branch Device Manager interface, click **Users** under Configuration.
   - Click on any line of data associated with the station that will be used for the call. The **Edit User** screen appears.
   - Verify the administration of the **Privilege** field. The user of the extension must have a privilege of administrator (Admin), High, or Medium to execute the facility test.
2. To obtain the facility test call access code:

a. On the Branch Device Manager interface, click **Feature Access Codes** under the **Configuration** heading.

b. Scroll down until you find **Facility Test Calls Activate** and record the associated code.

3. To place a test call:

   a. Dial the facility test access code (FAC).

   b. Dial the 7-digit port location MMMVSyy where:

      - MMM = For Communication Manager Branch the Media Gateway number is 001.
      - V = Gateway port identifier carrier = 8. On a telephone keypad, the number ’8’ also displays letters ’T’, ’U’, and ’V’.
      - S = Slot number
      - yy = Circuit number

      Circuit range depends on the media module on which the trunk is administered. For Media Module 711, the range is 1-8; for the Avaya T1/E1 Media Module 710, the range could be 1-23, 1-24, or 1-31, depending on the type of translation and signaling.

      For example, 001V301 would be used to test a trunk connected to slot three on circuit one.

4. Listen for one of the following tones:

   - Dial tone or silence: The trunk is connected. Go to step 5.

   Note:

   The dial tone heard is coming from the far-end. If the far-end is disabled, you will not hear dial tone. However, depending on the far-end administration, you may still be able to dial digits. Every digit dialed after the port number is transmitted using end-to-end DTMF signaling.

   - Busy tone: The trunk is either busy processing a call or is out of service.
   - Reorder tone: You cannot access the trunk.
   - Intercept tone: The port is either not a trunk, is not administered, or is a DID trunk.
   - Confirmation tone: The port is a tone receiver.

5. Place the call. If the call does not go through where ringing is heard, check the trunk administration.

I hear a busy tone when I try to access a line appearance on a local Communication Manager Branch

It can take several seconds for a trunk to release from a previous call. If someone just hung-up from a line appearance and you accessed that appearance before the line is released, you will hear a busy tone. Hang up from the line appearance and wait for a couple of seconds, then try the line appearance again.

Voice Mail

Branch Device Manager provides the following screens for status and troubleshooting of Communication Manager Branch voice mail:

- General: The **Voicemail General Report** screen displays information on voice mail usage, outcalls, and mailbox storage.
- Mailboxes: The **Mailbox Usage Report** screen displays usage information for each mailbox.
- System language files: The **System Language Files** screen displays the languages used for recorded messages on the system.

For more information on the Branch Device Manager voice mail screens, see the online help for Branch Device Manager.

Verifying voice mail administration

When troubleshooting or testing voice mail, it is important to understand how the voice mail was administered. It is possible that voice mail was administered incorrectly or that a voice mail feature was not turned on.

Local site voice mail administration

Verify the administration information in this section if you have a voice mail issue that affects all the users in a local Communication Manager Branch site:

- Cannot retrieve voice mail messages: In the Branch Device Manager interface, click **Service Numbers** under Configuration. Voice mail appears in the list of features under the Use heading. The number that you dial to access the voice mailbox displays under the **Extension** heading.
- The wrong system language is being used: The language for voice mail is defined in the **Voicemail and Automated Attendant System Parameters** screen. To access this screen, click **Voicemail and Automated Attendant** under the System Parameters heading.

Single user administration

Verify the administration information in this section if a single user is having voice mail problems:

1. In the Branch Device Manager interface, click **Users** under Configuration.

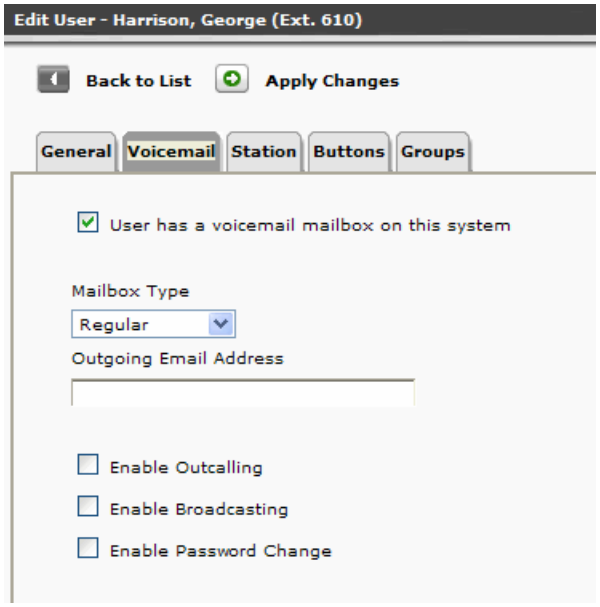
   The **User** screen appears.

2. To view the administration of a user, click any column of data associated with the user.

   The **Edit User** screen appears.

3. Click the **Voicemail** tab. The Voicemail screen appears as shown in example Figure 15.

Figure 15: Edit User screen - Voicemail tab

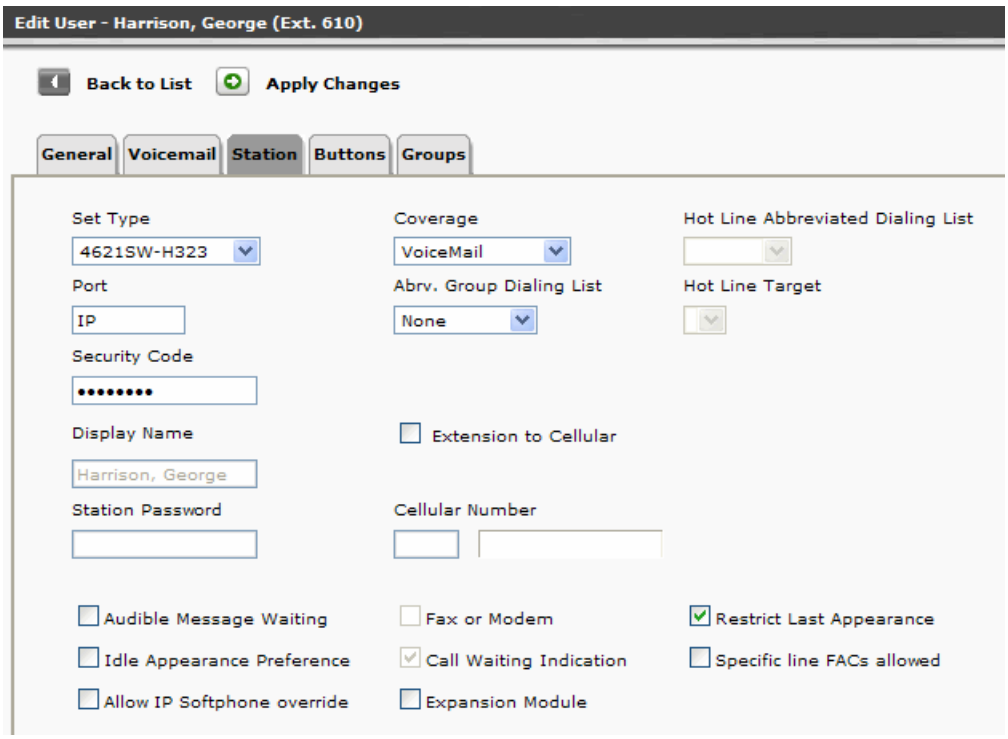


- Verify that there is a check in the **User has a voicemail on this system** field.
- In the **Mailbox Type** field, verify the type of mailbox that was administered. A mailbox can be one of the following types:
  - Regular: A regular mailbox has 20 minutes of storage and two personal greetings. The maximum length for a single message is two minutes.
  - Extended: An extended mailbox has 40 minutes of storage and two personal greetings. The maximum length for a single message is two minutes.
  - Informational: An informational mailbox plays an announcement to the caller but does not record a message.

- Verify the user permissions. A user can have one or more of the following permissions:
  - Enable Outcalling: When this field is set, a user can receive a call from the system when new voice mail is received. Outcalling is not a feature for fax, receipt response, and broadcast messages. Once Outcalling is administered, the user calls into voice mail to activate the feature and set the number that the system dials using the keypad on their telephone.
  - Enable Broadcasting: This feature enables the user to broadcast a message to all the mailboxes in the system.
  - Enable Password Change: This feature enables the user to change the password for the user's voice mail.

4. Click the Station tab. The Station screen appears as shown in example Figure 16.

Figure 16: Edit User - Station tab



- In the Station tab, verify that:
- VoiceMail appears in the **Coverage** field: If VoiceMail does not appear, unanswered calls to this user will not cover to voice mail.
- Audible Message Waiting is selected: This is an option only and is not necessary to make the voice mail function. If this option is selected the user receives a stutter dial tone indicating they have messages waiting in the mailbox when the user goes off-hook.

System mailbox capacity

The number of voice mailboxes can be configured; there is no maximum number.

Verify mailbox capacity

All mailbox types can exceed their capacity. Both the owner of the mailbox and a person calling to leave a message receives an audible message indicating that the mailbox is full:

- The caller receives the message "Sorry, you cannot leave a message because this mailbox is full."
- The owner receives the message, "Your mailbox is full. Please delete unneeded messages."

To check voice mailbox usage: On Branch Device Manager, click **Mailboxes** under Maintenance and Monitoring > Telephony > Voicemail and Automated Attendant. The **Mailbox Usage Report** displays. Using the Mailbox Usage Report you can see how many voice messages, fax messages, and total messages are in the mailbox. You can also verify how much space is being used.

The Mailbox Usage Report also displays zombies. A zombie is created when the owner of the mailbox is deleted but the mailbox was left administered. While a zombie does not count against the maximum number of mailboxes allowed on a system, it does take up space and should be removed. If a zombie is left administered and a new user is assigned the old extension number associated with the zombie, the new user will have access to all the messages, the greetings, and the voice signatures there were recorded for the previous user.

For more information on the **Mailbox Usage Report**, see the online help for Branch Device Manager.

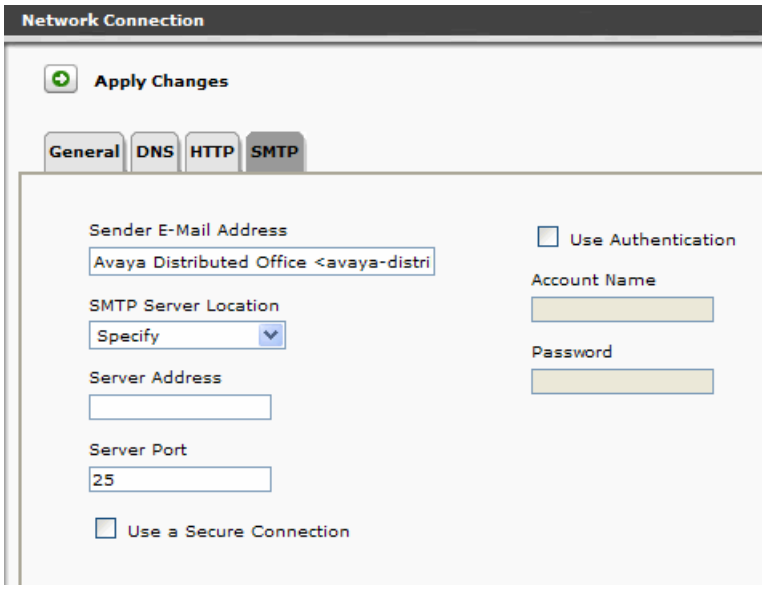
Voice mail fax

Voice mail can be used to receive fax messages. The fax message is sent to the users email address and a copy is stored on the voice mail system. The copy of the fax remains on the system until the user deletes it. The maximum size of a fax message is 1MB which equates to approximately 25 pages. Currently, there is no capability to send a fax using voice mail.

Voice mail administration must be correct to receive a fax. If you are experiencing problems check the following administration:

- Click **Network Connection** under Configuration > Platform. Click the SMTP tab.

Figure 17: Network Connection SMTP tab



The fields on the SMTP tab must be correct or voice mail fax will not work. If DNS is not used, the SMTP server's IP address must be entered. If authentication is used, you must enter the account name and password. If this is a secure connection, a certificate must be defined.

- On the Voicemail tab of the User's station form, verify that the user's email address is entered in the **Outgoing Email Address** field. A fax message is delivered to the user's email address and stored in the user's mailbox. If for some reason the user did not receive the email fax message the user can call into the mailbox and request a re-delivery of the fax email message.
- Check the capacity of the mailbox (see Verify mailbox capacity on page 72) to verify the user has enough space to store a fax message.
- If the wrong Caller Station Identification (CSID) is used when receiving a fax transmission: The parameters for CSID are defined in the **Voicemail and Automated Attendant System Parameters** screen. To access this screen, click **Voicemail and Automated Attendant** under the System Parameters heading.

Testing voice mail

Use the following steps to verify that voice mail is working properly:

1. If the user is administered correctly, call the extension of the user and verify that you receive a voice mail message.

2. Leave a message for the extension.
3. Verify that the message light comes on.

   If the message light does not go out after you delete the message it could be an indication that the message light is controlled by the auto attendant application. This could be the case when the station user is the owner of an auto attendant mailbox. To verify if the user is the owner of an auto attendant mailbox:

   a. Click **Automated Attendants** under the Automated Attendant Services heading on Branch Device Manager.
   b. Select the auto attendant by clicking on the name.
   c. Verify the number assigned to the **Message Waiting Indicator** field.
4. Listen to the voice mail message. Verify that the light goes out after you listen.
5. Delete the message.

If voice mail is administered correctly but is still not working, call the system administrator or your support organization for help.

Auto Attendant

This chapter contains information on troubleshooting auto attendant using Branch Device Manager.

The station’s message indicator does not light

A auto attendant can be assigned an owner. The station’s message waiting indicator of the owner lights when a message arrives in the auto attendant mailbox. To verify the owner of the auto attendant:

1. Click **Automated Attendants** in the Branch Device Manager interface.
2. Click on the name of the auto attendant.
3. Verify the extension in the **Message Waiting Indicator** field.

The station’s message indicator does not go out

A station’s message waiting indicator can be used for both auto attendant and voice mail. If the message waiting indicator is still on after all the auto attendant messages have been retrieved, check your voice mailbox for messages.

Out-of-hours greeting during working hours

The fixed schedule for auto attendant defaults to closed. Verify that the **Open** or **Closed** column is set to Open. To verify the setting:

1. Click **Automated Attendants** in the Branch Device Manager interface.
2. Click the name of the auto attendant.
3. Click the Fixed Schedule tab.
4. Verify that Open displays in the days of the week in which you want the auto attendant to answer. If you make any changes to this screen, click **Apply Changes**.

5. Click **Save Configuration** to permanently save the change. Save Configuration can be found on the right side near the top of the screen.

If all the settings are correct, check the Temporary Schedule tab. An ’On’ status for any day of the week in the Temporary Schedule overwrites the same day in the Fixed Schedule. Verify that the **Status** column and change the status to ’Off’ for days that should follow the Fixed Schedule. If you make any changes to this screen, click **Apply Changes**.

The selector code sends calls to the wrong place

This is an administration problem. To verify the administration:

1. Click **Automated Attendants** in the Branch Device Manager interface.
2. Click the name of the auto attendant.
3. Click the **Day Menu** tab. Find the selector code having the problem. Verify the action in the **Action** column associated with the selector code. If this is not the action you wanted, select the correct action from the drop-down menu. If this action transfers the call to an extension, verify the extension.

Voice Messaging System announcement on auto attendant

Communication Manager Branch provides a default auto attendant menu with a recording welcoming you to the Voice Messaging System. The default menu plays when you do not specify any records for the auto attendant.

Maximum length for a recorded message and an announcement

A recorded message and an auto attendant announcement are limited to two minutes each.

Fax calls do not work on auto attendant

Auto attendant must be administered correctly to receive fax calls on auto attendant. Verify the following administration:

1. Click **Automated Attendant** under the Automated Attendant Services heading in Branch Device Manager.
2. Click the name of the auto attendant.
3. Check the **Fax Coverage** field in the General tab. The following options are provided for the Fax Coverage field:
   - Disabled: This option drops incoming fax calls as soon as the fax tone is detected.
   - Extension: This option transfers the fax to the extension provided in the **Fax Extension** field.
     - When the Extension option is selected, the Fax Extension field appears. Auto attendant transfers the fax calls to the extension that is entered in the Fax Extension field.
   - Email: This option transfers the fax call to the email address provided in the **Outgoing Email** field. A copy of the fax message is saved in the automated attendant's mailbox. This option does not work with an informational mailbox type.
     - When the Email option is selected, an **Outgoing Email** field appears. Auto attendant transfers the fax calls to the email address entered in the Outgoing Email field.

Note:

The SMTP tab in the Network Connection screen must be configured correctly for the Email option to work.

Modem and Fax Problems

This section describes how to troubleshoot problems associated with fax and modems.

Fax and modem transmissions provide users with the ability to receive or send fax or modem transmissions between devices on a single Communication Manager Branch Platform, between two branch locations, or through PSTN trunks. Faxing over IP (FoIP) between branches and to internal voice mail is supported in T.38 fax mode. Modem over IP (MoIP) between branch locations is supported in modem pass-through mode.

Troubleshooting Fax Problems

If a user is experiencing fax problems:

1. Make sure the **Fax** box is checked for the affected analog station (**Configuration > Users >** select affected user > **Station** tab). This provides some privacy from call waiting and other intrusion tones.
2. Make sure the data privacy feature is enabled under Feature Access codes, which effectively does the same thing as Step 1 for only one call. This feature is similar to the CO **Disable Call Waiting** service code.
3. Know the route the fax call is taking:
   - If the fax call is a PSTN call directly to a fax machine, it is less likely to have problems than if the call came from the core or another branch (IP trunks).
   - If the fax call is being saved to voice mail, it goes through a transcoding (analog to IP) locally at the Communication Manager Branch unit or earlier if arriving over a SIP trunk.
   - If modems are not used, check the box to disable Modem over IP mode.
4. In voice mail:
   - Check the email destination for forwarding the fax to the affected station.
   - Under **Configuration**, click on **Platform > Network Connection**, then click on the SMTP tab to check information which needs to be set correctly for forwarding faxes.
   - Make sure the correct options are set on the VoiceMail System Parameters form for receiving faxes from voice mail.
   - Check the mailbox usage to verify the user has enough space to store a fax message.
5. If there was a power outage, the fax call should resume normally after power has been restored.

Troubleshooting Modem Problems

If a user is experiencing modem problems:

1. Check if the modem is in use. A modem is used for dial-in maintenance and dial-out alarming. If a modem is being used to deliver alarms to Avaya and the modem is in use, then alarms cannot be delivered to Avaya.
2. If there was a power outage, the modem call should resume normally after power is restored.
3. Know the route the modem call is taking:
   - If the modem call is a PSTN call directly to another modem, it is less likely to have problems than if the call came in from the core or another branch using IP trunks.
4. Older or slower (< 9.6 Kbps) modems are not supported and may not work over IP trunks.

AE services

The **CTI Maintenance screen** in Branch Device Manager provides status and maintenance for CTI objects. To access the **CTI Maintenance** screen, select Managed Objects > Maintenance > CTI.

Use the **CTI Maintenance** screen for the following:

- Restart CTI services
- Verify the status for the CTI links and the switch. The status includes the amount of time the links are in service, message counts for the last half hour, and the number of associations.
- A table showing the CTI client connections. This data includes the CTI User name that was used to authenticate, the IP address of the client, and when the client session began.

For more information on troubleshooting application enablement, see *Installation, configuration, and Troubleshooting Guide for Avaya Aura™ Communication Manager Branch application enablement* (03-602030).

LED Status Indicators

LEDs are important status indicators during installation, maintenance, troubleshooting, and repair. LEDs are not suitable for conveying detailed diagnostic information. Further diagnosis or troubleshooting is required.

Component	LED Description
MM316	MM316 LAN Media Module LED Status Indicators
MM710	MM710 T1/E1 Media Module LED Status Indicators
MM711	Standard Media Module LED Status Indicators
MM716	Standard Media Module LED Status Indicators
MM720	MM720 BRI Media Module LED Status Indicators
i40 BRI	Communication Manager Branch i40 BRI LED Status
i40 DS1	Communication Manager Branch i40 DS1 LED Status
i140 A14	Communication Manager Branch i40 A14 LED Status
i120	Communication Manager Branch i120 Platform LED Status

Standard Media Module LED Status Indicators

Name	Color	Description
ALM	Red	This LED indicates a media module failure or media module mismatch. This LED is also turned ON when the media module is inserted and should turn OFF after the media module initializes.

Name	Color	Description
TST	Green	This LED is turned ON during power-up self-testing and maintenance testing.
ACT	Yellow	This LED is turned ON when one or more ports are in use on the media module.

MM316 LAN Media Module LED Status Indicators

The MM316 Media Module has the following LEDs:

- A red ALM LED
- 40 dual-colored (yellow/green) faceplate port LEDs, one for each port
- A yellow LED for the 100/1000 Base-T Ethernet Port (LED 51)

The blinking rate is proportional to the traffic rate. All LEDs are turned on during a reset.

Name	Color	Description
ALM	Red	OFF after initialization tests have successfully passed. ON when a problem has been detected. BLINKING indicates an administration mismatch.
Port LED	ON Green	Link is up, port is enabled, no traffic, PoE delivered
Port LED	ON Yellow	Link is up, port is enabled, no traffic, no PoE delivered
Port LED	BLINK Green	Ethernet traffic with PoE being delivered
Port LED	BLINK Yellow	Ethernet traffic without Poe being delivered
51	ON Yellow	Link is up, port is enabled, no traffic, no PoE delivered
51	BLINK Yellow	Ethernet traffic without PoE delivered

MM710 T1/E1 Media Module LED Status Indicators

The MM710 T1/E1 Media Module has 4 LEDs.

Name	Color	Description
ALM	Red	This LED indicates a media module failure, a media module mismatch, a loss of signal, or the D-channel is down. This LED is also turned ON when the media module is inserted and should turn OFF after the media module initializes.
TST	Green	This LED is turned ON during power-up self-testing and maintenance testing.
ACT	Yellow	This LED indicates that the clock is synchronized with a source, usually the Central Office. The LED blinks 2.8 seconds ON and 300 ms OFF. This is the most common condition. The opposite blinking of the yellow LED is 300 ms ON and 2.8 seconds OFF. This is an error condition, and indicates that the MM710 T1/E1 media module is not synchronized with a clock. An infrequent occurrence is a steady yellow ON. This indicates in-use activity, only when clock synchronization is set to local.
SIG	Green	This LED indicates the presence of a signal on the T1/E1 line.

Synchronization

The yellow ACT LED displays the synchronization status of the MM710 media module.

- If the yellow ACT LED is solidly ON or OFF, it has *not* been defined as a synchronization source. If it is ON, at least one is channel is active. If the facility is an ISDN facility, the D-Channel will count as an active channel and will cause the yellow ACT LED to be ON.
- When the MM710 is driving a clock sync source line to the main clock, the yellow ACT LED does not indicate port activity but instead indicates that the MM710 is the sync source by flashing with a regular 3-second sequence:
  - If it has been specified as a sync source and is receiving a signal that meets minimum requirements for the interface, then the yellow ACT LED will flash ON for 2.8 seconds and will be OFF for 300 ms.
  - If it has been specified as a sync source and is not receiving a signal, or is receiving a signal that does not meet minimum requirements for the interface, then the yellow ACT LED will be OFF for 2.8 seconds and will flash ON for 300 ms.

T1/E1 initialization

The T1/E1 media module LEDs behave in the following manner during initialization. A visual indication of the media module's status is provided through the three faceplate LEDs:

- The yellow ACT LED is OFF while the red ALM and green TST LEDs are ON during the entire initialization sequence.
- If only the red ALM LED comes ON during power up or reset, either the media module processor is dead or the media module is being held permanently in reset.
- The green TST LED turns OFF upon completion of the diagnostic and initialization sequences.
- If the initialization tests fail, the red ALM LED remains ON.
- If the tests all pass, all LEDs are turned OFF until Communication Manager Branch starts using the media module.

MM720 BRI Media Module LED Status Indicators

Name	Color	Description
ALM	Red	This LED indicates a media module failure, a media module mismatch, or the B-Channel is down. This LED is also turned ON when the media module is inserted and should turn OFF after the media module initializes.
TST	Green	This LED is turned ON during power-up self-testing and maintenance testing.
ACT	Yellow	This LED is turned ON when one or more ports are in use on the media module.

Communication Manager Branch i40 BRI LED Status

Location	LED	Name	Color	Description
V3	ETR	Emergency Transfer	Green	ON when Emergency Transfer is activated
V3	ALM	Alarm	Red	This LED indicates a failure.
V3	TST	Test	Green	This LED is turned ON during power-up self-testing and maintenance testing.
V3	ACT	Activity	Yellow	This LED is turned ON when one or more ports are in use.

Location	LED	Name	Color	Description
System	MDM	Modem	Green	This LED turns ON when the modem is ready. It is OFF during shutdown, when a USB modem not plugged in, or when the modem is not responding or not functional.
System	ALM	Alarm	Red	An alarm is present in the system.
System	CPU	CPU	Green	OFF - A test is in progress. ON - Normal operation
System	PWR	Power	Green	OFF - No power BLINKING - Problem with power ON - Normal operation
	Ethernet Ports	Link State	Green	ON - Link is UP
	Ethernet Ports	Activity	Yellow	ON/Blinking - Traffic Activity

Communication Manager Branch i40 DS1 LED Status

Location	LED	Name	Color	Description
V3	ETR	Emergency Transfer	Green	Emergency Transfer has been activated.
V3	ALM	Alarm	Red	This LED is turned ON when a failure has been detected.
V3	TST	Testing	Green	This LED is turned ON during power-up self-testing and maintenance testing.
V3	ACT	Activity	Yellow	This LED is turned ON when one or more ports are in use on the media module.

1 of 2

Location	LED	Name	Color	Description
V4	ALM	Alarm	Red	Indicates a DS1 failure.
V4	TST	Test	Green	This LED is turned ON during power-up self-testing and maintenance testing.
	Ethernet Ports	Link State	Green	ON - Link is UP
	Ethernet Ports	Activity	Yellow	ON/Blinking indicates Traffic Activity
V4	ACT	Activity	Yellow	This LED indicates that the clock is synchronized with a source, usually the Central Office. The LED is blinking 2.8 seconds ON and 300 ms OFF. This is the most common condition. The opposite blinking of the YELLOW LED is 300 ms ON and 2.8 seconds OFF. This is an error condition and indicates that the MM710 E1/T1 media module is not synchronized with a clock. An infrequent occurrence is a steady YELLOW ON. This indicates in-use activity, only when clock synchronization is set to local.
V4	SIG	Signal	Green	This LED indicates the presence of a signal on the T1/E1 line.
System	MDM	Modem	Green	This LED turns ON when the modem is ready. It is OFF during shutdown, when the USB modem not plugged in, or when the modem is not responding or not functional.
System	ALM	Alarm	Red	An alarm is present in the system.
System	CPU	CPU	Green	OFF - A test is in progress. ON - Normal operation
System	PWR	Power	Green	OFF - No power BLINKING - Problem with power ON - Normal operation

2 of 2

Communication Manager Branch i40 A14 LED Status

Location	LED	Name	Color	Description
V3	ETR	Emergency Transfer	Green	Indicates that Emergency Transfer has been activated.
V3	ALM	Alarm	Red	Indicates a trunk failure when it is turned ON.
V3	TST	Testing	Green	This LED is turned ON during trunk power-up self-testing and maintenance testing of a trunk.
V3	ACT	Activity	Yellow	This LED is turned ON when one or more ports are in use on a trunk.
System	MDM		Green	This LED turns ON when the modem is ready. It is OFF during shutdown, when a USB modem not plugged in, or when the modem is not responding or not functional.
System	ALM	Alarm	Red	An alarm is present in the system.
System	CPU	CPU	Green	OFF - A test is in progress. ON - Normal operation
System	PWR	Power	Green	OFF - No power BLINKING - Problem with power ON - Normal operation
	Ethernet Ports	Link State	Green	ON - Link is UP
	Ethernet Ports	Activity	Yellow	ON/Blinking - Traffic Activity

Communication Manager Branch i120 Platform LED Status

The Communication Manager Branch i120 Platform supports the following Media Modules:

- MM314 (24 10/100 POE)
- MM316 (40 10/100 PoE)
- MM710 (T1/E1 ISDN PRI)
- MM711 (8 Port Analog)
- MM714B (8 Port Analog)
- MM716 (24 Line Analog)
- MM717 (24 DCP Ports)
- MM720 (8 ISDN BRI)
- MM722 (2 ISDN BRI)

Use the services port on the Communication Manager Branch to connect a laptop and configure the platform.

Location	Name	Color	Description
V7	ETR	Green	Emergency Transfer has been activated.
V7	ALM	Red	This LED indicates a media module failure or mismatch when it is turned ON. This LED is also turned ON when the media module is inserted and should turn OFF after it initializes.
V7	TST	Green	ON during power-up self-testing and maintenance testing.
V7	ACT	Yellow	ON when one or more ports are in use.
			1 of 2

Location	Name	Color	Description
System	MDM	Green	This LED turns ON when the modem is ready. It is OFF during shutdown, when the USB modem not plugged in, or when the modem is not responding or not functional.
System	ALM	Red	An alarm is present in the system.
System	CPU	Green	OFF - A test is in progress. ON - Normal operation
System	PWR	Green	OFF - No power BLINKING - Problem with power ON - Normal operation
Ethernet Ports	Link State	Green	ON - Link is UP
Ethernet Ports	Activity	Yellow	ON/Blinking - Traffic Activity
			2 of 2

Communication Manager Branch i120 platform construct

The Communication Manager Branch i120 platform has one construct.

Construct Description	Construct/Name
2 x MM711	Communication Manager Branch i120 - A (Analog)

Communication Manager Branch G450 Platform LED Status

The Communication Manager Branch G450 supports the following Media Modules:

- MM710 (T1/E1 ISDN PRI)
- MM711 (8 Port Analog)
- MM714B (8 Port Analog)

- MM716 (24 Line Analog)
- MM717 (24 DCP Ports)
- MM720 (8 ISDN BRI)
- MM722 (2 ISDN BRI)

Use the services port on the Communication Manager Branch to connect a laptop and configure the platform.

Location	Name	Color	Description
V7	ETR	Green	Emergency Transfer has been activated.
V7	ALM	Red	This LED indicates a media module failure or mismatch when it is turned ON. This LED is also turned ON when the media module is inserted and should turn OFF after it initializes.
V7	ACT	Yellow	ON when one or more ports are in use.
System	MDM	Green	This LED turns ON when the modem is ready. It is OFF during shutdown, when the USB modem not plugged in, or when the modem is not responding or not functional.
System	ALM	Red	An alarm is present in the system.
System	CPU	Green	OFF - A test is in progress. ON - Normal operation
System	PWR	Green	OFF - No power BLINKING - Problem with power ON - Normal operation
Ethernet Ports	Link State	Green	ON - Link is UP
Ethernet Ports	Activity	Yellow	ON/Blinking - Traffic Activity


G450
AVAYA
SYSTEM
MDM
ALM
CPU
PWR
USB
CONSOLE
SERVICES
COMPACT FLASH
CARD IN USE
ETR
CCA
ETH WAN
ETH LAN
RST
ASB
SHUT DOWN
T1/E1

Replacing Hardware

This section contains the procedures for replacing the following hardware components:

- Replacing Media Modules
- Replacing the Communication Manager Branch i40 Platform
- Replacing the Communication Manager Branch i120 Platform

Replacing Media Modules

Reasons for replacing a media module include:

- Repairing a damaged media module
- Changing the media module type

Most media modules are hot-swappable. This means a media module can be replaced while the system is running without any disruption to the rest of the system. Some configuration of Communication Manager Branch is necessary when a MM710 or MM720 media module is inserted.

Note:

If the media module is MM316: Although the MM316 is hot-swappable, replacing a MM316 Media Module will disrupt PoE and will cause the Communication Manager Branch i120 to reboot. The system will resume normal operation after about 5 minutes.

WARNING:

The Communication Manager Branch i120 must not be operated with any open slots. Empty slots should be covered with the supplied blank plates.

CAUTION:

The connector pins can be bent or damaged if the module is handled roughly or if misaligned and then forced into position.

CAUTION:

There are separate ESD paths to the chassis ground which connect to the media modules at the spring-loaded captive screws. Ensure the captive screws are securely tightened to prevent damage to the equipment.

To replace a media module:

1. Identify and mark all cables.

2. Undo the cables. Note the order in which they are removed.
3. Attach an ESD strap to your wrist.
4. Undo the captive screws and slide out the media module currently inserted into the Communication Manager Branch i120.
5. Position the media module squarely before the selected slot on the front of the Communication Manager Branch i120 and engage both sides of the module in the interior guides.
6. Slide the module slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengaged from the guides. See Figure 18: Inserting Media Modules.
7. Apply firm pressure to engage the connectors at the back of the chassis.

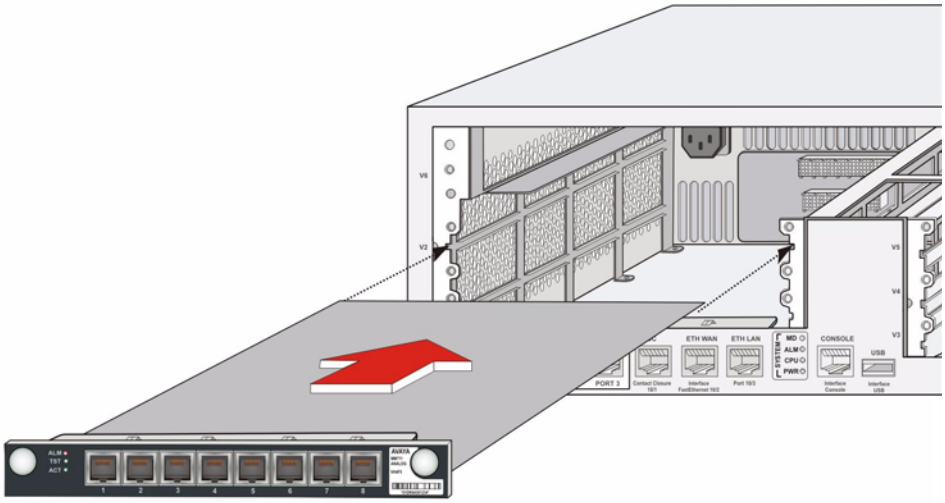
   Note:

   The media module connector has different length pins. The long pins engage first to provide grounding. Medium length and short pins provide power and signal.
8. Lock the media module into the chassis by tightening the spring-loaded captive screws on the front of the module.
9. Plug in the cables in the correct order (in the reverse of the order in Step 2).

   WARNING:

   To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Figure 18: Inserting Media Modules



Replacing the Communication Manager Branch i40 Platform

Circumstances may require that the Communication Manager Branch i40 Platform be replaced due to a hardware or firmware failure.

To replace the Communication Manager Branch i40:

1. If the original i40 is still in operation, backup the configuration files to an FTP server on the customer LAN. Make sure that the **Save Configuration** button is pushed in the Branch Device Manager before doing the backup and powering down. To backup the configuration files, see Backing up Communication Manager Branch using Branch Device Manager
2. Attach an ESD strap to your wrist.
3. If the original i40 is still in operation, power down the system by removing the power cord from the wall power source. This should be done at a time when there will be a minimum interruption in service.
4. Reversing the procedures documented in *Mounting the Communication Manager Branch i40*, remove the i40 from its rack mount.
5. Use the procedures documented in *Mounting the Communication Manager Branch i40* to install the replacement i40 hardware into the rack mount.

6. Power up the system following procedures documented in *Mounting the Communication Manager Branch i40*.
7. Obtain the Authentication File and have its ID updated with the Automatic Registration Tool (ART) or through the Global Customer Care Center (GCCC).
8. There are three possible solutions to restoring the original announcements on the new platform:
   a. Use Branch Central Manager to restore the platform announcements to the new platform. Branch Central Manager has the ability to download the files to the new platform.
   b. Use Communication Manager Branch to restore the announcement files ONLY. Do this by removing all directories and files from the backup on the USB/FTP (after copying them somewhere else) and keep only the GWANNC directory, which contains all of the announcement files and call restore files.
   c. Use Communication Manager Branch to download the files one by one. Note that there can be up to 99 files.

Replacing the Communication Manager Branch i120 Platform

Circumstances may require that the Communication Manager Branch i120 be replaced, either because of hardware or firmware failure, or because of newer technology. Depending upon these circumstances, some or all of the components inserted into the Communication Manager Branch i120 (various media modules) may be reused in the replacement Communication Manager Branch i120.

To replace the Communication Manager Branch i120:

1. If the original Communication Manager Branch i120 is still in operation, backup the configuration files to an FTP server on the customer LAN. Make sure that the **Save Configuration** button is pushed in the Branch Device Manager before doing the backup and powering down. To backup the configuration files, see Backing up Communication Manager Branch using Branch Device Manager
2. Attach an ESD strap to your wrist.
3. If the original Communication Manager Branch i120 is still in operation, power down the system by removing the power cord from the wall power source. This should be done at a time when there will be the minimum interruption in service.
4. Remove all modules from the Communication Manager Branch i120, and carefully set them aside (assuming they will be reused).
5. Reversing the procedures documented in *Mounting the Communication Manager Branch i120*, remove the Communication Manager Branch i120 from its rack mount.

6. Use the procedures documented in *Mounting the Communication Manager Branch i120* to install the replacement Communication Manager Branch i120 hardware into the rack mount.
7. Install the media modules in the appropriate slots.
8. Power up the system following the procedures documented in *Mounting the Communication Manager Branch i120.*
9. Obtain the Authentication File and have its ID updated with the Automatic Registration Tool (ART) or through the Global Customer Care Center (GCCC).
10. There are three possible solutions to restoring the original announcements on the new platform:
    a. Use Branch Central Manager to restore the platform announcements to the new platform. Branch Central Manager has the ability to download the files to the new platform.
    b. Use Communication Manager Branch to restore the announcement files ONLY. Do this by removing all directories and files from the backup on the USB/FTP (after copying them somewhere else) and keep only the GWANNC directory, which contains all of the announcement files and call restore files.
    c. Use Communication Manager Branch to download the files one by one. Note that there can be up to 256 files.

Replacing the Communication Manager Branch G450 Platform

Circumstances may require that the Communication Manager Branch G450 be replaced, either because of hardware or firmware failure, or because of newer technology. Depending upon these circumstances, some or all of the components inserted into the Communication Manager Branch i120 (various media modules) may be reused in the replacement Communication Manager Branch i120.

To replace the Communication Manager Branch G450:

1. If the original Communication Manager Branch G450 is still in operation, backup the configuration files to an FTP server on the customer LAN. Make sure that the **Save Configuration** button is pushed in the Branch Device Manager before doing the backup and powering down. To backup the configuration files, see Backing up Communication Manager Branch using Branch Device Manager
2. Attach an ESD strap to your wrist.
3. If the original Communication Manager Branch G450 is still in operation, power down the system by removing the power cord from the wall power source. This should be done at a time when there will be the minimum interruption in service.

4. Remove all modules from the Communication Manager Branch G450, and carefully set them aside (assuming they will be reused).
5. Reversing the procedures documented in *Mounting the Communication Manager Branch G450*, remove the Communication Manager Branch G450 from its rack mount.
6. Use the procedures documented in *Mounting the Communication Manager Branch G450* to install the replacement Communication Manager Branch G450 hardware into the rack mount.
7. Install the media modules in the appropriate slots.
8. Power up the system following the procedures documented in *Mounting the Communication Manager Branch G450.*
9. Obtain the Authentication File and have its ID updated with the Automatic Registration Tool (ART) or through the Global Customer Care Center (GCCC).
10. There are three possible solutions to restoring the original announcements on the new platform:
    a. Use Branch Central Manager to restore the platform announcements to the new platform. Branch Central Manager has the ability to download the files to the new platform.
    b. Use Communication Manager Branch to restore the announcement files ONLY. Do this by removing all directories and files from the backup on the USB/FTP (after copying them somewhere else) and keep only the GWANNC directory, which contains all of the announcement files and call restore files.
    c. Use Communication Manager Branch to download the files one by one. Note that there can be up to 256 files.

Network Troubleshooting

Network Diagnostics

To aid in troubleshooting network problems, Branch Device Manager provides an interface for the following commands:

- Packet Internet Groper (PING): The PING command is used to test whether a particular host is reachable over the IP network. PING works by sending echo request packets to the target host and listening for Internet Control Message Protocol (ICMP) echo response replies. PING uses interval timing and response rates to estimate the time elapsed for a message to travel to a remote place and back again and packet loss rate between hosts.

  You can use PING to test WAN connectivity between Communication Manager Branch and the default gateway or between Communication Manager Branch and individual IP stations.

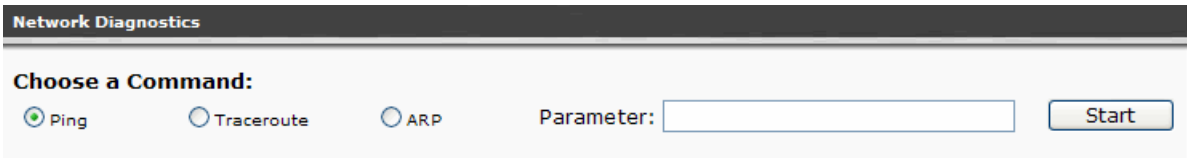
- Traceroute: The Traceroute command maps the path that data packets take between Communication Manager Branch and other endpoints outside of the local network. The output from the traceroute lists all the routers used by the packets during their journey. The time it takes traceroute to complete is an indication of the packet speed of travel.

  If you cannot PING a server, you can use traceroute to verify where the network outage may reside by determining how far into the network you can get.

- Address Resolution Protocol (ARP): The ARP command shows the content of the ARP cache of the Communication Manager Branch which includes the MAC addresses that the Communication Manager Branch recently communicated with. Execute the ARP command to verify that Communication Manager Branch can communicate other devices on the same IP subnet and when you want to resolve an IP address to a physical hardware address. For example, ARP could be used to verify that Communication Manager Branch can reach the default gateway or router. If the IP address used in ARP is not valid or the Ethernet link failed, ARP displays incomplete in the Hardware Address (HWaddress) column.

To execute the PING, the traceroute, or the ARP command, click **Network Diagnostics** under Maintenance and Monitoring. The **Network Diagnostics** screen appears as shown in example Figure 19.

Figure 19: Network Diagnostics screen

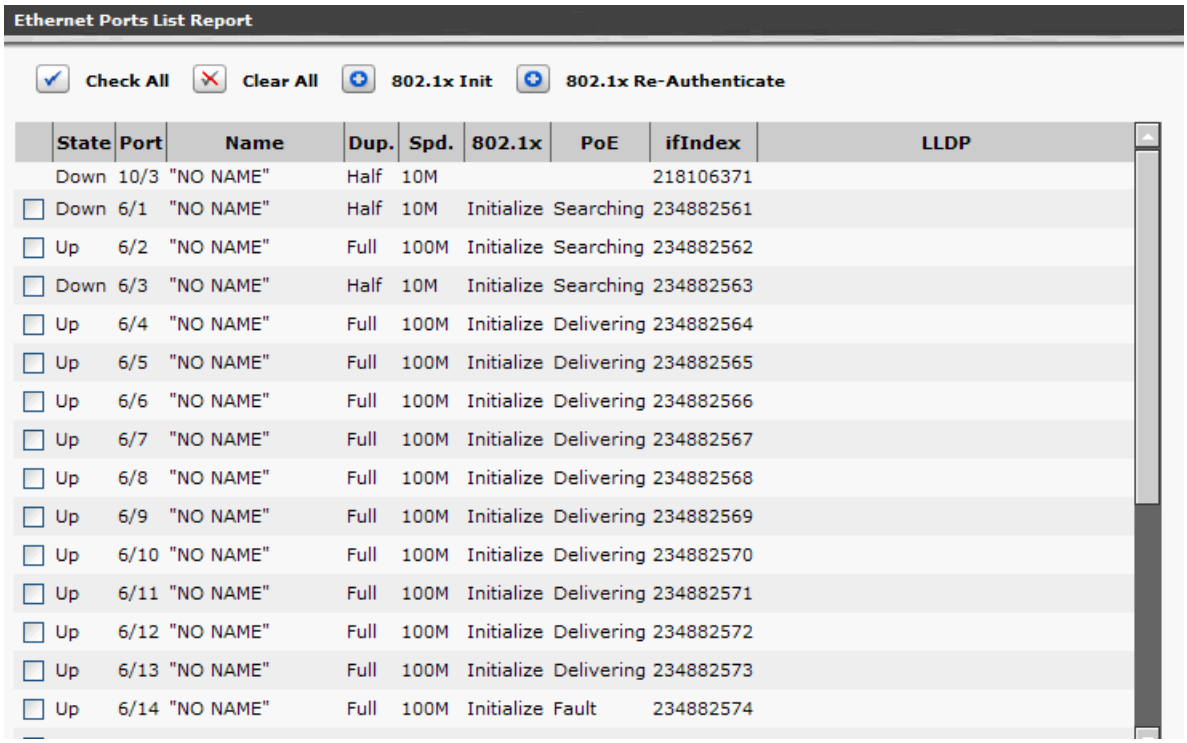


Ethernet Switch port information

Ethernet Ports List Report

To display the **Ethernet Port Lists Report** screen, click **Ports** under Maintenance and Monitoring > Ethernet Switch.

Figure 20: Ethernet Ports List Report screen



State	Port	Name	Dup.	Spd.	802.1x	PoE	ifIndex	LLDP
Down	10/3	"NO NAME"	Half	10M			218106371	
Down	6/1	"NO NAME"	Half	10M	Initialize	Searching	234882561	
Up	6/2	"NO NAME"	Full	100M	Initialize	Searching	234882562	
Down	6/3	"NO NAME"	Half	10M	Initialize	Searching	234882563	
Up	6/4	"NO NAME"	Full	100M	Initialize	Delivering	234882564	
Up	6/5	"NO NAME"	Full	100M	Initialize	Delivering	234882565	
Up	6/6	"NO NAME"	Full	100M	Initialize	Delivering	234882566	
Up	6/7	"NO NAME"	Full	100M	Initialize	Delivering	234882567	
Up	6/8	"NO NAME"	Full	100M	Initialize	Delivering	234882568	
Up	6/9	"NO NAME"	Full	100M	Initialize	Delivering	234882569	
Up	6/10	"NO NAME"	Full	100M	Initialize	Delivering	234882570	
Up	6/11	"NO NAME"	Full	100M	Initialize	Delivering	234882571	
Up	6/12	"NO NAME"	Full	100M	Initialize	Delivering	234882572	
Up	6/13	"NO NAME"	Full	100M	Initialize	Delivering	234882573	
Up	6/14	"NO NAME"	Full	100M	Initialize	Fault	234882574	

The Ethernet Ports List Report contains the following information:

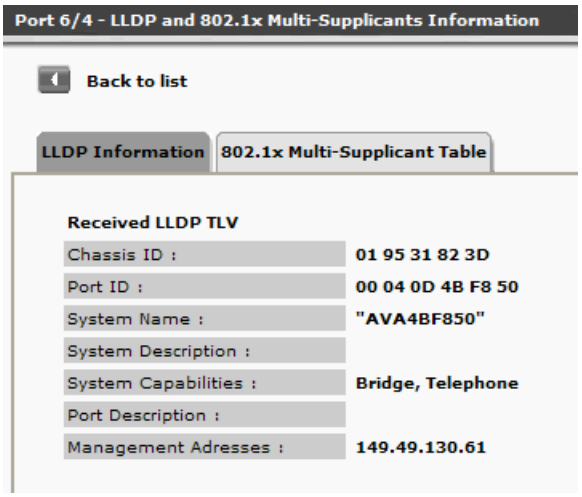
- State: Up or Down
- Port: The module and the port number displays.
- Name: The port name displays if one is assigned.
- Duplex: Half or full duplex
- Speed: 10, 100, or 1000M
- 802.1x: The 802.1x protocol enables Communication Manager Branch to authenticate devices before they are allowed to communicated through the Ethernet switch.

- PoE: This field contains the PoE status of disabled, searching, delivering power, fault, or test.
- IFIndex: The index number is sent in the SNMP trap and can be found in the SNMP MIB interface table.
- Link Layer Discovery Protocol (LLDP): This field contains the system name of the of the connected machine.

  Clicking any column of data for a specified port opens the LLDP and 802.1x Multi-Supplicants Information screen. There are two tabs on this screen, the LLDP Information tab and the 802.1x Multi-Supplicant Table tab.

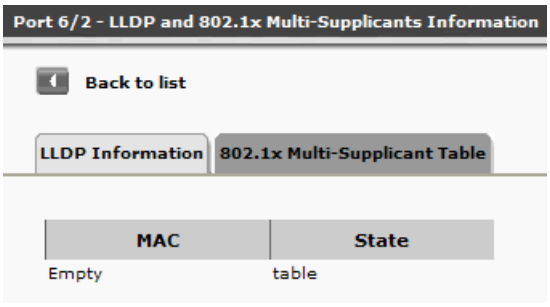
  LLDP defines a set of advertisement messages called TLVs. LLDP allows stations attached to a LAN to advertise information regarding the station's point of LAN attachment to other stations on the same LAN. To see the LLDP TLV information, click one of the columns of data listed for the port. The LLDP Information tab displays.

Figure 21: Ethernet Ports List Report - page two LLDP tab



To see 802.1x Multi-supplicant information, click the 802.1x Multi-Supplicant Table tab. In the Multi-supplicant mode, every device must authenticate itself. The Ethernet switch only allows frames with authenticated MAC addresses to enter into the network. The Multi-supplicant tab displays the MAC address and state of the port. If you connect two devices, such as a PC and an IP endpoint to the same port, each device will have to authenticate itself independently of the other to gain access to the network.

Figure 22: Ethernet Ports List Reports screen - page 2 LLDP and 802.1x information

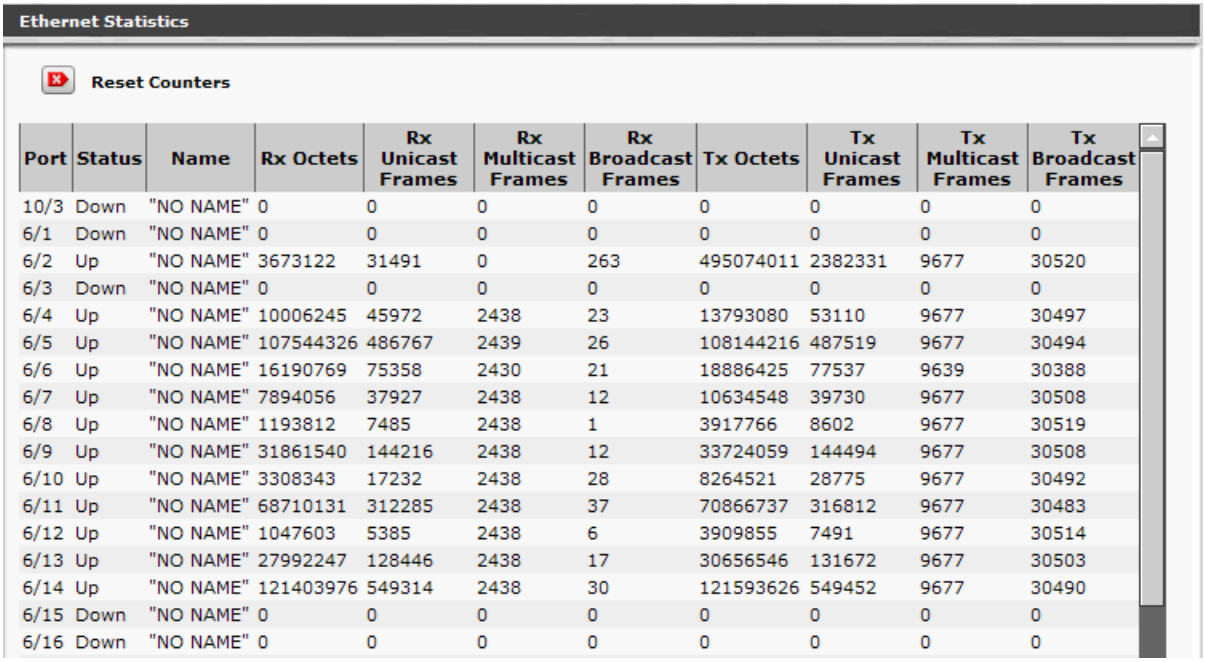


Ethernet Statistics

The **Ethernet Statistics** screen can be used to determine the state of the port and verify if the port is sending and receiving data. The columns with Rx in the heading contains statistics about received data. The columns with Tx in the heading contains statistics about transmitted data.

To display the **Ethernet Statistics** screen, click **Statistics** under Maintenance and Monitoring > Ethernet Switch.

Figure 23: Ethernet Statistics screen



Port	Status	Name	Rx Octets	Rx Unicast Frames	Rx Multicast Frames	Rx Broadcast Frames	Tx Octets	Tx Unicast Frames	Tx Multicast Frames	Tx Broadcast Frames
10/3	Down	"NO NAME"	0	0	0	0	0	0	0	0
6/1	Down	"NO NAME"	0	0	0	0	0	0	0	0
6/2	Up	"NO NAME"	3673122	31491	0	263	495074011	2382331	9677	30520
6/3	Down	"NO NAME"	0	0	0	0	0	0	0	0
6/4	Up	"NO NAME"	10006245	45972	2438	23	13793080	53110	9677	30497
6/5	Up	"NO NAME"	107544326	486767	2439	26	108144216	487519	9677	30494
6/6	Up	"NO NAME"	16190769	75358	2430	21	18886425	77537	9639	30388
6/7	Up	"NO NAME"	7894056	37927	2438	12	10634548	39730	9677	30508
6/8	Up	"NO NAME"	1193812	7485	2438	1	3917766	8602	9677	30519
6/9	Up	"NO NAME"	31861540	144216	2438	12	33724059	144494	9677	30508
6/10	Up	"NO NAME"	3308343	17232	2438	28	8264521	28775	9677	30492
6/11	Up	"NO NAME"	68710131	312285	2438	37	70866737	316812	9677	30483
6/12	Up	"NO NAME"	1047603	5385	2438	6	3909855	7491	9677	30514
6/13	Up	"NO NAME"	27992247	128446	2438	17	30656546	131672	9677	30503
6/14	Up	"NO NAME"	121403976	549314	2438	30	121593626	549452	9677	30490
6/15	Down	"NO NAME"	0	0	0	0	0	0	0	0
6/16	Down	"NO NAME"	0	0	0	0	0	0	0	0

Content Addressable Memory (CAM) Table

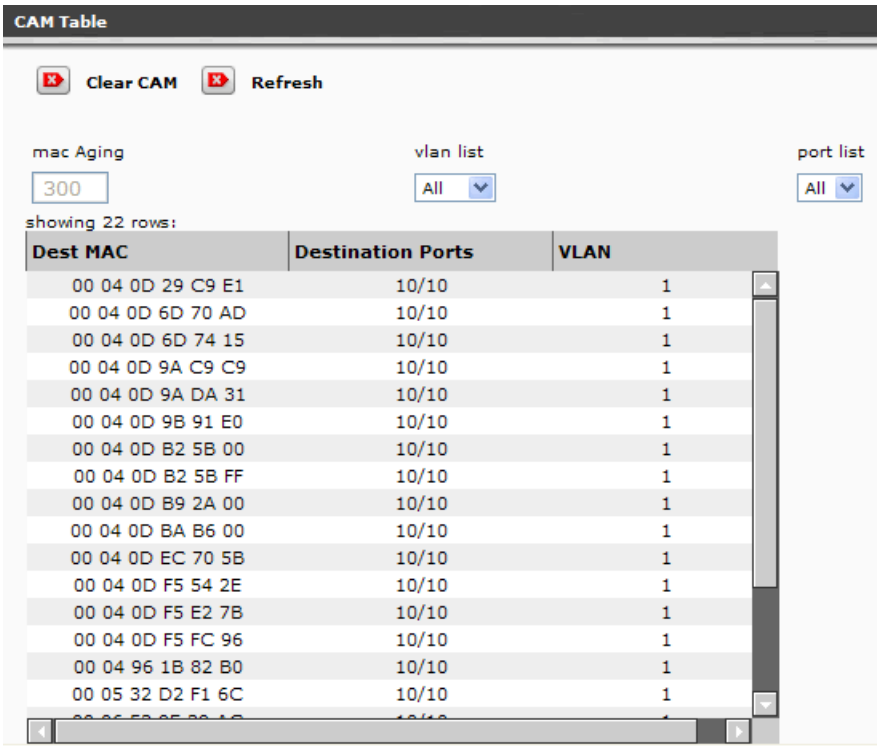
When the switch receives a Data Frame from one of its ports, it updates the CAM Table with the frame's source MAC address and the port on which it was received. The CAM Table displays a list of all known MAC addresses on which an Ethernet port is connected. To access the CAM Table, click **CAM Table** under Maintenance and Monitoring > Platform > Ethernet Switch. The **CAM Table** screen displays as shown in example Figure 24.

The information shown in the CAM Table is static and does not update automatically. When troubleshooting a network problem, use the screen's **Refresh** button to display current information.

To validate the information in the CAM Table, use the **Clear CAM** button to remove all entries. Using **Clear CAM** forces the switch to rebuilt the table with up-to-date information.

If the switch has not heard from a MAC address for 300 seconds (as shown in the **MAC Aging** field) it removes it.

Figure 24: CAM table



DHCP server diagnostics

Communication Manager Branch contains a DHCP server that can be used to serve IP addresses to stations. If the Communication Manager Branch DHCP server is used, the system provides information on DHCP bindings and DHCP statistics. To obtain this information click **DHCP Server** under Maintenance and Monitoring > Platform > Data Services. The **DHCP Binding and Statistics** screen appears displaying the following information:

- A list of active bindings: This list displays IP address that the DHCP server is currently allocating for IP stations.
- The number of DHCP discovers, requests, declines, releases, and informs
- The number of DHCP offers, acknowledgements, and negative acknowledgements
- The number of BOOTP requests and replies

Using the tools and information

The tools and information provided in the Branch Device Manager interface are designed to help troubleshoot network issues. This section contains some examples of how to use this information.

Example one, The following steps could be used to find the physical Ethernet port on which a specific host is connected:

1. Click **Network Diagnostics** under Maintenance and Monitoring. Execute the PING command to verify the IP address and connectivity.
2. Execute the ARP command to find the MAC address of the host.
3. Click **CAM Table** under Maintenance and Monitoring > Platform > Ethernet Switch. Identify the port the host is connected to by looking up the MAC address in the CAM Table.
4. Click **Statistics** under Maintenance and Monitoring > Ethernet Switch. In the **Ethernet Statistics** screen, verify the state of the port and if it is sending and receiving data.

Example two: The following steps could be used to provide information on an IP station that is not working properly:

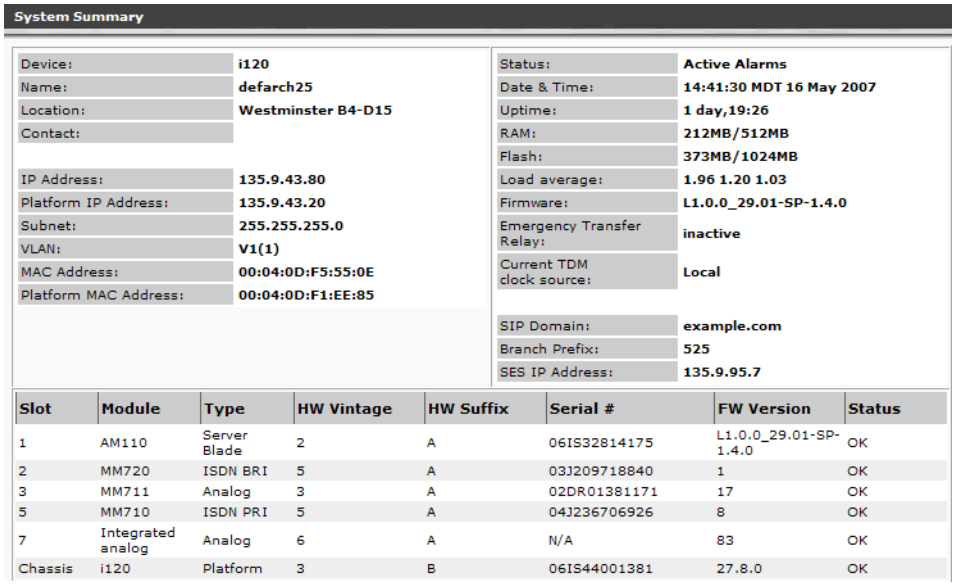
1. Click **Statistics** under Maintenance and Monitoring > Platform > Ethernet Switch. In the **Ethernet Statistics** screen, find the port in the list. Is the port Up or Down? Is the port sending and receiving data?
2. Click **Ports** under Maintenance and Monitoring > Platform > Ethernet Switch. Find the port on the list. Verify that the port is getting PoE.

Example three: Use the following steps to identify excessive broadcast messages:

1. Click **Statistics** under Maintenance and Monitoring > Ethernet Switch.
2. Verify that there is not an excessive count in the received fields of the ports.

Alarms

This section describes the alarm messages which are displayed on the Alarms page and the recommended actions for resolving the alarm. If the Status **Maintenance & Monitoring > Summary** page is Active Alarms, there are active alarms in the system.

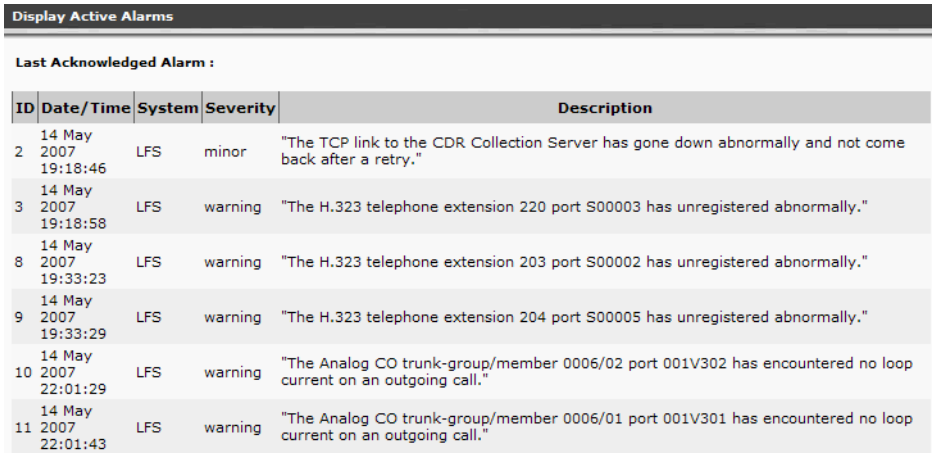


System Summary

Device:	i120	Status:	Active Alarms
Name:	defarch25	Date & Time:	14:41:30 MDT 16 May 2007
Location:	Westminster B4-D15	Uptime:	1 day,19:26
Contact:		RAM:	212MB/512MB
		Flash:	373MB/1024MB
IP Address:	135.9.43.80	Load average:	1.96 1.20 1.03
Platform IP Address:	135.9.43.20	Firmware:	L1.0.0_29.01-SP-1.4.0
Subnet:	255.255.255.0	Emergency Transfer Relay:	inactive
VLAN:	V1(1)	Current TDM clock source:	Local
MAC Address:	00:04:0D:F5:55:0E		
Platform MAC Address:	00:04:0D:F1:EE:85	SIP Domain:	example.com
		Branch Prefix:	525
		SES IP Address:	135.9.95.7

Slot	Module	Type	HW Vintage	HW Suffix	Serial #	FW Version	Status
1	AM110	Server Blade	2	A	06IS32814175	L1.0.0_29.01-SP-1.4.0	OK
2	MM720	ISDN BRI	5	A	03J209718840	1	OK
3	MM711	Analog	3	A	02DR01381171	17	OK
5	MM710	ISDN PRI	5	A	04J236706926	8	OK
7	Integrated analog	Analog	6	A	N/A	83	OK
Chassis	i120	Platform	3	B	06IS44001381	27.8.0	OK

The Alarms can be viewed on the Branch Device Manager under **Maintenance & Monitoring > Alarms**.



Display Active Alarms

Last Acknowledged Alarm :

ID	Date/Time	System	Severity	Description
2	14 May 2007 19:18:46	LFS	minor	"The TCP link to the CDR Collection Server has gone down abnormally and not come back after a retry."
3	14 May 2007 19:18:58	LFS	warning	"The H.323 telephone extension 220 port S00003 has unregistered abnormally."
8	14 May 2007 19:33:23	LFS	warning	"The H.323 telephone extension 203 port S00002 has unregistered abnormally."
9	14 May 2007 19:33:29	LFS	warning	"The H.323 telephone extension 204 port S00005 has unregistered abnormally."
10	14 May 2007 22:01:29	LFS	warning	"The Analog CO trunk-group/member 0006/02 port 001V302 has encountered no loop current on an outgoing call."
11	14 May 2007 22:01:43	LFS	warning	"The Analog CO trunk-group/member 0006/01 port 001V301 has encountered no loop current on an outgoing call."

A list of tests are also included in each alarm message section. These tests are executed during periodic and scheduled maintenance, and can be run on-demand. See the repair procedures for the tests to help troubleshoot and resolve the alarm.

If the alarm description contains...	See...
Analog telephone extension	Analog Telephone Alarms
Digital CO trunk-group/member	Digital CO Trunk Alarms
Analog CO trunk-group/member	Analog CO Trunk Alarms
Digital DID trunk-group/member	Digital DID Trunk Alarms
Analog DID trunk-group/member	Analog DID Trunk Alarms
H.323 telephone extension	H.323 Telephone Alarms
ISDN PRI D-Channel	ISDN PRI D-Channel Alarms
ISDN BRI B-Channel	ISDN PRI B-Channel Alarms
Media Gateway	Media Gateway Alarms
TCP link to the CDR Collection Server	To log into the Media Gateway:
ISDN BRI port	ISDN BRI Port Alarms
ISDN BRI trunk-group/member	ISDN BRI Trunk Alarms
Digital TIE trunk-group/member	Digital TIE Trunk Alarms
SIP trunk	SIP Trunk Alarms

Analog Telephone Alarms

The Port Diagnostic Test (#35), ONS Ringer Application Test (#48), and Port Audit and Update Test (#36) are run on Analog Telephones.

Analog Telephone Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The analog telephone extension X port Y is OK	No action required
LFS	warning	The analog telephone extension X port Y failed	Call the analog phone. If the phone does not ring, replace it.
LFS	warning	The analog telephone extension X port Y has been locally taken out of service.	The phone has been busied out. Release the phone.
LFS	minor	The analog telephone at extension X port Y has had its media module fail or been removed.	Reseat or replace the media module.
LFS	minor	The analog telephone at extension X port Y couldn't get ringing voltage from its media module.	Ringing voltage is absent. Replace the media module.

Digital CO Trunk Alarms

The Port Audit and Update Test (#36) runs on Digital CO trunks.

Digital CO Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The Digital CO trunk-group/member X/Y port Z is OK	No action required
LFS	warning	The Digital CO trunk-group/member X/Y port Z has been placed out of service locally.	The Digital CO trunk (T1/E1) has been busied out. Release the trunk if appropriate.
LFS	minor	The Digital CO trunk-group/member X/Y port Z has encountered hardware problems with the associated media module or it has been removed.	Reinsert or replace the media module.
LFS	minor	The Digital CO trunk-group/member X/Y port Z has encountered hardware problems with the associated media module.	The DS1 Interface media module detected a hardware fault. Test the media module and follow the repair steps for the test(s) that fail.
LFS	warning	The Digital CO trunk-group/member X/Y port Z has been taken out of service remotely.	Check the status of the far-end.

Analog CO Trunk Alarms

The following tests are run on Analog CO Trunks:

- CO Port Diagnostic Test (#3)
- Port Audit and Update Test (#36)

In a certain situation the service state of analog CO trunks can be reported incorrectly for a short period of time. If a user administers a CO trunk in the Branch Device Manager while no actual trunk is plugged into the analog port, then the Communication Manager Branch checks the state of the trunk. Since the dial-tone test fails (it's not plugged in), the trunk is reported as out of service. The user then connects a trunk to the port, but the Branch Device Manager status page will still report the trunk as out-of-service.

The trunk will work (and be reported as in-service) as soon as either a call is made on it OR a periodic audit that runs every 15 minutes sees a successful dial-tone test. Until then, the CO trunk will be reported as out-of-service.

If the trunk is connected BEFORE being administered in Branch Device Manager, then the test that runs at administration time will succeed.

Analog CO Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The Analog CO trunk-group/ member X/Y port Z is OK	No action required
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has been placed out of service locally.	The Analog CO trunk has been busied out. Release the trunk if appropriate.
LFS	minor	The Analog CO trunk-group/ member X/Y port Z has encountered problems with the associated media module or it has been removed.	Reinsert or replace the media module.
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered battery reversal at the far end.	This is usually caused by the CO. This could occur if the trunk was just installed and for some reason the Tip and Ring wires were reversed. Refer the problem to CO. Ask them to remove the battery reversal option.
			1 of 5

Analog CO Trunk Alarms (continued)

System	Severity	Alarm Description	Recommended Action
LFS	minor	The Analog CO trunk-group/ member X/Y port Z has encountered a stuck ground detector.	Ground detector stuck active. Test the affected media module. If the test aborts with Error Code 1000, disconnect Tip and Ring and repeat the test. If the test still aborts, replace the media module. If the test passes, refer problem to CO. If any other error code is received, follow the repair steps for the test.
LFS	warning	The Analog CO trunk-group/ member X/Y port Z is not seeing a release from the far end.	CO not releasing after call is dropped from far end, or the loop is not open after a disconnect. Refer the problem to the CO.
LFS	minor	The Analog CO trunk-group/ member X/Y port Z is not detecting dialtone from the far end.	Test the affected media module. If the test fails, replace the media module.
			2 of 5

Analog CO Trunk Alarms (continued)

System	Severity	Alarm Description	Recommended Action
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered single polarity ringing current.	This error results from abnormal ringing current, but does not prevent the incoming call from being accepted. One cause could be that the reverse current detector associated with the port is failing. (Will not be detected by any tests.) Another cause could be that normal current is not detected. In this case, neither incoming nor outgoing calls can be completed, and the dial tone test will also fail. The last cause could be that certain types of noise are present on the CO line during the silent period of ringing. 1. Check for other errors. If every test passes, then either the reverse current detector is defective or the CO line is noisy. 2. If the CO line is suspect, make Tip and Ring observations. If the line is determined to be noisy, refer the problem to the CO. 3. If the reverse current detector is defective, ignore this error.
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered the loop opening too slowly after a disconnect.	This error indicates an on-board problem, although the trunk may be functional. Replace the media module.
			3 of 5

Analog CO Trunk Alarms (continued)

System	Severity	Alarm Description	Recommended Action
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered no loop current after answering incoming call.	The incoming destination has already answered and no loop current has been detected. Test the media module. If this is a hard fault, the dial tone test and every outgoing call should also fail. Check for other errors.
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered no tip ground current on an outgoing call.	This error occurs when an attempt is made to seize a ground-start CO trunk for an outgoing call and Tip ground is either not detected or the caller hangs up before Tip ground is detected. 1. Busyout and test the affected port. If any tests fail, refer to the description of the tests and the associated error codes. Release the port. 2. If users continue to report troubles, check for other errors and make test calls to determine whether the problem should be referred to the CO. Busyout the affected port, and test it. If the Dial Tone Test #0 passes, ignore this error. Release the port.

4 of 5

Analog CO Trunk Alarms (continued)

System	Severity	Alarm Description	Recommended Action
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered no loop current on an outgoing call.	This error occurs on attempt to seize a loop or ground-start trunk for an outgoing call. An error occurs if loop current is not detected or the caller hangs up before it is detected. Busyout and test the affected port. If the CO Port Diagnostic Test #3 passes and this error keeps occurring, refer problems to CO. Release the port.
LFS	warning	The Analog CO trunk-group/ member X/Y port Z has encountered ringing with no ground	This error is detected on an incoming call on a ground-start CO trunk. The CO trunk media module has not detected a Tip ground before ringing current is detected. This may indicate that the ground detector is not working. However, the call will be accepted. Busyout and test the affected port. If any tests fail, refer to the description of the tests and the associated error codes. Release the port. If users continue to report troubles, check for other errors and make test calls to determine whether the problem should be referred to the CO.
			5 of 5

Digital DID Trunk Alarms

The Port Audit and Update Test (#36) is run on Digital DID trunks.

Digital DID Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The Digital DID trunk-group/ member X/Y port Z is OK	No action required
LFS	warning	The Digital DID trunk-group/ member X/Y port Z has been placed out of service locally.	The trunk has been busied out. Release the trunk if appropriate.
LFS	minor	The Digital DID trunk-group/ member X/Y port Z has encountered hardware problems with the associated media module or it has been removed.	Reinsert or replace the media module.
LFS	warning	The CO is not releasing the Digital DID trunk-group/member X/Y port Z.	Test the media module. Follow the repair steps for any test that fails. If all tests pass, refer the problem to the CO.
LFS	warning	The Digital DID trunk-group/ member X/Y port Z has encountered a delayed release on disconnect.	Test the media module. Follow the repair steps for any test that fails. If all tests pass, refer the problem to the CO.
LFS	warning	The Digital DID trunk-group/ member X/Y port Z has encountered an inconsistent signaling change.	Test the media module and follow the repair steps for any test that fails.

Analog DID Trunk Alarms

The Port Audit and Update Test (#36) is run on Analog DID trunks.

Analog DID Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The Analog DID trunk-group/member X/Y port Z is OK	No action required
LFS	warning	The Analog DID trunk-group/member X/Y port Z has encountered incoming dialing problems.	Verify that the trunk is administered correctly. If so, refer the problem to the CO.
LFS	warning	The Analog DID trunk-group/member X/Y port Z has been placed out of service locally.	The trunk has been busied out. Release the trunk if appropriate.
LFS	minor	The Analog DID trunk-group/member X/Y port Z has encountered hardware problems with the associated media module or it has been removed.	Reinsert or replace the media module.
			1 of 2

Analog DID Trunk Alarms (continued)

System	Severity	Alarm Description	Recommended Action
LFS	warning	The Analog DID trunk-group/member X/Y port Z has encountered rotary pulse problems.	Verify the trunk-administered interdigit-timing parameters. Test the trunk by performing an incoming test call. Refer the problem to the CO.
LFS	warning	The CO is not releasing the Analog DID trunk-group/member X/Y port Z.	Loop current active, CO is not releasing trunk after switch disconnect. Occurs when the switch end drops first and the CO does not release the trunk within 4 minutes. 1. Verify the interface to the network with a hand telephone set. If calls are placed correctly, then refer problem to the CO. 2. If unable to place calls or this equipment is not available, check the status of the port. If active but not connected, disconnect bridging clips at the network interface. Check the status of the trunk. If the trunk went idle, then replace the clips. If the trunk is still active but unable to place calls, refer the problem to the CO.

2 of 2

H.323 Telephone Alarms

The following tests are run on H.323 Telephones:

- Digital Station Lamp Update (#16)
- Digital Station Audits Test (#17)
- Registration Status Inquiry Test (#1372)

H.323 Telephone Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The H.323 telephone extension X is OK	No action required.
LFS	warning	The H.323 telephone extension X has unregistered abnormally.	The station is now basically an AWOH station and is no longer being maintained.
LFS	warning	The H.323 telephone extension X has been placed out of service.	The phone has been busied out. Release the phone.
LFS	warning	The link to the H.323 telephone extension X has gone down abnormally.	The link has gone down between the terminal and its gateway to the switch. This likely means that the IP station has unregistered.

ISDN PRI D-Channel Alarms

The following tests are run on the ISDN PRI D-Channel:

- Primary Signaling Link Hardware Check (#636)
- Remote Layer 3 Query (#637)
- Layer 2 Status Query Test (#647)

ISDN PRI D-Channel Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The ISDN PRI D-Channel (Signaling Group X) is OK	No action required
LFS	warning	The ISDN PRI D-Channel (Signaling Group X) has been down for more than 90 seconds. It may come back.	The D-Channel connection has been lost for more than 90 seconds. The associated B-Channels will be placed in the ISDN Maintenance/Far-End state and will not be usable for outgoing calls, although incoming calls will still be accepted. The switch will automatically attempt to recover the signaling link. 1. Check the results of the Primary Signaling Link Hardware Check (#636). Follow the repair steps for any error codes. 2. When the link does recover, the B-Channels will be negotiated back to the In-Service state and their alarms will be retired. When this error occurs, the state of the Signaling Group is changed to out of service. Verify the state of the signaling group.
LFS	minor	The media module associated with ISDN PRI D-Channel (Signaling Group X) has been removed or is having problems.	If the media module has been removed, reinsert or replace the media module. If the media module has not been removed, test the media module and note the results of the Primary Signaling Link Hardware Check (#636)

1 of 2

ISDN PRI D-Channel Alarms (continued)

System	Severity	Alarm Description	Recommended Action
LFS	warning	ISDN PRI D-Channel (Signaling Group X) has failed its layer 2 (LAPD) query test. Is it configured and connected properly?	The Layer 2 Query Test failed for the D-Channel. See Layer 2 Status Query Test (#647).
LFS	minor	ISDN PRI D-Channel (Signaling Group X) has failed its layer 3 (MDL) query test. Is it configured properly on both ends?	The Remote Layer 3 Query (#637) failed. Investigate elements of the ISDN PRI D-Channel(s) for both this switch and the far-end switch. If Test #637 fails twice in a row, the B-Channels will be alarmed and made unavailable for outgoing calls (although incoming calls will still be accepted). When Test #637 succeeds and the far-end switch starts responding properly, the DS1 ISDN Trunk (B-Channels) will be placed back into normal operation, and their alarms will be retired.
			2 of 2

ISDN PRI B-Channel Alarms

The following tests are run on the ISDN PRI B-Channel:

- Port Audit and Update Test (#36)
- Signaling Link State Audit Test (#255)
- Service State Audit Test (#256)
- Call State Audit Test (#257)

ISDN PRI B-Channel Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The ISDN PRI B-Channel trunk-group/member X/Y port Z is OK	No action required.
LFS	warning	The ISDN PRI B-Channel trunk-group/member X/Y port Z has been taken out of service locally.	The ISDN PRI B-Channel has been busied out. Release the ISDN PRI B-Channel.
LFS	minor	The ISDN PRI B-Channel trunk-group/member X/Y port Z has been taken out of service remotely.	The far-end switch changed its ISDN service state to either *out of service* or *maintenance*. This may be either a temporary condition due to far-end testing of the trunk or a hardware problem with the trunk. Outgoing calls will not be allowed over the trunk. Test the trunk and investigate the status of the trunk.
LFS	warning	The ISDN PRI B-Channel trunk-group/member X/Y port Z is not recognized by the far end. Check configuration on each side.	This trunk is not recognized by the far-end switch. Investigate the trunk administration for both switches and make changes as necessary.
LFS	minor	The ISDN PRI B-Channel trunk-group/member X/Y port Z has been rejected 10 times by the far end. Check configuration on each side.	This may indicate a service-state mismatch between the near and far ends for this trunk that is affecting the end user or that the ISDN trunk is not administered at the far end. Verify that the far end has this trunk administered. If problems persist, busyout the ISDN trunk to take it out of the hunt group.

Media Gateway Alarms

The following tests are run on Media Gateways:

- Link State Audit Test (#1527)
- Media Gateway Hyperactivity Audit Test (#1659)

Media Gateway Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The Media Gateway number X is OK	No action required.
LFS	major	Keepalive messages to Media Gateway number X have failed.	The LAN or the platform is down.
LFS	major	Other problems on Media Gateway X. Log into it and check error log or look for notifications directly from it.	Log into the Media Gateway and check for errors. Test the Media Gateway and follow the repair steps for tests that fail.
LFS	minor	Media Gateway X has unregistered.	The link has unregistered with the platform. There is a problem on the platform.
LFS	warning	Media Gateway X has stopped periodic maintenance due to high traffic.	Due to high traffic, the media gateway socket control process turned off board and port periodic maintenance. When traffic levels decline, periodic maintenance will be turned on again and the alarm resolved.

To log into the Media Gateway:

1. In the Branch Device Manager, select **Maintenance and Monitoring> Alarms**.

   A list of all alarms, including Media Gateway, is displayed.

CDR Collection Server Alarms

The following tests are run on the TCP link to the CDR Collection Server:

- Link Tear Down Test (#213)

- Link Retry Test (#215)

CDR Collection Server Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The TCP link to the CDR Collection Server is OK	No action required.
LFS	warning	The TCP link to the CDR Collection Server has been locally placed out of service.	The CDR link has been busied out and the CDR link is down. Release the CDR link.
LFS	minor	The TCP link to the CDR Collection Server has gone down abnormally and not come back after a retry.	See CDR Link Troubleshooting Procedures
LFS	warning	The TCP link to the CDR Collection Server has overflowed and records are being buffered.	Overflow of CDR records generated in the switch due to the heavy trunk traffic and low speed CDR output device. No action is necessary for this Error Type.

ISDN BRI Port Alarms

The following tests are run on an ISDN BRI Port;

- Level 1 Status Query Test (#1242)
- CRC Error Counter Test (#623)
- Receive FIFO Error Counter Test (#625)
- BRI Layer 3 Query Test (#1243)
- BRI Port Slip Query Test (#1244)
- Clear Error Counters (#270)

ISDN BRI Port Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The ISDN BRI port X is OK	No action required.
LFS	minor	The ISDN BRI port X has been disconnected from the far end.	Loss of continuity of Layer 1 to the far end. Test the media module. If Layer 1 cannot be activated, the port is taken out of service.
LFS	warning	The ISDN BRI port X has been taken out of service locally.	The ISDN BRI port has been busied out. Release the ISDN BRI port.
LFS	warning	The ISDN BRI port X has encountered the unexpected expiration of a timer.	The ISDN BRI port is generating too many uplinks. If too many events occur within a certain time, the port is alarmed and taken out of service. Test the port and follow the repair steps for any errors.
LFS	warning	The ISDN BRI port X has encountered a CRC error on the D-channel.	This error is most likely due to a problem with backplane wiring, a noise source, or no termination (an open circuit). It usually does not indicate a problem with the media module.
LFS	minor	The ISDN BRI port X has encountered a layer 3 query failure.	The Layer 3 Query test is repeated every 15 minutes until it passes.
LFS	warning	The ISDN BRI port X has encountered a framing slip.	A frame of information had to be repeated or deleted. Slips usually occur when the received bit rate is not synchronized with the TDM bus clock.

ISDN BRI Trunk Alarms

The following tests are run on an ISDN BRI Trunk:

- Signaling Link State Test (#1251)
- Service State Audit Test (#256)
- Call State Audit Test (#257)

ISDN BRI Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The ISDN BRI trunk-group/member X/Y port Z is OK.	No action required.
LFS	warning	The ISDN BRI trunk-group/member X/Y port Z has been taken out of service locally.	The ISDN BRI Trunk has been busied out. Release the trunk if appropriate.
LFS	minor	The media module associated with ISDN BRI trunk-group/member X/Y port Z has either been removed or experienced a hardware problem.	If the media module has been removed, reinsert it or replace it. Investigate hardware problems.
LFS	warning	The ISDN BRI trunk-group/member X/Y port Z has been taken out of service remotely.	The far-end has reported that this channel is not administered. The trunks are placed in the out-of-service state.
LFS	minor	The D channel associated with the ISDN BRI trunk-group/member X/Y port Z has gone down.	The Signaling Link is down.
LFS	minor	The remote end has rejected ISDN BRI trunk-group/member X/Y port Z as a B channel.	Test the media module and the platform. Check for transmission problems. Test the port.

Digital TIE Trunk Alarms

The Port Audit and Update Test (#36) is run on Digital TIE Trunks.

Digital TIE Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The Digital TIE trunk-group/member X/Y port Z is OK	No action required.
LFS	warning	The Digital TIE trunk-group/member X/Y port Z has been placed out of service locally.	The Digital TIE trunk has been busied out. Release the trunk if appropriate.
LFS	minor	The Digital TIE trunk-group/member X/Y port Z has encountered hardware problems with the associated media module or it has been removed.	Reinsert or replace the media module.
LFS	warning	The Digital TIE trunk-group/member X/Y port Z never received an on-hook from the far end.	Check with the far-end switch or operating company for proper trunk connection.
LFS	warning	The Digital TIE trunk-group/member X/Y port Z encountered a delayed far-end on-hook.	The trunk has received the belated “on-hook” that it has been waiting for from the far-end switch. This error can be ignored.
LFS	warning	The Digital TIE trunk-group/member X/Y port Z T1/E1 facility has been taken out of service.	Investigate the media module or platform for problems.
LFS	warning	The Digital TIE trunk-group/member X/Y port Z encountered an outgoing seize failure.	The trunk could not be seized.

SIP Trunk Alarms

The following tests are run on SIP Trunks:

- Ethernet Port Status Test (#1386)
- MedPro Status Test (#1392)
- Signaling Group PING Test (#1387)

SIP Trunk Alarms

System	Severity	Alarm Description	Recommended Action
LFS	clear	The SIP trunk (Signaling Group X) is OK	No action required.
LFS	warning	The SIP trunk (signaling group X) has been taken out of service locally.	The SIP trunk has been busied out. Release the trunk if appropriate.

Logs

Logs can be viewed, saved to disk, or sent to Avaya for analysis. The following sections describe the Log screen, how to filter a log, how to view a log, and how to send a log.

The Debug Traces log contains debugging information.

The Restart log contains information regarding system restarts.

The Watchdog log contains information regarding the following:

- Software starts/restarts/failures
- Shutdowns and reboots
- Processor occupancy (excessive CPU cycles)
- SNMP traps started/stopped
- Memory
- Process sanity

Interpreting Log Entries

The beginning of each entry in the log contains timestamp information separated by colons (:), and looks similar to the following:

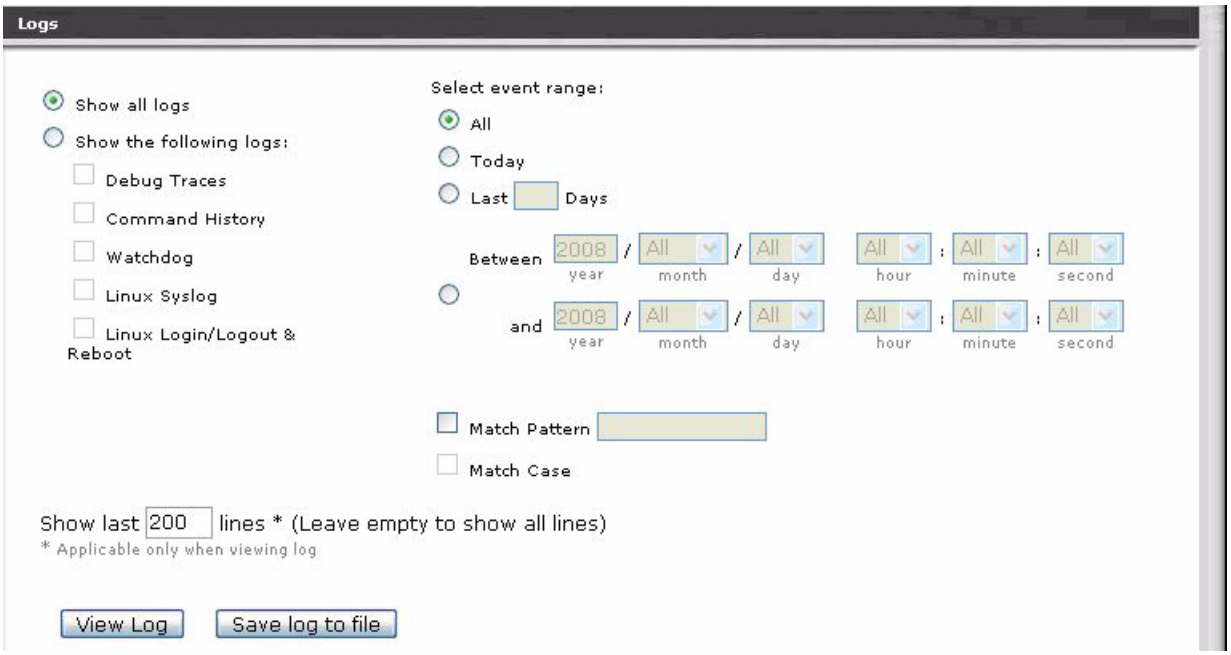
```
20070227:11065800:96896
```

The information is interpreted as follows:

- **20070227** is the date (February 27, 2007)
- **11065800** is the time of the logged event (11 hours, 06 minutes, 58 seconds, 00 milliseconds (ms) or 11:06:58 AM)
- **96896** is the sequence number of this log entry

Log Filtering/Viewing

Debug traces, restart events, watchdog events, and system logs can be accessed from the **Maintenance & Monitoring > Logs** page.



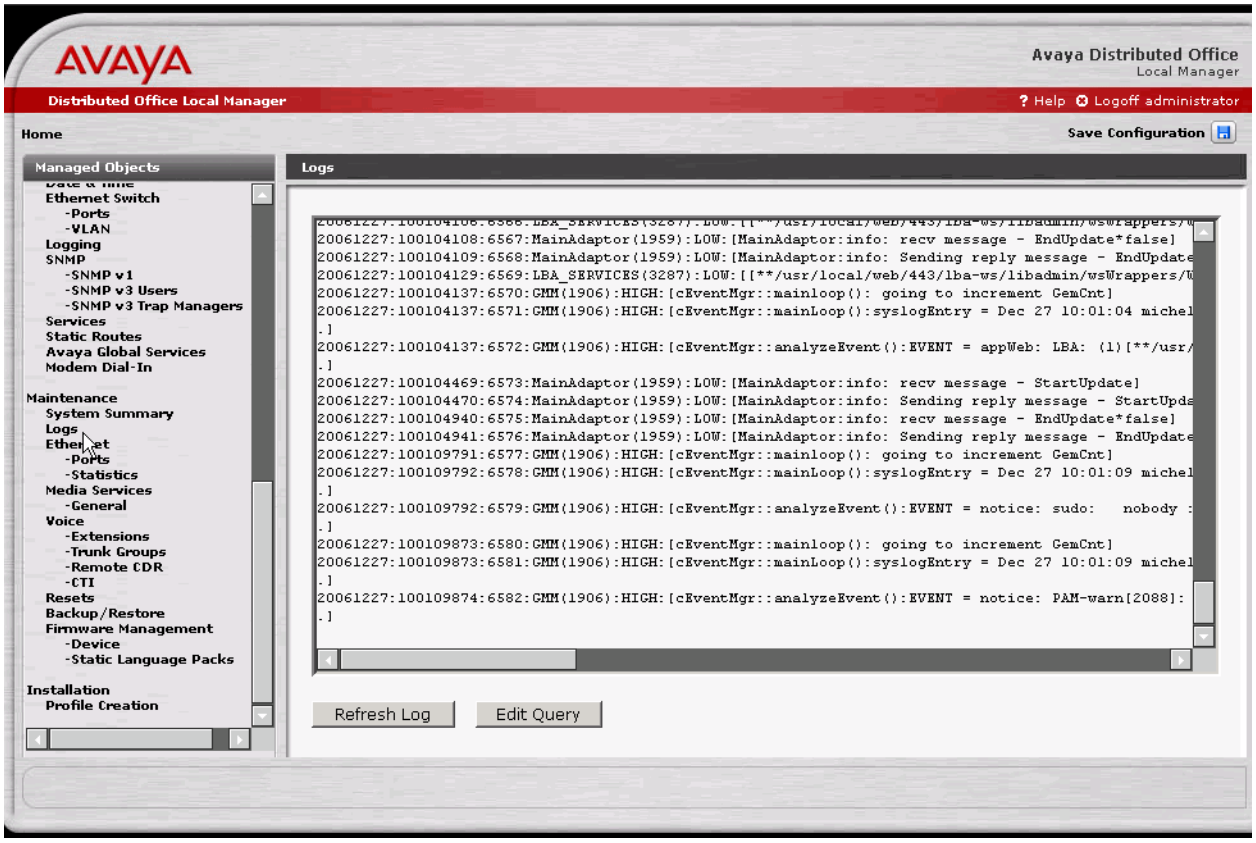
The easiest information to decipher will be from the Linux Syslog. Select **Show the following logs:** and select **Linux Syslog**. The event range should be **All**.

A pattern can be entered which will cause only those entries which match that pattern to be displayed. For example, to view the syslog entries that relate to IP Telephone Events, check the **Match Pattern** box, enter **IPEVT** in the larger **Match Pattern** box, then click on **View Log**

Only the entries which include IPEVT will be displayed on the screen.

Use the **Show all logs** option to maximize the search results for **Match Pattern**.

The following is an example of a log file:



Command History

Communication Manager Branch 1.2 contains a log called **Command History**. The Command History displays an audit trail of changes previously made to the system setup or configuration, a very helpful tool when trying to troubleshoot a current problem.

Any change followed by successful submit instruction ("Apply Change", "Set", "Start", "Remove", "Reset", "Save Configuration") to the Server side and successfully passed the business logic tests appears in the Command History archive.

Log Filtering/Download

To download a log, select which log you want to view, the range, and any pattern that should be matched. Uncheck the **Match Pattern** box to display everything in the log. Click on **Download Log**. A pop-up menu will appear with a pre-named file. The options are to **Open with Notepad** and **Save to Disk**. It is ***not*** good for these Unix-formatted text files to be opened with Notepad.

When you are satisfied with the selection, click on OK.

Log View - Platform Events

To view platform events, check the **Match Pattern** box and enter **>#1** in the larger **Match Pattern** box. This character string appears in the event entries, such as the following example:

20070425:04656000:79288:defarch25 err: : >#1,YY,ACT,_WD,A,22,MIN,EVE,N,00/00:00:00:00,none,none,WARNING: Watchdog killing TraceLogger (pid1910) because heartbeats stopped!#

Watchdog events are included in the output. They show when software processes restart.

Debug Reports

Debug reports can be sent to Avaya Support for analysis. A Debug Report contains the syslog, database files, core, and debug log files. The Debug report contains information regarding the following processes:

Process	Function
prc_mgr	Manages start-up and recovery of LFS
fast_map	Maintenance action process (map) that runs high-level maintenance actions
capro	Call processing including user manager, service dispatcher, and connection manager
hmm	High-level maintenance manager
mdm	Maintenance data manager
watchd	Maintains and monitors heartbeats for all processes. Writes to syslog and wdlog, does not write to the debug trace log.

Select **Reports** under **Maintenance & Monitoring,** then select **Extended Debug Report**. A pop-up window will appear asking what Firefox should do with this file. The default is Open with WinZip, which is the default and should be selected. Click on **OK**

IP Telephone Events

The output for filtering the Linux syslog with the pattern IPEVT will list:

- IP stations that are up or down
- Registering/unregistering gateways and IP endpoints
- Reason for IP phone unregistration
- IP address of station registering

The following shows a sample IP event output display:

Figure 25: Sample IP event log

```
20061109:131342365:34112:defarch25 notice: logm:IPEVT IPT_REG board=PROCR ip= 161.127.228.25
   net_reg= 1  ext= 200 ip= 161.127.228.64: 3000 net_reg= 1 reason=normal
20061109:131342365:34112:defarch25 notice: logm:IPEVT IPT_REG board=PROCR ip= 161.127.228.23
   net_reg= 1  ext= 241 ip= 161.127.228.93: 3000 net_reg= 1 reason=endpoint_request
20061109:131342365:34112:defarch25 notice: logm:IPEVT IPT_UNREG board=PROCR
ip=161.127.228.36 net_reg= 1  ext= 248 ip= 161.127.228.47: 3000 net_reg= 1 reason=2015
```

The last entry in **Figure 25: Sample IP event log** lists a reason code of 2015. The station was forced to unregister because it had been moved. A list of reason codes and their explanations are found in Reason Codes for IP Telephone Events.

Reason Codes for IP Telephone Events

Reason Codes for IPEVT

Reason Code	Explanation
2000	Unregistration Request rejected because no station user record exists for unregistering user (internal software error).
2002	Unregistration Request rejected because of failure to build an unregistration request confirm (UCF) message (internal software error).
2004	Unregistration Request rejected because the no station user record exists for the unregistering user (internal software error).
2007	Force Unregistration Request. Unregister user because there is no signaling connection. RAS is alive, but the signaling connection has gone down (user cannot make calls). Re-register the endpoint.
2008	Force Unregistration Request. Unregister associated H.323 user because there is no signaling connection. Re-register the endpoint.
2009	Force Unregistration Request. Extension is already registered, but received a forced login registration request (RRQ). Send a URQ to the existing extension.
2010	Forced Unregistration Request. The Gatekeeper is unregistering the endpoint because its call signaling connection has closed.
2011	Force Unregistration Request. After an endpoint registers it should initiate the TCP connection and send a SETUP message. The SETUP message has not been received from the endpoint, and no Q931 Call object exists. The endpoint cannot make calls, so unregister it.
2012	Force Unregistration Request. Unregister endpoint that has aged out. Endpoint's time to live (TTL) expired without receiving a keep-alive request (RRQ).
2015	Forced Unregistration Request. Unregister user because the extension has been removed.
2017	Forced Unregistration Request. Unregister the endpoint if there are no station user-records remaining.
2018	Forced Unregistration Request. The release command was run on the extension or port.
2019	Forced Unregistration Request. The release command was run on the Remote Office extension or port.
	1 of 4

Reason Codes for IPEVT (continued)

Reason Code	Explanation
2021	Custom Selection of VIP Direct Inward Dialing numbers feature is not active.
2022	Announcement present but not administered.
2023	Announcement present but no announcements administered for the board.
2024	Registration rejected because unable to create an entry in the MTM complex table.
2025	Registration rejected because the option chosen by the endpoint in the RRQ for the emergency call does not match the option administered on the station form.
2026	Xmobile offhook request rejected because Xmobile station has been taken out of service.
2027	User attempted to play announcement and file was not found on board.
2028	User attempted to play announcement and file had bad format.
2029	Gatekeeper Request rejected because the Non Standard Data (NSD) from the registered application has an invalid object ID.
2030	Gatekeeper Request rejected because of failure to decode Non Standard Data (NSD) element.
2031	Gatekeeper Request rejected because of unexpected Non Standard Data (NSD) message from the registered application endpoint.
2032	Force Unregistration Request. Instruct the RAS manager to cleanup a User ID which had just been registered prior to a system restart. This event is not logged, but only passed in the URQ.
2033	Force Unregistration Request. Reset ip-stations was executed from the SAT to force unregister endpoints.
2038	Getting the calling party number from the incoming side of the call failed.
2039	Keep Alive Registration Request. Registration rejected because no endpoint identifier was provided.
2040	Gatekeeper Request rejected because no resources available for signaling connection.
2041	Registration Request rejected because no Digital Signal Processor (DSP) resources are available.
2042	Registration Request rejected because no Digital Signal Processor (DSP) resources are available.
	2 of 4

Reason Codes for IPEVT (continued)

Reason Code	Explanation
2043	ARQ rejected because srcInfo and destinationInfo contents indicate the multipoint ept (VSX) is calling itself.
2044-2046	Not assigned.
2047	Registration rejected because it was received from unauthorized media platform.
2048	Registration rejected because it is not ready for a media gateway re-registration.
2049	VOIP Resources unavailable.
2050	No gateway resource available.
2051	Remote Office invalid request (GRQ) No Sig Group available.
2052	Remote Office invalid registration request (RRQ) No Sig group available.
2053	MGKeepAlive: Wakeup() media platform heartbeat missed, indicates lack of traffic from specified platform.
2054	UMSocket: SockWrite() Congestion on the Signaling Link due to PCD buffer exhaustion.
2055	Reset the media platform Signaling Link due to error in Sending packets.
2058	IncomingMsg. Null caps received on terminating end of H323 trunk.
2059	Change of security code through Feature Access Code not supported for IP.
2061	Post message digit timeout.
2062	Post message too many digits.
2063	Post message not station user.
2064	Registration rejected because of failure to encode Non-standard Data (NSD) message.
2070	Media gateway attempted registration with “warm start” condition, but the controller needs “cold start” data.
2071	Media gateway attempted to register with a different serial number.
2072	Conference or transfer 2 Meet-me conference call.

3 of 4

Reason Codes for IPEVT (continued)

Reason Code	Explanation
2073	User attempted to download firmware to a station. User does not have console permission.
2074	Attempt to record an announcement while that announcement is playing.
2075	User does not have console permissions
2076	IP Registration Rejection (RRJ) because of no call present on the switch side. But there is a call present on the ept.
2077	Force Unregistration Request. Unregister endpoint whose call preservation timer (H323 link loss delay timer) expires.
2078	OPTIM Extend Call via extend call button press was denied.
2079	Registration rejected because set in wrong state (for example on call, Out of Service (OOS)).
2081	IP Softphone in shared control configuration with DCP is forced unregistered because softphone switched to invalid state.
2082	A TLS socket was rejected because of the constraint on the maximum number of TLS peers.
2083	A peer cert was rejected by common name checking.
2084	Handshake failed, for example due to no common cipher suite.
2085	An expired certificate was returned and rejected.
2088	Bad Record Max. For example, an attacker does not have the correct private key, which can go undetected until the MAC of the exchange is checked.
2089	Bad Record Max. For example, an attacker does not have the correct private key, which can go undetected until the MAC of the exchange is checked.
2090	TLS shutdown received. Listen socket could not be created.
2092	Post message invalid Station Security Code (SSC).
2093	Cannot start announcement.
2094	Establish a socket on an IP trunk. The far end might be mis-administered.
	4 of 4

Maintenance Tests

This section describes the maintenance tests which are executed, the meaning of the error codes, and how to troubleshoot and resolve problems.

If the recommended action does not solve the problem, escalate it to the next level.

Dial Tone Test (#0)

The Dial Tone Test attempts to seize a port and check for dial tone. This test is run on Analog CO Trunks.

Dial Tone Test (#0)

Error Code	Test Result	Description / Recommendation
	ABORT	Could not allocate system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. 1. Determine the service state of the port. If the service state indicates that the port is in use, wait until the port is idle before retesting. 2. Rerun the test at 1-minute intervals up to 5 times.
1001	ABORT	System resources required to run this test were not available. 1. Rerun the test at 1-minute intervals up to 5 times.
1002	ABORT	The system could not allocate time slots for the test. 1. Rerun the test at 1-minute intervals up to 5 times.
1004	ABORT	The port was seized by a user for a valid call. 1. Determine the service state of the port. If the port is in use, wait until the port is idle before retesting. 2. Rerun the test at 1-minute intervals up to 5 times.
		1 of 2

Dial Tone Test (#0) (continued)

Error Code	Test Result	Description / Recommendation
1005	ABORT	The trunk has been administered as incoming-only or DID trunk group type. Dial tone can only be obtained on outgoing trunks. Wrong configuration for this test. This error can be ignored.
2000	ABORT	Response from the test was not received within the time allowed. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The trunk was seized, but dial tone could not be detected. 1. Test another administered outgoing port on the media module. Failure of more than one port indicates a problem toward the CO. 2. If no service problems exist on the port, continue to use the port until the media module can be replaced as a last resort. Perform a trunk test call to see if the trunk is operable.
2002	FAIL	Seizure failed due to a hardware problem. The fault is usually caused by a disconnected trunk. 1. Check the trunk wiring to ensure good connection. Repeat the test. 2. If the test still fails, locate another identical CO trunk and swap its wiring with the one under test. Repeat the test on both trunks, and determine whether the problem follows the trunk or remains at the original port. If the problem follows the trunk, refer the problem to the CO. If the problem remains at the port, replace the media module and repeat the test.
	PASS	Trunk was seized and dial tone was detected. Investigate user-reported troubles on this port by examining the trunk or external wiring.
Any	NO BOARD	See NO BOARD for the repair procedures.
		2 of 2

CO Port Diagnostic Test (#3)

For ground start trunks, media module port relays are operated and checked to see if the port can detect and apply ground on the Tip lead. This test also verifies that there is no external ground on the Ring lead. In the absence of other failures, the media module should be replaced only if this test fails with the CO line disconnected.

This test also checks the on-board programmable transmission circuits that allow the media module to support transmission characteristics of several different countries.

This test runs on Analog CO Trunks.

CO Port Diagnostic Test (#3)

Error Code	Test Result	Description / Recommendation
	ABORT	Could not allocate system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1000 1004	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. 1. Determine the service state of the port. If the port is in use, wait until the port is idle before retesting. 2. Rerun the test at 1-minute intervals up to 5 times.
1005	ABORT	Test is not valid for the present configuration. This error can be ignored.
2000	ABORT	Response from the test was not received within the time allowed. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	Failure to detect ground or faulty ground detected on Ring lead. 1. Repeat the test. 2. If the test fails again, repeat the test with the CO line removed. 3. If the test fails, replace the media module. If the test passes, refer the problem to the CO.
	PASS	The port is able to apply ground for outgoing calls and detect ground for incoming calls. However, it does not provide information if a CO line is actually connected. Investigate user-reported troubles on this port by examining the trunk or external wiring.
0	NO BOARD	See NO BOARD for the repair procedures.

Digital Station Lamp Update (#16)

This test lights all lamps on the terminal as specified. The lamp updates run only if the station is in-service. The lamp updates are blocked from taking place if the station is not in the in-service state. This test does not affect the status of the Message Waiting lamp. This test runs on H.323 telephones.

Digital Station Audits Test (#16)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
1	ABORT	This port may have been busied out. 1. Determine the service state of the port. 2. Attempt to release the port. 3. Make sure the terminal is connected. 4. Rerun the test at 1-minute intervals up to 5 times.
3	ABORT	Station may be in ready-for-service or out-of-service state. 1. Verify the service state of the station. 2. Make sure the terminal is connected. 3. Rerun the test at 1-minute intervals up to 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. 1. Determine the service state of the port. If the port is in use, wait until it is idle before testing. Attendants are always in use (off-hook) if the handset is plugged in and the port is not busied out. 2. If the port status is idle, rerun the test at 1-minute intervals up to 5 times.
		1 of 2

Digital Station Audits Test (#16) (continued)

Error Code	Test Result	Description / Recommendation
	FAIL	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
	PASS	The message to light every station lamp was successfully sent to the port. 1. Observe the station lamps being lit when running the test. If all lamps do not light, the other test results may indicate related problems that do not allow the lamps to light. 2. Investigate troubles by examining the station, wiring, and connections.
		2 of 2

Digital Station Audits Test (#17)

This test is run on a station only if the station is in-service. The following audits are performed:

- Switch Hook Inquiry: This is an update of the server's software records based on the on-hook/off-hook status of the data module or voice terminal.
- Station ID Request: A request is made to the data module or station for its status. The data module or station returns its configuration and health information. This information is checked and a pass/fail result is provided.
- EPF inquiry: The test requests the status of the Electronic Power Feed.
- Bad Scan Inquiry: An uplink message is sent containing a count generated by certain events relating to the link conditions. This can be an indication of communication problems between the server and the media module.
- Ringer Update: This updates the ringer state according to the server's records.
- DTMP Administration Update: This sends a message to the digital station to refresh the default value that causes the station to send touch-tones only in the primary information channel. This value is initially set when the station is put in-service and each time the station's state changes from another state to in-service.

This test is run on H.323 telephones.

Digital Station Audits Test (#17)

Error Code	Test Result	Description / Recommendation
1	ABORT	Switch Hook Audit timed out. 1. Verify that the voice terminal is connected and repeat the test. 2. If the test aborts, replace the voice terminal and repeat the test.
2	ABORT	Station ID request failed or the health bit is defective. 1. Verify that the voice terminal is connected and repeat the test. 2. If the test aborts, replace the voice terminal and repeat the test.
3	ABORT	EPF Audit failed. 1. Verify that the voice terminal is connected and repeat the test. 2. If the test aborts, replace the voice terminal and repeat the test.
		1 of 3

Digital Station Audits Test (#17) (continued)

Error Code	Test Result	Description / Recommendation
4	ABORT	Bad Scan Inquiry failed. 1. Resolve any outstanding media module maintenance problems. 2. Rerun the test at 1-minute intervals up to 5 times.
5	ABORT	Ringer Update failed. 1. Verify that the voice terminal is connected. 2. Verify that the voice terminal is not busied out. 3. Repeat the test. 4. If the test continues to abort, replace the voice terminal and repeat the test.
6	ABORT	Touch-tone update failed. 1. Rerun the test at 1-minute intervals up to 5 times.
7	ABORT	Downloadable parameter downlink failed. 1. Rerun the test at 1-minute intervals up to 5 times.
8	ABORT	Terminal Levels Audit failed (Digital Stations only). 1. Verify that the voice terminal is connected and repeat the test. 2. If the test aborts, replace the voice terminal and repeat the test.
1000	ABORT	System resources required to run this test are not available. 1. Rerun the test at 1-minute intervals up to 5 times.
1706	ABORT	IP endpoint is not registered. 1. Verify the IP phone is connected. 2. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the time allowed. 1. Rerun the test at 1-minute intervals up to 5 times.
2100	ABORT	Internal error. 1. Rerun the test at 1-minute intervals up to 5 times.
		2 of 3

Digital Station Audits Test (#17) (continued)

Error Code	Test Result	Description / Recommendation
	FAIL	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
	PASS	The audits passed. 1. If complaints still exist, investigate by using other port tests and by examining the wiring and connections.
		3 of 3

Port Diagnostic Test (#35)

The battery feed chip provides power to the telephone equipment, signaling, transmission, and balance. This test checks the signaling and switch hook capabilities of the battery feed chip by terminating the port, applying battery, and trying to detect a current.

This test is run on Analog Telephones.

Port Diagnostic Test (#35)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 5 times.
1000	ABORT	System resources required to run this test are not available. The port may be busy with a valid call. 1. Determine the service state of the port. If the port is in use, wait until it is idle before testing. 2. If the port status is idle, retest the port. 3. If the test continues to abort, check for wiring errors toward the CO which may cause the trunk to lock up. 4. If the wiring is good, reset and retest the port. 5. If the test continues to abort, replace the media module.
		1 of 2

Port Diagnostic Test (#35) (continued)

Error Code	Test Result	Description / Recommendation
1004	ABORT	The port was seized by a valid call during the test. 1. Determine the service state of the port. If the port is in use, wait until it is idle before testing. Attendants are always in use (off-hook) if the handset is plugged in and the port is not busied out. 2. Rerun the test at 1-minute intervals up to 5 times.
1005	ABORT	The test is not applicable for this type of port. This error can be ignored.
2000	ABORT	Response from the test was not received within the time allowed. 1. Rerun the test at 1-minute intervals up to 5 times.
2012	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The port's battery feed chip is unable to supply sufficient power to the terminal equipment. This may occur when the test is performed at the same time the terminal equipment goes off-hook. 1. Determine the service state of the port. If the port is in use, wait until it is idle before testing. 2. Rerun the test at 1-minute intervals up to 5 times. 3. If the test continues to fail, determine whether the customer is experiencing problems on this line. Replace the media module only if the customer is experiencing problems.
	PASS	The port’s battery feed chip is able to provide power to the station equipment to detect on-/off-hook. 1. If touch-tones are not heard when buttons are pressed, replace the media module. 2. Investigate user-reported troubles on this port by using other port tests, by examining station wiring, or by examining the station. 3. If problems continue, refer the problem to the CO.
0	NO BOARD	See NO BOARD for the repair procedures.

2 of 2

Port Audit and Update Test (#36)

The Port Audit and Update Test sends port level translation data from the switch processor to the media module to verify that the port's translation and current state are correct.

When the ringer is in the off state, this test also turns off the station's ringer to prevent constant ringing caused by defective hardware.

This test runs on the following system components:

- Digital CO Trunks
- Analog CO Trunks
- Digital DID Trunks
- Analog DID Trunks
- ISDN PRI B-Channels
- Digital TIE Trunks

Port Audit and Update Test (#36)

Error Code	Test Result	Description / Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1000	ABORT	System resources required to run this test were not available. 1. Determine the service state of the port. If the port is in use, wait it is idle before retesting. 2. If the port is idle, rerun the test at 1-minute intervals a maximum of 5 times.
1004	ABORT	The port was seized by a valid call during the test. 1. Determine the service state of the port. If the port is active, wait until it is idle. 2. Rerun the test at 1-minute intervals up to 5 times. 3. If the test continues to abort and the port is not in use, escalate the problem.
1005	ABORT	This test is not applicable for this type of port. Ignore this error.
		1 of 2

Port Audit and Update Test (#36) (continued)

Error Code	Test Result	Description / Recommendation
1006	ABORT	The port has been busied out and is out of service 1. Verify the service state of the port. If the port is out of service, determine why. If it is OK to put the port back in service, release the port and retry the test.
2000	ABORT	Response to the test was not received within the time allowed. 1. Retest the port at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Retest the port at 1-minute intervals up to 5 times.
	FAIL	Possible internal software failure. 1. Retest the port at 1-minute intervals up to 5 times.
1	FAIL	This failure does not indicate a hardware problem. This condition may occur when the switch hook audit is performed at the same time that the terminal equipment goes off-hook. 1. Determine when the port is available for testing. 2. When the port becomes available for testing, rerun the test at 1-minute intervals up to 5 times.
5	FAIL	Message Waiting Lamp update failed. Possible internal software error. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
7	FAIL	Translation update failed. Possible internal software error. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
8	FAIL	Ringer update failed. Possible internal software error. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
	PASS	The software and the port processor have the same status. Investigate user-reported troubles on this port by running other port tests, examining the wiring, or by inspecting the station.
0	NO BOARD	See NO BOARD for the repair procedures.

2 of 2

ONS Ringer Application Test (#48)

The Ringing Application Test applies momentary ringing voltage to the terminal equipment to determine if the terminal equipment is connected to the port. The test may cause some terminal equipment to ring briefly during daily maintenance.

This test is run on Analog Telephones.

ONS Ringer Application Test (#48)

Error Code	Test Result	Description / Recommendation
	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1000 1004	ABORT	System resources required to run this test are not available. 1. Determine the service state of the port. If the port is in use, wait until the port is idle. 2. Retest the port at 1-minute intervals up to 5 times.
1004	ABORT	The port was seized with a valid call during the test. 1. Determine the service state of the port. If the port is in use, wait until the port is idle. 2. Retest the port at 1-minute intervals up to 5 times.
1005	ABORT	This test is not applicable for this type of port. This error can be ignored.
1008	ABORT	Could not allocate a ringing circuit. Every ringing circuit may be in use. 1. Retest the port at 1-minute intervals up to 5 times. 2. Test other ports on the media module. If ABORT 1008 does not occur on other ports, then all four ring phases are in use.
2000	ABORT	Response to the test was not received within the time allowed. 1. Retest the port at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate necessary system resources to run this test. 1. Retest the port at 1-minute intervals up to 5 times.

1 of 2

ONS Ringer Application Test (#48) (continued)

Error Code	Test Result	Description / Recommendation
	FAIL	The terminal equipment is not connected to the media module. Some terminal equipment may fail even when connected properly. 1. Remotely test the equipment. 2. Check all of the wiring between the station equipment and the switch. Run the test again. 3. If the test still fails, the set may be defective. Check the set and replace it, if necessary.
	PASS	The station is connected properly. This test may also pass if no terminal equipment is connected and the terminal is located very far from the switch. Investigate user-reported troubles on this port by using other port tests, examining station wiring, or examining the station.
0	NO BOARD	See NO BOARD for the repair procedures.
		2 of 2

Control Channel Looparound Test (#52)

The Control Channel Looparound test queries a media module for its board code and vintage to check the operation of the control channel and media module communication.

The test passes if the media module responds with the correct media module code and vintage. The test aborts if there is no response. The test fails otherwise.

Control Channel Looparound Test (#52)

Error Code	Test Result	Description / Recommendation
2000	ABORT	Response from the test was not received in the time allowed. 1. Rerun the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate needed system resources. 1. Rerun the test at 1-minute intervals up to 5 times.
2500	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The media module failed to return its board code or vintage. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to fail, reset the media module, then retest the media module. 3. If the test continues to fail, replace the media module.
	PASS	The media module is communicating correctly with the switch.
0	NO BOARD	See NO BOARD for the repair procedures.

Loss of Signal Alarm Inquiry Test (#138)

The Loss of Signal Alarm Inquiry Test verifies the synchronization status, echo cancellation, and continuity of the DS1 link.

A Loss of Signal Alarm indicates that the media module is unable to derive the synchronization clock from the DS1 facility. If the media module is administered as a timing source, and it detects a Loss of Signal alarm, the media module will stop providing the synchronization clock for the system and will transmit a Yellow alarm to the remote DS1 endpoint.

When the Loss of Signal alarm is confirmed, every trunk or port of the media module is put into the out-of-service state. The inquiry test will run every 10 minutes until the loss of signal has been restored.

Loss of Signal Alarm Inquiry Test (#138)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The media module detects a Loss of Signal alarm. The physical link is broken or the remote DS1 endpoint is down. All trunks or ports of this media module are out-of-service. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
1400 1401	FAIL	The Echo Canceller function failed. This could be a hardware problem on the media module. 1. Reset the media module. 2. Retest the media module. 3. If Test 138 still fails, replace the media module.
	PASS	DS1 signal is present and the physical link is healthy.
0	NO BOARD	See NO BOARD for the repair procedures.

Blue Alarm Inquiry Test (#139)

A Blue Alarm is a signal sent by the remote DS1 endpoint when it is out-of-service. The Blue Alarm Inquiry Test checks the Blue Alarm status of the remote DS1 endpoint.

When a local DS1 media module detects a Blue Alarm signal from the remote DS1 endpoint, it transmits a Yellow Alarm to the remote DS1 endpoint and sends a BLUE ALARM message to the system. When the Blue Alarm is confirmed, the system places all trunks or ports of the DS1 media module into the out-of-service state. The inquiry test runs every 10 minutes until the Blue Alarm is cleared.

When the Blue Alarm is cleared, the DS1 media module stops transmitting the Yellow alarm and places the trunks or ports back into the service state they were in before the Blue Alarm occurred.

Blue Alarm Inquiry Test (#139)

Error Code	Test Result	Description/ Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals for a maximum of 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals for a maximum of 5 times.
	FAIL	The remote DS1 endpoint is out-of-service. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	Remote DS1 endpoint is in-service.
0	NO BOARD	See NO BOARD for the repair procedures.

Red Alarm Inquiry Test (#140)

The Red Alarm Inquiry Test checks the framing status of the DS1 Interface media module.

A DS1 Interface Media Module raises a Red alarm when the framing pattern of the incoming DS1 bit stream has been lost. When the DS1 media module detects a Red Alarm, it transmits a Yellow Alarm to the remote DS1 endpoint and sends a Red Alarm message to the system. After the Red Alarm is confirmed, the system places every trunk or port of the DS1 media module into the out-of-service state. The inquiry test runs every 10 minutes until the Red Alarm is cleared.

When the Red Alarm is cleared, the DS1 media module stops transmitting the Yellow alarm to the remote DS1 endpoint. The system restores all trunks or ports of the DS1 media module to the service state they were in before the Red Alarm occurred.

Loss of Multiframe Alarm

If the DS1 media module is administered using DMI-BOS signaling, it raises a LMA (Loss of Multiframe Alarm) when it cannot interpret the incoming signaling bits to synchronize to the multiframe pattern received in the 24th channel. Once the DS1 media module detects an LMA, the media module transmits a RMA (Remote Multiframe Alarm) to the remote DS1 endpoint.

Loss of Multiframe Alarm (#140)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate resources for this test. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The DS1 media module detected a Red Alarm. An out-of-frame condition occurred. The DS1media module will transmit a Yellow Alarm to the remote DS1 endpoint until the Red Alarm is retired. 1. f the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures

1 of 2

Loss of Multiframe Alarm (#140) (continued)

Error Code	Test Result	Description / Recommendation
1	FAIL	The DS1 media module detected a loss of multiframe alarm (LMA). An out-of-frame condition occurred on the DS1 media module. The DS1 media module will transmit a remote multiframe alarm (RMA) to the remote DS1 endpoint until the LMA is retired. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	No Red alarm was detected on the DS1 media module.
0	NO BOARD	See NO BOARD for the repair procedures.
		2 of 2

Yellow Alarm Inquiry Test (#141)

This test runs on the DS1 Interface media module. The Yellow Alarm Inquiry Test determines whether the remote DS1 endpoint is transmitting a Yellow alarm. A Yellow Alarm indicates that the remote DS1 endpoint has an out-of-frame condition.

Once the Yellow alarm is confirmed, all trunks on the DS1 media module are put into the out-of-service state. The Inquiry test will be run every 10 minutes until the Yellow Alarm is cleared. When the Yellow Alarm is cleared, all trunks on the DS1 media module are restored back to their previous service state before the Yellow Alarm was raised.

The Yellow Alarm corresponds to the yellow F2 state documented in CCITT recommendation I.431.

Remote Multiframe Alarm

A Remote Multiframe Alarm (RMA) indicates that the remote DS1 endpoint is in a Loss of Multiframe Alarm condition while the DS1 media module is administered using the DMI-BOS common-channel signaling. The RMA is handled as a Yellow alarm.

Yellow F5 State Alarm

For 32-channel E1 operation with CRC4 on, the F5 fault state is defined as a fault in the user-network interface, specifically in the direction from the user to the network. Refer to CCITT recommendation I.431

Yellow Alarm Inquiry Test (#141)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Retry the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The DS1 interface media module detected a yellow alarm sent by the remote DS1 endpoint. An out of frame condition occurred at the DS1 endpoint. 1. f the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
1	FAIL	The DS1 Interface media module detected a Remote Multiframe Alarm sent by the remote DS1 endpoint. An out-of-frame condition occurs on the remote DS1 endpoint. 1. f the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
2	FAIL	The DS1 Interface media module is reporting a yellow F5 State alarm. There is a fault in the user-network interface from the user to the network. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	No Yellow alarm or Remote Multiframe Alarm or F5 State Alarm was received from the remote DS1 endpoint.
0	NO BOARD	See NO BOARD for the repair procedures.

Major Alarm Inquiry Test (#142)

This test runs on the DS1 Interface media module. The Major Alarm Inquiry Test determines if the received average DS1 bit error rate on the DS1 facility is greater than 1/1000. All trunks on the DS1 media module are put in the out-of-service state if a Major Alarm lasts for more than 20 minutes.

When the Major Alarm is cleared, all trunks on the DS1 media module are restored to their previous service state before the Major Alarm occurred.

Major Alarm Inquiry Test (#142)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	The DS1 Interface media module detects a Major alarm. The DS1 bit error rate is greater than 1/1000. The performance of the DS1 link between the DS1 media module and the remote DS1 endpoint is very poor. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	No Major alarm was detected on the DS1 media module.
0	NO BOARD	See NO BOARD for the repair procedures.

Minor Alarm Inquiry Test (#143)

This test runs on the DS1 Interface media module. The Minor Alarm Inquiry test determines if the received DS1 bit error rate is greater than 1/1,000,000 and less than 1/1000.

Every trunk or port on the DS1 media module is kept in the in-service state after the Minor Alarm is confirmed. The Minor Alarm Inquiry test runs every 10 minutes until the Minor Alarm is cleared.

Minor Alarm Inquiry Test (#143)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	A Minor Alarm was detected. The performance of the DS1 link between the DS1 media module and the remote DS1 endpoint is poor. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	No Minor Alarm was detected on the DS1 media module.
0	NO BOARD	See NO BOARD for the repair procedures.

Slip Alarm Inquiry Test (#144)

Slips occur when the transmitter and receiver are not running at precisely the same clock rate. The DS1 Interface media module can detect both positive and negative slips on the DS1 facility. The Slip Alarm Inquiry Test displays the total number of slips that have occurred on a DS1 link if there are any.

Slip Alarm Inquiry Test (#144)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1 to 88	FAIL	The DS1 media module detected a slip alarm. The Error Code value is the number of slips detected since the last slip alarm inquiry test. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	No Slip Alarm was detected on the DS1 media module.
0	NO BOARD	See NO BOARD for the repair procedures.

Misframe Alarm Inquiry Test (#145)

A Misframe Alarm indicates that framing bits observed on a DS1 media module are in error. The Misframe Alarm Inquiry test queries the total number of misframes that have occurred on a DS1 media module since the last inquiry.

If the DS1 media module is supplying the system synchronization source when the threshold of misframes is reached, a Minor Alarm against the DS1 media module is raised, but every trunk or port of the DS1 media module remains in the in-service state.

Misframe Alarm Inquiry Test (#145)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Retry the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
ANY	FAIL	The DS1 media module detected errors in the received framing bits pattern. The Error Code value is the number of misframes detected since the last misframe alarm inquiry test. Major bit and minor bit error rate errors often accompany misframe alarms. Clearing the cause of these errors may clear the misframes which are occurring. 1. If the DS1 media module connects to a T1 network facility or to another switch, see T1 Network Facility Procedures
	PASS	No Misframe Alarm was detected on the DS1 media module.
0	NO BOARD	See NO BOARD for the repair procedures

DS1 Translation Update Test (#146)

The DS1 Translation Update Test sends the board-level information specified by System Administration to the DS1 Interface media module. Translation includes the following data: DS1 Link Length between two DS1 endpoints, Synchronization Source Control, All Zero Suppression, Framing Mode, Signaling Mode, Time Slot Number of 697-Hz Tone, Time Slot Number of 700-Hz Tone, etc.

DS1 Translation Update Test (#146)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	Internal system software error. 1. Verify the DS1 media module translation. 2. Rerun the test at 1-minute intervals up to 5 times.
	PASS	Translation data has been downloaded successfully to the DS1 media module.
0	NO BOARD	See NO BOARD for the repair procedures.

Link Tear Down Test (#213)

This test is destructive.

This test disconnects the existing TCP link between the system and the external output device. If the link has already been disconnected, this test just returns PASS.

Link Tear Down Test (#213)

Error Code	Test Result	Description / Recommendation
40	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
50	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
1010	ABORT	The CDR link has been busied out and is out-of-service. 1. Release the CDR link from the busyout state. 2. Retest the CDR link.
2012	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
	FAIL	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
	PASS	The CDR link was successfully torn down.

Link Retry Test (#215)

This test sends a message to the output device to make a data call to the extension where the output device connects. If the link is already up, this test passes without making any data call.

Link Retry Test (#215)

Error Code	Test Result	Description / Recommendation
10	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
20	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
30	ABORT	Internal system error. 1. See CDR Link Troubleshooting Procedures.
1010	ABORT	The link has been busied out and is out-of-service. 1. Release the CDR link from the busyout state. 2. Retest the CDR link.
2012	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
	FAIL	The link cannot be established. 1. See CDR Link Troubleshooting Procedures for instructions.
	PASS	The CDR link is up.

Signaling Link State Audit Test (#255)

This test checks the state of critical signaling link hardware components as required by the ISDN PRI B-Channel.

Signaling Link State Audit Test (#255)

Error Code	Test Result	Description / Recommendation
None or 0	ABORT	Internal system error. 1. Rerun the test up to 5 times at 1-minute intervals.
1114	ABORT	The signaling link is in a transitional state 1. Rerun the test up to 5 times at 1-minute intervals.
4	FAIL	There is a problem with the signaling channel. 1. Test the media module or platform. Resolve any problems. 2. Check for transmission problems and resolve if any are found. 3. Retest the port.
8	FAIL	There is a problem with the media module. 1. Verify that the media module is physically inserted and administered. 2. Reset the media module. 3. Rerun the test. 4. If the test fails again with this Error Code, replace the media module.
	PASS	The signaling link hardware is working properly.

Service State Audit Test (#256)

This test performs a service state audit with the far-end terminal adapter to ensure both sides agree on the service state.

If no reply is received within 2 minutes, the system will automatically try once again. If that attempt fails, the system will then attempt recovery by automatically retrying approximately every 15 minutes. If the port was initially in the INS (in-service) state, it will now be placed in the

MTC/FE (maintenance state, far-end problem) state. Until a Service State audit attempt is successful, no outgoing calls will be placed over this port, but incoming calls will be accepted. The service state of this port does not affect the service state of other ports. If an incoming call that uses this port is presented while in such a state, a Service State audit attempt will immediately be attempted (that is, the system will not wait for the 15-minute cycle, but will instead try to recover immediately).

PASS for this test only means that a message to the far end was successfully sent.

This test is run on ISDN PRI B-Channels and ISDN BRI trunks.

Service State Audit Test (#256)

Error Code	Test Result	Description / Recommendation
1000	ABORT	Needed resources not available, or the port is on a call or initializing. 1. Verify the service state of the port. If the port is in-service, wait until it is idle. 2. Rerun the test at 1-minute intervals up to 5 times.
1005	ABORT	This test does not run on this type of port. This error can be ignored.
1113	ABORT	Signaling link failed 1. Test the trunk and check the results of either the Signaling Link State Audit Test (#255) or the Signaling Link State Test (#1251).
1114	ABORT	Signaling link in transitional state 1. Rerun the test up to 5 times at 1-minute intervals.
1116	ABORT	The trunk is not in a service state which is appropriate for running the test. This test is only performed in the OOS/FE state. 1. Verify the service state of the trunk and rerun the test.
1117	ABORT	A service state audit message is outstanding 1. Wait 2 minutes, then test the port again.
2100	ABORT	Could not allocate needed resources 1. Rerun the test up to 5 times at 1-minute intervals.
	FAIL	Internal system error 1. Rerun the test up to 5 times at 1-minute intervals.
		1 of 2

Service State Audit Test (#256) (continued)

Error Code	Test Result	Description / Recommendation
	PASS	Wait 4 minutes, then check the service state of the port. 1. If the port is in-service, the negotiation succeeded. 2. If the port is in the MTC/FE (maintenance far-end) state, the negotiation failed. The system will automatically retry the test approximately every 15 minutes. Incoming calls will be accepted, but no outgoing calls will be originated on this port. If an incoming call is presented, another Service State audit will be immediately performed in an attempt to bring the port into the proper state.
		2 of 2

Call State Audit Test (#257)

This test audits internal call state data by querying the far-end terminal adapter as to the ISDN state of the call. This can be helpful when trying to clear a hung call. If a call is active on the port, the switches on both sides of the connection should agree on the ISDN state of the call as defined in the ISDN Protocol Specification. If the internal call state data on the near-end switch is different than that of the far-end terminal adapter, the call will be torn down.

The ISDN specification allows up to 2 minutes for a reply. If a reply is not received within the 2 minute window, the test logs a protocol time-out violation against the associated signaling channel. This test is run on ISDN PRI B-Channels and ISDN BRI trunks.

Call State Audit Test (#257)

Error Code	Test Result	Description / Recommendation
1019	ABORT	Audit already in progress 1. Wait 2 minutes, and try again.
1113	ABORT	Signaling link failed 1. Test the trunk and check the results of either the Signaling Link State Audit Test (#255) or the Signaling Link State Test (#1251).
1114	ABORT	Signaling link in transitional state 1. Rerun the test up to 5 times at 1-minute intervals.
		1 of 2

Call State Audit Test (#257) (continued)

Error Code	Test Result	Description / Recommendation
1116	ABORT	The trunk is in an out-of-service ISDN service state. A call cannot be made if the trunk is in this state. No action is necessary. 1. Verify the trunk service state.
2100	ABORT	Could not allocate needed resources 1. Rerun the test up to 5 times at 1-minute intervals.
	FAIL	Internal system error 1. Rerun the test up to 5 times at 1-minute intervals.
	PASS	A call-state auditing message was successfully sent to the far-end terminal adapter to verify the state of the call active on this port. If a call-state mismatch is found, the call is torn down within two minutes. If no call was active, no message was sent.
		2 of 2

Clear Error Counters (#270)

This test is not an actual test in the strict sense of the word.

The ports on the media module continually run self-tests whenever the port is idle. An on-board counter is incremented for each failure. This test clears the counter so that if the port continues to fail during or after testing, the system can take the appropriate action (log or alarm the failure, initiate other tests).

This test should never abort or fail. It is run on ISDN BRI ports.

Clear Error Code Counters (#270)

Error Code	Test Result	Description / Recommendation
Any	ABORT	This test should never abort. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to abort, escalate the problem.
		1 of 2

Clear Error Code Counters (#270) (continued)

Error Code	Test Result	Description / Recommendation
Any	FAIL	This test should never fail. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
	PASS	The message to clear the media module's counter for Background Maintenance Failures has been sent successfully.
		2 of 2

LANBIC Receive Parity Error Counter Test (#595)

This test reads and clears the LANBIC Receive Parity Error Counter on the BRI media module. This counter is incremented by the media module when it detects a parity error in data received from the packet bus.

These errors may indicate a media module problem, packet bus problem, or a problem with another media module on the bus. This test is useful for verifying the repair of the problem.

LANBIC Receive Parity Error Counter Test (#595)

Error Code	Test Result	Description / Recommendation
2000	ABORT	Response to the test was not received within the allowed time. 1. Retest the media module at 1-minute intervals up to 5 times. 2. If the test aborts repeatedly up to five times, reset the media module and retest. 3. If the test aborts again with Error Code 2000, replace the media module.
		1 of 2

LANBIC Receive Parity Error Counter Test (#595) (continued)

Error Code	Test Result	Description / Recommendation
2012	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Retry the command at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
2500	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
1–10	FAIL	The media module detected parity errors. The error code indicates the value of the on-board error counter. 1. Retry the command at 1-minute intervals up to 5 times. 2. If the test continues to fail, escalate the problem.
	PASS	No errors were detected by media module.
		2 of 2

CRC Error Counter Test (#623)

This test reads the port's CRC error counters that are maintained on the media module. The Cyclic Redundancy Check (CRC) is a means of error detection to determine the integrity of data frame contents. The CRC error counter is incremented by the media module when it detects a CRC error. The test passes if the value of the counter is 0, meaning the error is cleared. If the counter is non-zero, the test fails and the value of the counter is displayed in the `Error Code` field.

This test is run on ISDN BRI ports.

CRC Error Counter Test (#623)

Error Code	Test Result	Description / Recommendation
2000	ABORT	Response was not received from the media module within the allowed time. 1. Rerun the test 5 times. 2. If the test aborts repeatedly up to 5 times, reset and retest the media module. 3. If the test aborts again, replace the media module.
2012 2100	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
Any	FAIL	The media module is detecting CRC errors. The **Error Code** field contains the value of the counter. This error occurs when a frame with a bad CRC is received over the D-Channel by the media module. The problem is most likely due to a problem with the wiring to the set or adjunct, interference on the wiring caused by a noise source such as an electrical motor or generator, or no termination (open circuit). It usually does not indicate a problem with the media module.
	PASS	The error counter was cleared successfully.

Receive FIFO Error Counter Test (#625)

This test reads and clears the port's Receive FIFO error counter maintained on the media module. This counter is incremented by the media module when it detects an overflow of its receive buffers. The test passes if the value of the counter is 0 (that is, the error is cleared). If the counter is not zero, the test fails, and the value of the counter is displayed in the Error Code field.

This error can occur if signaling frames are being received from a packet bus at a rate sufficient to overflow the receive buffers on the media module for a port or if a hardware fault is causing the receive buffers not to be emptied properly. This test is useful for verifying the repair of the problem.

This test is run on ISDN BRI ports.

Receive FIFO Error Counter Test (#625)

Error Code	Test Result	Description / Recommendation
2000	ABORT	Response to the test was not received within the allowed time. 1. Retest the media module at 1-minute intervals up to 5 times. 2. If the test aborts repeatedly up to 5 times, reset the media module and retest. 3. If the test aborts again, replace the media module.
2012	ABORT	Internal system error. 1. Retest the media module at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate necessary system resources to run test. 1. Retest the media module at 1-minute intervals up to 5 times.
Any	FAIL	The media module is detecting errors. The Error Code field contains the value of the counter. 1. Retest the media module at 1-minute intervals up to 5 times. 2. If the test continues to fail, review the results of other tests in the test sequence. Note the results of the Receive FIFO Error Counter (#625) test. Follow the repair procedures for any of the tests that fail. 3. If the tests for the endpoints pass and the Receive FIFO Error Counter test continues to fail, check the wiring to the endpoints, then retest.
	PASS	The Receive FIFO error counter has a value of 0 and the test passed.

Primary Signaling Link Hardware Check (#636)

The ISDN-PRI Signaling Group D-Channel port depends on the health of the DS1 Interface Media Module on which it resides. This test will fail if there are problems with either the ISDN-PRI Primary D-Channel port or the DS1 Media Module.

Primary Signaling Link Hardware Check (#636)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
8	FAIL	There is a problem with the DS1 Interface Media Module or the ISDN-PRI Signaling Channel (D-Channel). No ISDN trunk or PRI endpoint calls can be made until the problem is resolved. 1. Verify that the media module is physically inserted and administered. 2. Check for transmission problems and resolve if any are found. 3. Reset the media module. 4. Rerun the test. 5. If the test fails again with this error code, replace the media module.
	PASS	The basic physical connectivity of the primary D-Channel is intact and functional. Try this test repeatedly to ensure the link is up and to uncover any transitory problems.
0	NO BOARD	See NO BOARD for the repair procedures.

Remote Layer 3 Query (#637)

This test checks the health of the D-Channels and DS1 media modules. It will query the far-end switch or terminal adapter to determine whether the signaling connection is functioning properly at Layer 3. It will select a B-Channel in the in-service or maintenance service state and send an ISDN layer-3 SERVice message, which requires a response from the far end. The test will not be performed if there are no B-Channels in an appropriate ISDN service state (as when none are administered or they are all out of service).

A PASS result indicates only that a message was successfully sent to the far-end switch or terminal adapter. The ISDN PRI Specification allows up to two minutes for a response.

This test checks the communication path from the processor through the media module, and on to the far-end switch or terminal adapter. It ensures that the communication path between the switch and the far-end is up and operational, and that the two endpoints can properly exchange ISDN control messages.

Remote Layer 3 Query (#637)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error. 1. Rerun the test a 1-minute intervals up to 5 times.
1006	ABORT	This is a NORMAL ABORT. There are no associated B-Channels in an ISDN in-service or maintenance service state. For country protocol 1 interfaces (including the USA), this error means either: • there are no B-Channels administered in this signaling group • all B-Channels in this signaling group are out-of-service or are in a “pending” state (PINS or PMTC, indicating that a B-Channel maintenance message for that B-Channel has been sent and not yet acknowledged). 1. Administer or release an ISDN trunk or PRI endpoint. Then, retry this test when at least one B-Channel is in the in-service or maintenance state. For systems not using country protocol 1 interfaces, there are no B-Channels administered in this signaling group.
1019	ABORT	There is already a Remote Layer 3 Query in progress. 1. Wait two minutes, then follow the procedures for when this test passes.
1113	ABORT	The signaling channel is down. Therefore, no messages can be sent to the far-end switch or terminal adapter. 1. Examine the results of the Primary Signaling Link Hardware Check (#636) and the Signaling Link Board Check (#643) and follow recommendations provided there.

1 of 2

Remote Layer 3 Query (#637) (continued)

Error Code	Test Result	Description / Recommendation
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
2500 or none	ABORT	Internal system error **or** administration problem 1. Determine whether any B-Channels are administered. If not, then this is a normal ABORT since this test cannot run unless at least one B-Channel is administered. If at least one B-Channel is administered, there is an internal system error. Rerun the test at 1-minute intervals up to 5 times.
	FAIL	Internal system error. 1. Determine whether any B-Channels are administered. If not, then this is a normal ABORT since this test cannot run unless at least one B-Channel is administered. If at least one B-Channel is administered, there is an internal system error. Rerun the test at 1-minute intervals up to 5 times.
	PASS	A message was sent to the far-end switch or terminal adapter. The ISDN PRI specification allows up to 2 minutes for a reply. 1. If there is still a problem with a particular ISDN trunk or PRI endpoint, busyout the trunk and retest the port.
0	NO BOARD	See NO BOARD for the repair procedures.
		2 of 2

Signaling Link Board Check (#643)

This test checks the health of the critical DS1 Interface media module hardware components required by the signaling link.

Signaling Link Board Check (#643)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
8	FAIL	The media module is not in service. 1. Verify the service state of the media module. 2. Retest the media module.
	PASS	The media module transporting the ISDN-PRI Signaling Link Port is in service.
Any	NO BOARD	See NO BOARD for the repair procedures.

Layer 2 Status Query Test (#647)

The Layer 2 Status Query Test checks the Layer 2 status of the ISDN-PRI Signaling Channel (D-Channel). This test will fail if there is a hardware failure or a facility problem, or if the primary ISDN-PRI D-Channel is not administered correctly.

The Primary Link Hardware Test (#636) and the Remote Layer 3 Query Test (#637) will detect most problems caused by hardware failures or incorrect administration.

Layer 2 Status Query Test (#647)

Error Code	Test Result	Description / Recommendation
1132	ABORT	The port location for the D-Channel is not known. This condition should not be possible since an administered media module must be specified when a Signaling Group is administered: 1. Rerun the test at 1-minute intervals up to 5 times.
1134	ABORT	The associated media module is not administered. This condition should not be possible since an administered media module must be specified when a Signaling Group is administered. 1. Rerun the test at 1-minute intervals up to 3 times.
2500	ABORT	Internal system error: 1. Rerun the test at 1-minute intervals up to 5 times.
1	FAIL	Layer 2 of the primary signaling channel is down: 1. Examine the results of the Primary Signaling Link Hardware Check (#636), and follow recommendations provided there. 2. If Test #636 passes, the Layer 2 Query test may still fail if the signaling channel at the far end has not been administered correctly or if the signaling channel has been busied out. a. Verify that the Primary Signaling Channel (D-Channel) at the far end has been administered correctly. b. Verify that the port used for the Primary D-Channel has not been busied out at the far end.
3	FAIL	The D-Channel is down. 1. Examine the results of the Primary Signaling Link Hardware Check (#636) and follow the recommended procedures if the test fails. 2. If Test #636 passes, the Layer 2 Query test may still fail if the signaling channel at the far end has not been administered correctly or if the signaling channel has been busied out. a. Verify that the D-Channel at the far end has been administered correctly. b. Verify that the port used for the D-Channel has not been busied out at the far end.
	PASS	The Primary Signaling Channel is up.
Any	NO BOARD	See NO BOARD for the repair procedures.

Level 1 Status Query Test (#1242)

This test determines the state of the transmission facility of a BRI port at the Level 1 (L1) physical layer: Activated, Pending Activation, or Deactivated.

The Activated state is the correct state for an ISDN-BRI port. In this state, the L1 interface can send and receive synchronized signals. This test passes if the state of L1 is Activated. This test also passes if software has taken this port out of service. See the description of the L1 “Deactivated State” below for more details.

The Pending Activation state indicates a problem with the channels, the wiring, or the DS1 Interface media module. When in this state, the Level 1 interface is either not receiving any L1 framing from the channel or it is communicating with the channel but cannot transition to the Activated state.

The Deactivated state indicates a problem with the DS1 Interface media module. When in this state, either the Level 1 interface is not active, an idle signal is transmitted to the channels, or Layer 1 was deactivated by the switch. When a port is placed in the out-of-service state, Level 1 is also put into the Deactivated state. This could be due either to the system detecting a fault with the port or the port was manually busied out.

Level 1 Status Query Test (#1242)

Error Code	Test Result	Description / Recommendation
1187	ABORT	The media module or port may be busied out. 1. Look in the Alarms list and check if this port or media module is busied out. If the port or media module is busied out, release it. **CAUTION:** When you release a media module, you release every port associated with it. If certain ports still need to be busied out, use the busyout action for that port. 2. Make sure the endpoint is connected. 3. Retry the command at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Test the media module at 1-minute intervals up to 5 times. 2. If the test aborts repeatedly up to 5 times, reset the media module. 3. Rerun the test. If the test aborts again with this error code, replace the media module.
		1 of 3

Level 1 Status Query Test (#1242) (continued)

Error Code	Test Result	Description / Recommendation
2012	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1	FAIL	Received a status of Level 1 Pending Activation. U interface is down, indicating a problem with a connection between the switch and the NT1. 1. Verify that the connections between the switch and the NT1 are good. Verify that the NT1 has power. 2. Test the port and review the results of the Level 1 Status Query Test #1242 to verify the repair. 3. If this test still fails, follow the manufacturer's repair procedures for the NT1. Then test the port and review the results of the Level 1 Status Query test to verify repair.
2	FAIL	Received a status of Level 1 Pending Activation. U interface up, S/T interface down, which indicates a problem with the NT1 or the wiring between the NT1 and the BRI endpoint (S/T interface). 1. Test the port and review the results of the Level 1 Status Query test to verify the repair. 2. If this test still fails, follow the manufacturer's repair procedures for the NT1. Then test the port and review the results of the Level 1 Status Query test to verify repair.
3	FAIL	Received a status of Level 1 Deactivated. The port is out-of-service. 1. Determine the service state of the port to verify that the port is out-of-service. If the service state of the port is not out-of-service, escalate the problem to the next tier. 2. If the port has been busied out, try releasing the port. Then retest the port and review the results of Level 1 Status Query test. 3. If this test still fails, follow the repair procedures for any test that fails. Retest the port and note the results of the Level 1 Status test. If the test continues to fail for this reason, escalate the problem.

2 of 3

Level 1 Status Query Test (#1242) (continued)

Error Code	Test Result	Description / Recommendation
4	FAIL	Received a status of Level 1 Pending Activation. The NT1 has a loss of power indicating a problem with the NT1. 1. Follow the manufacturer's repair procedures for the NT1. 2. Test the port and review the results of the Level 1 Status Query test to verify the repair.
	PASS	Level 1 is activated or software has taken the port out of service.
		3 of 3

BRI Layer 3 Query Test (#1243)

This test checks the application layer communications across the in-service ISDN D-Channel. The test passes if a status inquiry message is successfully sent, fails if the signaling link is down, and aborts if a query is already running or there is an internal error.

BRI Layer 3 Query Test (#1243)

Error Code	Test Result	Description / Recommendation
1005	ABORT	Wrong configuration. 1. This error can be ignored.
1019	ABORT	This test is already running. 1. This error can be ignored.
1113	ABORT or FAIL	The signaling link is down. 1. Test the port at 1-minute intervals up to 5 times. 2. Escalate the problem if the BRI Layer 3 Query test (#1243) continues to abort or fail.
		1 of 2

BRI Layer 3 Query Test (#1243) (continued)

Error Code	Test Result	Description / Recommendation
1187	ABORT	The media module or port may have been busied out by a technician. 1. Determine if the media module or port has been busied out. If it has, release the media module or port. 2. Make sure the terminal is connected. 3. Retry the command at 1-minute intervals up to 5 times.
2012	ABORT	Internal system error. 1. Retry the command at 1-minute intervals up to 5 times.
2100	ABORT	Could not allocate the necessary system resources to run this test 1. .Retry the command at 1-minute intervals up to 5 times.
	PASS	A Status Enquiry message was successfully sent.
		2 of 2

BRI Port Slip Query Test (#1244)

Slips occur when the transmitter and receiver are not running at precisely the same clock rate. The BRI Port Slip Query Test polls the total number of slips that have occurred on a link.

If the slip count is over the threshold, a MINOR alarm is raised against the media module, leaving every port of the media module in the in-service state.

BRI Port Slip Query Test (#1244)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
2000	ABORT	Response to the test was not received within the allowed time. 1. Rerun the test at 1-minute intervals up to 5 times.
2012	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 5 times.
		1 of 2

BRI Port Slip Query Test (#1244) (continued)

Error Code	Test Result	Description / Recommendation
2100	ABORT	Could not allocate the necessary system resources to run this test. 1. Rerun the test at 1-minute intervals up to 5 times.
1 to 88	FAIL	The media module and the remote endpoint are not synchronized to the same clock rate. The Error Code equals the number of slips detected by the media module since the last Slip Alarm Inquiry test. 1. Rerun the test at 1-minute intervals up to 5 times. 2. If the test continues to fail: a. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding. b. Check the physical connections of DS1 Interface media module and cable. c. Replace the local DS1 Interface media module and repeat the test. d. If the test fails again, contact T1 Network Service to diagnose the remote DS1 endpoint.
	PASS	No Slips are detected on the media module.
0	NO BOARD	See NO BOARD for repair procedures.
		2 of 2

Signaling Link State Test (#1251)

This test checks the current state of the signaling link. The test looks at the media module translations, checks that the media module is physically inserted, then gets the state of the D-Channel and service state of the port.

The test passes if the signaling link (D-Channel) is connected and operating normally. The test fails if the media module is not installed, the signaling link is disconnected, or if the port is out of service. The test aborts otherwise.

This test is run on ISDN BRI trunks.

Signaling Link State Test (#1251)

Error Code	Test Result	Description / Recommendation
	ABORT	Internal system error 1. Rerun the test at 1-minute intervals up to 5 times.
1114	ABORT	The signaling link is in a transitional state. 1. Rerun the test at 1-minute intervals up to 5 times.
8	FAIL	The signaling link is down. 1. Rerun the test at 1-minute intervals up to 5 times.
9	FAIL	The port is out of service. 1. Determine the service state of the port. 2. Attempt to release the port. 3. Rerun the test at 1-minute intervals up to 5 times.
	PASS	The signaling link is connected and operating normally.

Registration Status Inquiry Test (#1372)

The Registration status inquiry reports the H.323 registration status of the endpoint. An endpoint must be registered and authenticated in order to receive service from the system.

Registration is initiated when the endpoint user attempts to login using the Avaya registration software application running on the endpoint PC. The user must provide a valid extension and security code. The registration messages are sent to the IP address of the Ethernet port.

A registered extension has a port type of SNNNNN, where N is a digit from 0–9. A non-registered extension has a port type of X.

This test is run on H.323 telephones.

Registration Status Inquiry Test (#1372)

Error Code	Test Result	Description / Recommendation
Any	FAIL	The endpoint has not successfully registered. 1. Verify that the user is entering the: • correct extension and security code • correct IP address of the Ethernet port 2. Verify that the extension has been enabled for IP Softphone operation. 3. If several endpoints cannot register, investigate any errors of the Ethernet port. 4. Examine the Ethernet cabling from the endpoint PC to the Ethernet hub.
	PASS	The endpoint is successfully registered and continues to respond to registration handshaking. The endpoint is considered registered by the system, but refer to the results of tests #17 and #1373 which run an interactive test with the endpoint.

Ethernet Port Status Test (#1386)

This test checks the status of the Ethernet port that is the near-end gatekeeper of this signaling group. If the Ethernet port is in service, the test passes. If it is out of service, the test fails.

Note:

Failure of this test will take the signaling group out of service.

Ethernet Port Status Test (#1386)

Error Code	Test Result	Description / Recommendation
1125	ABORT	Ethernet Link is not in service. 1. Determine if the Ethernet link is in service or not. If the link is not in service, release the link and repeat the test. 2. If the test continues to abort after releasing the link, escalate the problem.
2000	ABORT	Response to the test was not received within the allowed time. 1. If this result occurs repeatedly, attempt to reset the media module if the other ports on the media module are idle (amber LED is off). 2. Rerun the test. 3. If this result occurs again, replace the media module.
2100	ABORT	The system resources to run the test could not be allocated. 1. Rerun the test at 1-minute intervals up to 5 times.
2500	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 3 times.
	FAIL	The Ethernet port corresponding to the near-end address of the signaling group that is out of service has failed. There may be problems with the on-board Ethernet NIC (eth1). 1. Test the port and note the result of the Signaling Group PING Test (#1387). • If the test continues to fail, escalate the problem. • If the test passes, wait for the sessions to come up.
	PASS	The Ethernet port corresponding to the near-end address of the signaling group that is in service has passed this test. Every session on the Ethernet link is up.

Signaling Group PING Test (#1387)

This test does not perform a ping to the Core Router. It only pings the LSS process.

Refer to the ping and traceroute commands on the **Network Diagnostics** page under **Maintenance & Monitoring** to perform actual ping and traceroute actions. The IP addresses can be obtained from the proper configuration page. In the case of the Core Router, the IP addresses may be obtained from the **System Summary** page.

Signaling Group PING Test (#1387)

Error Code	Test Result	Description / Recommendation
None 1 2	ABORT	Internal Error. 1. Rerun the test at 1-minute intervals up to 3 times.
7	ABORT	Destination unreachable. 1. Verify that the far-end IP address is reachable. 2. Once verified, retest and verify that the Signaling Group Ping test (#1387) passes.
1005	ABORT	Configuration for this test is incorrect. 1. If Layer 3 or LRQ is enabled for this H.323/SIP signaling group, this error can be ignored. There is no need to run the ping test. 2. Verify that the link is in service. 3. Verify that the routing table has destinations that are reachable through this port. 4. Repeat the test. 5. If the test aborts with Error Code 7 after step 2 is verified, escalate the problem.
1124 1125	ABORT	Link is not in service. 1. Check if the link is in service or not. If the link is not in service, release the link and repeat the test. 2. If the test continues to abort after the link has been released, escalate the problem.

1 of 2

Signaling Group PING Test (#1387) (continued)

Error Code	Test Result	Description / Recommendation
2000	ABORT	Response to the test was not received within the allowed time. 1. If this result occurs repeatedly, attempt to reset the media module if the other ports on the media module are idle (amber LED is off). 2. If this result occurs again, replace the media module.
2012	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 3 times.
2100	ABORT	The necessary system resources to run the test could not be allocated. 1. Rerun the test at 1-minute intervals up to 3 times.
2500	ABORT	Internal system error. 1. Rerun the test at 1-minute intervals up to 3 times.
2800 2801	ABORT	Could not find this IP address. No IP address defined. 1. Verify translations and retest.
2802	ABORT	Different IP address pinged than software had allocated for the test. 1. Rerun the test at 1-minute intervals up to 3 times.
7 89 1007	FAIL	**PING** to the destination failed through this port because the destination was down. 1. Verify that at least one destination that is reachable through this port is “up”. 2. Retest the port and verify that the Signaling Group Ping test (#1387) passes.
Any	PASS	PING through this port was successful.

2 of 2

MedPro Status Test (#1392)

This test determines if at least one media processor port is in service and can be used by this signaling group. If at least port one exists and is in service, the test passes. Otherwise, the test fails.

MedPro Status Test (#1392)

Error Code	Test Result	Description / Recommendation
None 2012 2100	ABORT	Internal system error. Internal system error. Could not allocate the necessary system resources to run this test. 1. Retry the command at 1-minute intervals up to 3 times
	FAIL	Problems with VoIP resource on the Media Gateway and/or no contact with Media Gateway. 1. Test the media gateway and follow the repair actions for any test that fails. 2. Test the Signaling Group and verify the result of the H.323 Signaling Group Ping test (#1387). If the test continues to fail, escalate the problem. If the test passes, wait for the sessions to come up.
	PASS	Every session on the Ethernet link is up.

Link State Audit Test (#1527)

This test verifies the Media Gateway H.248 link state and alarm state.

Link State Audit Test (#1527)

Error Code	Test Result	Description / Recommendation
1007	ABORT	The media gateway is not administered. 1. Verify that the media gateway is administered. 2. Rerun the test.
2012	ABORT	System call failed. 1. Retry the test at one-minute intervals up to 5 times.
1	FAIL	The Gateway has been unregistered longer than the Link Loss Delay Timer. 1. A Major alarm is raised.
769	FAIL	The Gateway is in link bounce. It has been unregistered less than the Link Loss Delay Timer. 1. A Minor alarm is raised.
	PASS	The link is up and there is no alarm.

Media Gateway Hyperactivity Audit Test (#1659)

This test resolves hyperactive registration alarms if the hyperactive condition no longer exists.

Media Gateway Hyperactivity Audit Test (#1659)

Error Code	Test Result	Description / Recommendation
2012	ABORT	Internal error. 1. Rerun the test at 1-minute intervals up to 3 times.
	PASS	The hyperactivity audit test passed.

NO BOARD

No media module was detected by the test. The test could not relate the internal ID to the port. This could be due to incorrect translations, no media module is inserted, an incorrect media module is inserted, or an insane media module is inserted.

1. Verify that the media module is properly translated and inserted. Resolve any problems.
2. If the media module is correctly inserted, reset the media module, then retest the media module.

This should re-establish the linkage between the internal ID and the port. If not, verify that a valid media module is inserted.

T1 Network Facility Procedures

If the DS1 Media Module connects to a T1 network facility or to another switch, do the following:

1. Verify that both endpoints of the DS1 link are administered using the same signaling mode, framing mode, and line coding.
2. Contact the T1 Network Service or a technician at the far-end switch to diagnose the remote DS1 endpoint.
3. Check the physical connection of the DS1 board to the terminating device, and check the premise distribution system or the intra-premise wiring for physical connection failures.
4. Replace the local DS1 Interface media module and repeat the test.

CDR Link Troubleshooting Procedures

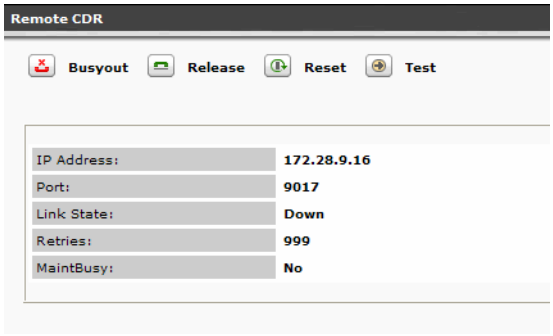
The following are the procedures for troubleshooting and restoring the CDR link:

1. Make sure the administered information is correct.

   The information for the CDR data format, Collector IP address, and Collector Port can be found under **Configuration > System Parameters > General**. Click on the **Misc** tab.

2. Determine the status of CDR link.

   Under **Maintenance & Monitoring > Telephony**, click on **Remote CDR**. Make sure that the extension has been administered and that the CDR link is not busied out for maintenance. If it is busied out, determine why, then release the CDR link if appropriate.



3. Where does the CDR link connect to?

   Determine the destination of the CDR link.

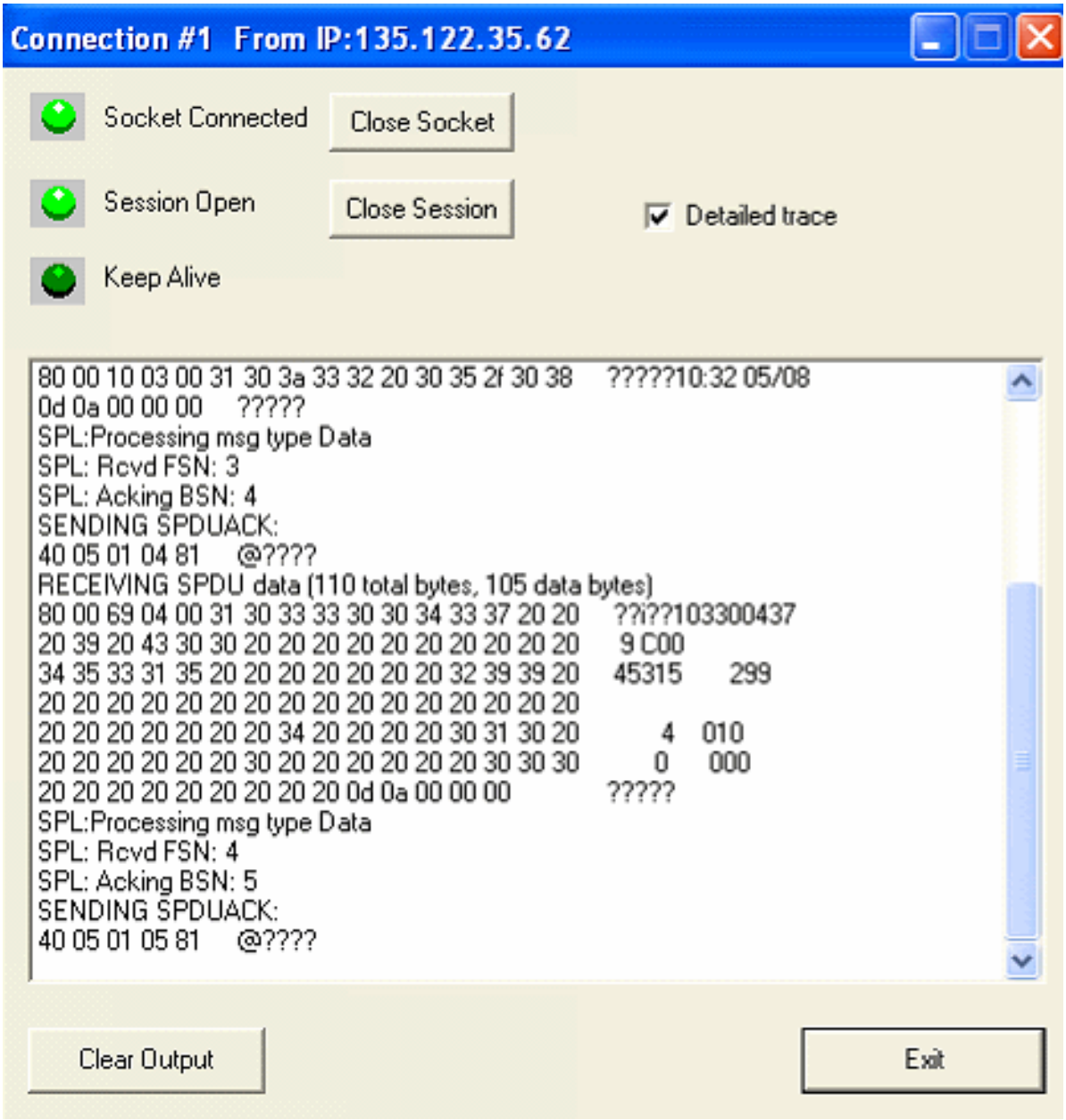
4. Is the external CDR output device available?

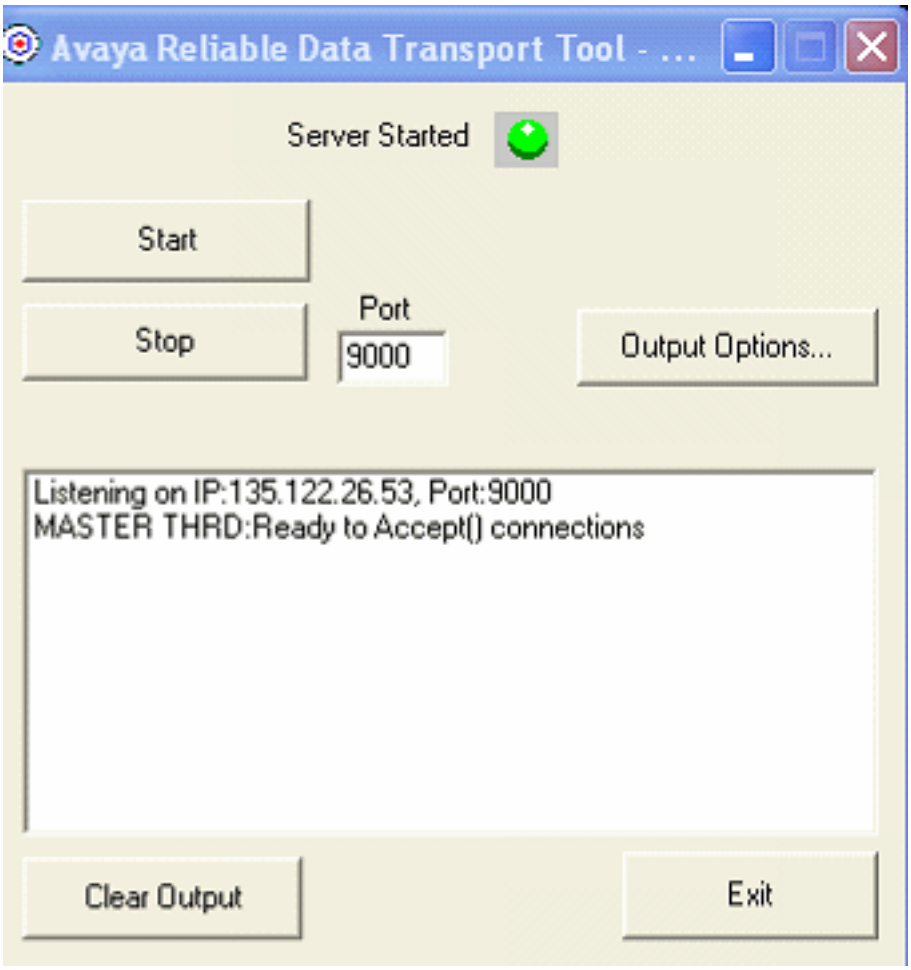
   Make sure that the CDR output device is on-line and ready for service. Check the physical connectivity to the CDR output device.

5. If the problem is not found in the above steps, check the media module for any problems.

6. If using reliable transport, use the Reliable Data Transport Tool to see if the platform is sending data. The tool was developed by Avaya, but is not supported by Avaya. The link to the tool is ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/definity/RDTT_Readme_2.1.doc Install RDTT on the PC/server which will collect the data. Install the Server option only. The tool and its associated files will be created by default under the directory C:\Program Files\Avaya\Avaya Reliable Data Transport Tool. The User Guide.doc contains descriptions of the

fields and their meanings. The output from RDTT will look like the following if data is being sent:




Avaya Reliable Data Transport Tool - ...
Server Started
Start
Stop
Port
9000
Output Options...
Listening on IP:135.122.26.53, Port:9000
MASTER THRD:Ready to Accept() connections
Clear Output
Exit

Backing Up Branch Central Manager and Communication Manager Branch

Avaya Network Configuration Manager

Avaya Network Configuration Manager (NCM) is an optional tool can be used to backup the configuration files for the Communication Manager Branch. Backups can be performed on demand or automated using the NCM's scheduling capability. NCM backs up the following configuration files:

- The Main Configuration file including:
  - Translations
  - Platform configuration information (IP addresses, Vlans, etc.)
  - Services configuration (DHCP server, NTP server, etc.)
- Voice mail configuration file such as passwords, etc.
- SIP Profile Data such as SIP user information (contact lists, etc.)

Note:

NCM does not perform a complete backup of Communication Manager Branch. To perform a complete backup of Communication Manager Branch use Branch Device Manager.

Note:

User greetings and voice mailboxes are not backed up by NCM. Currently there is no scheduling capability to backup user greetings and voice mailboxes. They must be backed up manually using Branch Device Manager.

For more information on how to use NCM, see the Avaya Network Configuration Manager User Guide at http://support.avaya.com.

Backing up Branch Central Manager

Note:

Branch Central Manager cannot be used to perform a backup on a local Communication Manager Branch. Branch Central Manager backs up the data and logs on the Branch Central Manager server only.

Read the following information before you perform a backup on Branch Central Manager:

- Branch Central Manager backup options:
  - Manual backups: You can manually run a backup at any time.
  - Schedule backups:
    - Run a backup one time only on a specific date and time.
    - Reoccurring backups: Schedule the backup to run daily, weekly, or monthly at the same time on the same day of the week.
- A Branch Central Manager backup includes the following information:
  - Administration data stored in the Main Configuration files:
    - All templates
    - All groups
    - All jobs in the job queue/log except the jobs that are running
    - All system settings such as those for job queue/log retention and system log file size
  - All profiles including SIP Profile Data: SIP user information such as contact lists, etc.
  - Voice mail configuration file: The voice mail configuration file contains voice mail user information such as passwords, etc.

  Note:

  User’s voice mail greetings and mailboxes are backed up by Branch Device Manager not Branch Central Manager.

  - System logs
- A backup includes the files from the active bank only. If the backup is used in a restore operation, the backup files are copied to the active bank.

The frequency in which you perform a backup on Branch Central Manager is determined on the amount of changes and additions that are being made. Avaya recommends that a backup be performed a least once a week.

Note:

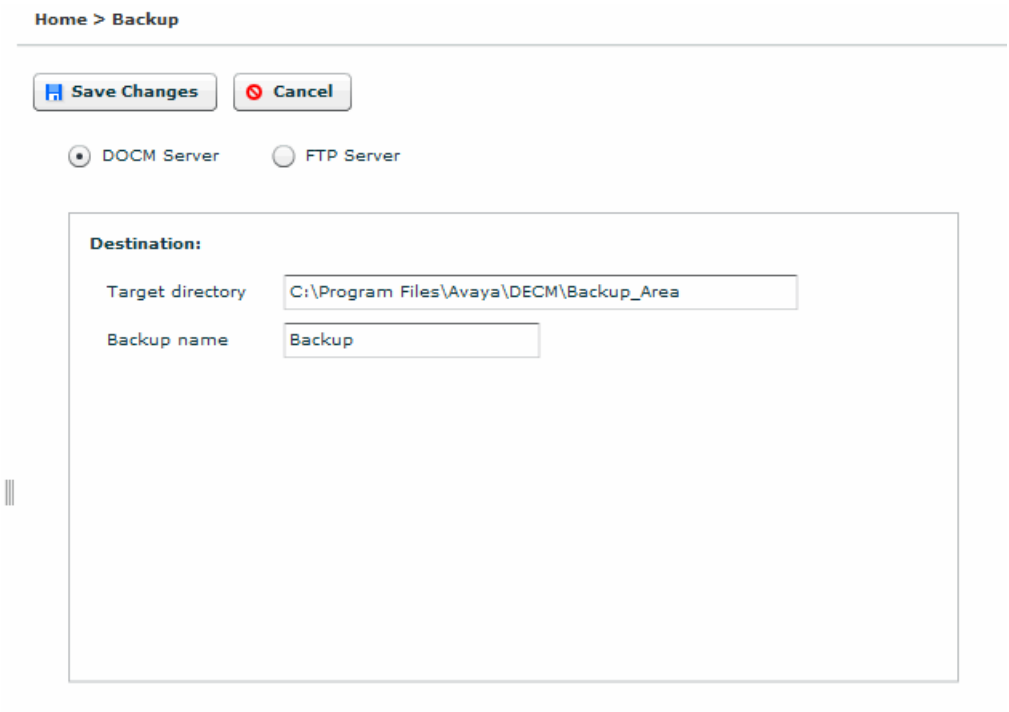
Due to possible interdependencies between files, Avaya recommends that you backup all the files at once.

Procedure to backup Branch Central Manager

Use the following steps to backup Branch Central Manager:

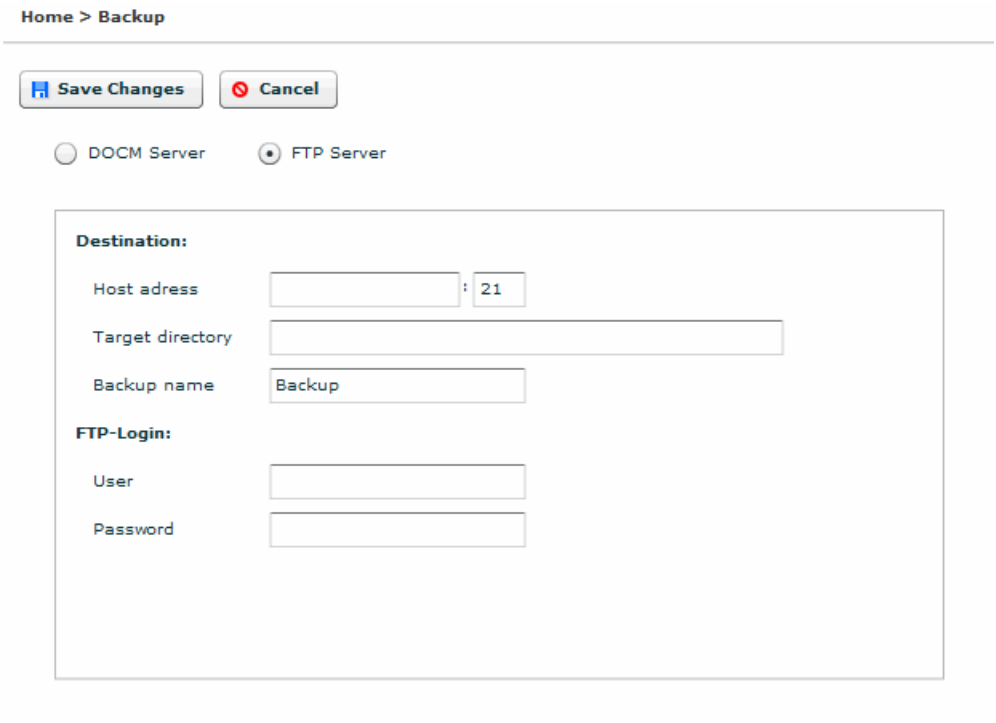
1. On the navigation pane, click **Backup** under Utilities. The main backup screen appears. The main backup screen contains a list of non-scheduled backups, scheduled backups, and completed backups.
2. Click **Add**. A new screen appears as shown in example Figure 26.

Figure 26: Branch Central Manager backup to CMBE - Branch Central Manager Server



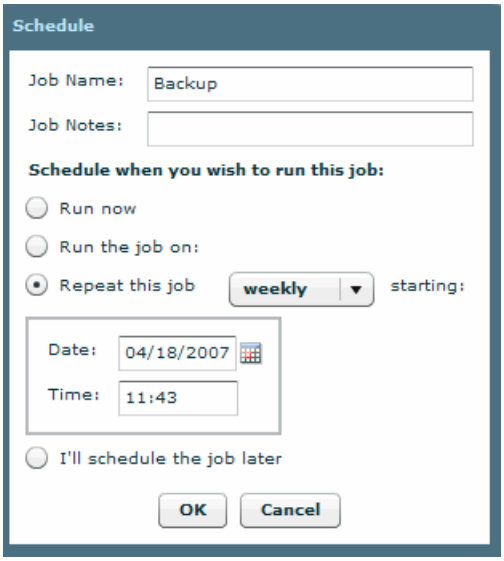
3. Select the method of backup:
   - Manager Branch Central Manager Server: When you choose the Branch Central Manager Server option, backup files are copied to a target directory on the Branch Central Manager server. When Branch Central Manager Server is selected, enter a full path name in the Target directory field and a backup name.
   - FTP Server: When you choose the FTP Server option, additional fields appear as shown in example Figure 27. Enter information in the Host address, Target directory, and Backup name field. You must enter a valid user login and password to perform the backup.

Figure 27: Branch Central Manager backup to FTP Server



4. Click **Save Changes**. The **Schedule** screen appears as shown in example Figure 28.

Figure 28: Branch Central Manager backup schedule screen



5. In the **Schedule** screen:
   - Enter a job name.
   - Enter additional information concerning this backup.
   - Select one of the following under the 'Schedule when you wish to run this job' heading:
     - Run now: When this option is selected the rest of the fields are inactive. A backup with the run now option displays a status of planned. The backup runs after it is planned.
     - Run this job on: When this option is selected the backup runs only once at a specified date and time.
     - Repeat this job: When this option is selected a backups runs according to a schedule. From the Starting drop-down menu, choose daily, weekly, or monthly and enter a date and time to schedule the job.
     - I'll schedule the job later: When this option is selected the rest of the fields are inactive.
6. Click **OK**. The new backup appears on the list in the main backup screen.
7. The main backup screen does not automatically refresh. To get the current status of a backup, click **Refresh**.
8. To remove a backup from the list, highlight the backup and click **Remove**.

Backing up Communication Manager Branch using Branch Device Manager

Overview

The the platform, and the service pack contain two boot banks, bank A and bank B. A boot bank is a partition in the flash disk that contains the version of Communication Manager Branch, configuration and administration information, etc. One boot bank is active while the other is inactive. It is possible that the boot banks may contain different information.

A backup copies the information on the active bank of the platform only. It does not backup the image of the platform or the firmware of the media modules. The platform image and media module firmware files can be downloaded from http://support.avaya.com and added to the backup directory to create a full backup. For more information, see Creating a full backup on page 221.

When you are connected through the Services port, you can perform a backup to a USB flash disk but you cannot backup to an FTP server that is running on the laptop.

Before you begin a backup

Read the following information before backing up the local Communication Manager Branch:

- A backup is copied from the active bank. If a backup containing the Main Configuration file is used in a restore operation, the backup files are copied to the inactive bank, the banks are swapped, and the system reboots.
- A complete backup on an FTP server requires 600MB for an i40, 900MB for an Communication Manager Branch i120, and 1.13GB for a Communication Manager Branch G450. This requirement is based on a system running at maximum capacity of administered users and voice mail.
- A complete backup on a USB flash drive requires at least 2GB.
  - Branch Device Manager will not backup to a USB flash disk if it does not contain enough space.
  - To obtain additional space on the USB flash disk, Branch Device Manager allows you to delete unwanted backups as part of the backup procedure.
- A USB flash disk must be a FAT16 or FAT32 format.
- While a complete backup contains all the files needed to restore the system on which the backup was performed, it does not contain all the files needed to duplicate the Communication Manager Branch system. To duplicate a Communication Manager Branch the platform image and the firmware files of the media modules must be downloaded from the support Web site and placed in the backup directory. The images, firmware, and service pack combined with a complete backup create a full backup. You can use a full backup to duplicate a system of the same type such as i120 to i120 and i40 to i40. Any attempts to duplicate a system with a system of a different type will fail.

  For more information on creating a full backup see Creating a full backup on page 221.
- Record and save the master key that was administered on the Communication Manager Branch system during the time of the backup. The master key is used to encrypt all other passwords. You will not be able to restore the backup if you do not have the master key that was administered at the time the backup was performed.
- When a backup completes there are two readme files that are created in the backup directory on the FTP server or the USB flash disk. The readme file is called readme.txt. They contain all the files that were successfully backed up.

Supported FTP and SCP servers

The FTP and SCP servers listed in Table 4 are supported for Communication Manager Branch backups, restores, uploads and downloads.

Table 4: Supported FTP and SCP servers table

Server	Operating System	Version
FileZilla	Microsoft Windows	0.9.5
proFTPd	Linux	1.3.0
IIS	Microsoft Windows	5.0 and later
vsFTPd	Linux	2.0.3
wu-FTPd	Linux	2.6.2
PureFTP	Linux	1.0.21
Default FTP server	Solaris Sun	5.8 and later
OpenSSH	Microsoft Windows	3.8
OpenSSH	Linux Solaris Sun	4.6
WINSSHD	Microsoft Windows	4.23

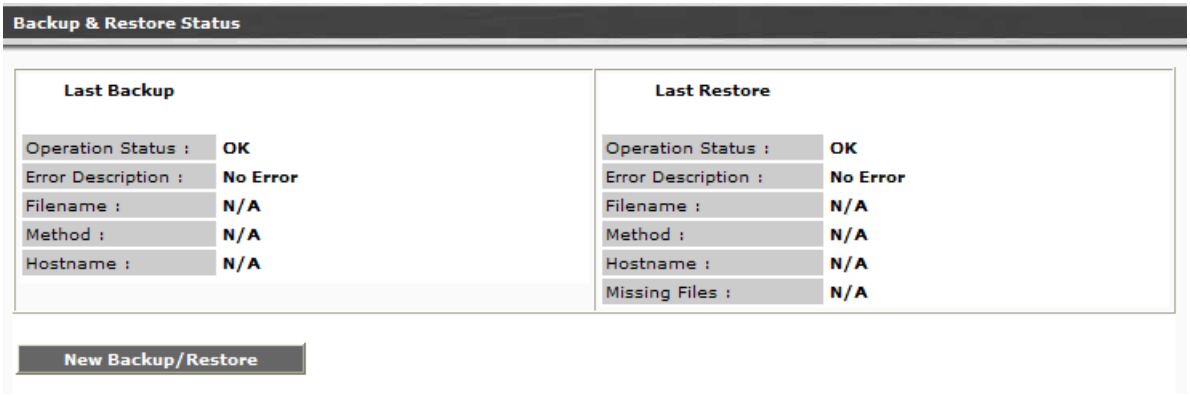
Procedure to backup to an FTP server

Using the Branch Device Manager interface, perform the following steps to backup to an FTP server:

1. Click **Backup and Restore** under the Maintenance and Monitoring > Configuration Administration.

   The **Backup and Restore Status** screen displays as shown in example Figure 29. The Backup and Restore Status screen contains information on the last backup and the last restore.

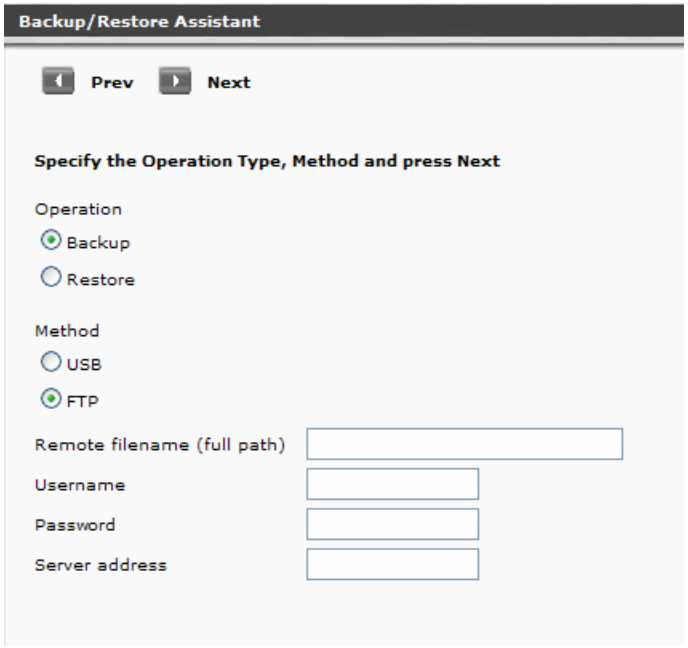
Figure 29: Backup and restore status screen



2. Click **New Backup/Restore**.

   The Backup and Restore Assistant screen appears as shown in example Figure 30. The Backup and Restore Assistant steps you through the rest of the backup.

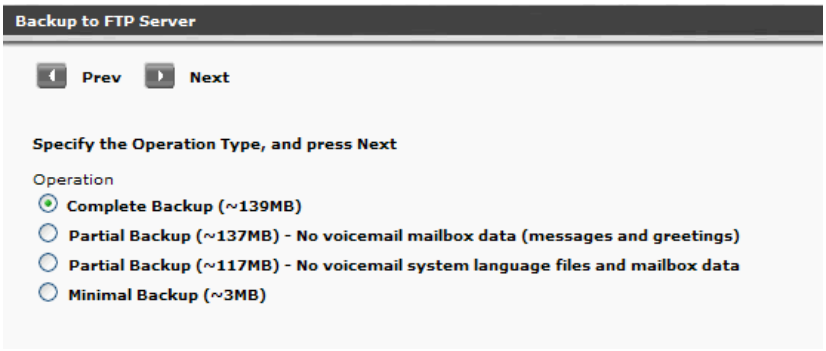
Figure 30: Backup and restore assistant screen



3. On the Backup/Restore Assistant screen choose:
   a. A backup operation by clicking the radio button next to **Backup**.
   b. The backup method by clicking the radio button next to **FTP**. When FTP is selected, you must enter information in the following fields:
      - Remote filename (full path): Enter a path of the FTP server that includes the filename where the backup will be stored. The path and file name can be up to 128 characters in length and cannot include illegal symbols such as *,:,?,|,{}, and a space.
      - Username: Enter the login for the FTP server. The Username can be up to 32 characters in length.
      - Password: Enter the password for the FTP server. The password can be up to 32 characters in length.
      - Server address: Enter the IP address of the FTP server or enter the hostname if it is defined in the system's DNS servers.
   c. Click **Next**.

      The Backup to FTP Server screen appears as shown in example Figure 31.

Figure 31: Backup Assistant - Backup to FTP Server



4. Select the backup operation that you want to perform. The following is a detailed list of what is included in each backup operation. For a quick reference, see Table 5.
   - **Complete Backup**: A complete backup contains the following data:
     - Configuration files for the Communication Manager Branch:
       - Translations
       - Installation profiles
       - Platform configuration information (IP addresses, Vlans, etc.)
       - Services configuration (DHCP server, NTP server, etc.)
       - Voicemail and auto attendant configuration.
       - SIP profile data

- AES keytab file
- Alarm client configuration file: This file is used to send alarms to Avaya Services.
- Image files for the Communication Manager Branch
- Locally stored IP phone files: A total of 40MB is used with a maximum of:
  - 40 scripts including the setting file, language files, and upgrade scripts
  - 16 IP phone images
- System announcements: A complete backup includes up to 256 files with a maximum size of 7MB.
- Voice mail and system language files: A complete backup can include up to two files with each file being a maximum size of 15MB.
- Auto Attendant files such as announcements and menu prompts.
- Trusted certificates: A maximum of 10 trusted certificates can be backed up. There is no backup and restore capability for the server certificate used for the HTTPS/SIP Proxy on the Communication Manager Branch. The server certificate is valid for a specific Communication Manager Branch only. A new server certificate must be generated if the Communication Manager Branch is changed.
- Unicode phone message files: Unicode phone message files are used on H.323 type phones to support languages other than the default system languages.
- User voice mail boxes and greetings

Note:

The platform image, service pack, and media module firmware can be added to the backup directory to create a full backup. For more information, see Creating a full backup on page 221.

- **Partial Backup**: This partial backup includes everything in the complete backup except for the voice mail data such as messages and greetings. Choosing this backup reduces the size and the time for the backup. Voice mail data can add 250MB for the i40, 560MB for the Communication Manager Branch i120, and 790MB for the Communication Manager Branch G450.

Important:

There is no option available to backup the voice mail and the user greetings only. Use the Complete Backup option to backup voice mail and user greetings.

- **Partial Backup**: This partial backup includes everything in the complete backup except the voice mail system language files and mailbox data. Choosing this backup reduces the size and time for the backup. Each system language file can add up to 15MB to the backup.
- **Minimal Backup**: A minimal backup contains administrator data only such as:
  - Configuration files: and installation profiles

- AES configuration file
- Unicode Phone message files
- Locally stored IP phone files for scripts and language files only. A minimal backup does not include IP phone images.
- System announcements
- Auto Attendant files with announcements and menu prompts
- Trusted certificates
- Alarm Client configuration file

Important:
A Minimal backup does not include user information stored in the voice mail configuration file and SIP Profile Data.

Use Table 5 as a quick reference for backup content information.

Table 5: Backup operation and contents

Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Translations	X	X	X	X
Installation profiles	X	X	X	X
Platform configuration information	X	X	X	X
Services configuration information	X	X	X	X
Voice mail and auto attendant configuration information	X	X	X	X
Voice mailboxes and greeting	X			
SIP profile data	X	X	X	
AES keytab file	X	X	X	X
Alarm client configuration file	X	X	X	X
Locally stored IP phone files	X	X	X	
System announcements	X	X	X	X
System language files	X			
Auto Attendant files such as announcements and menu prompts	X	X	X	X

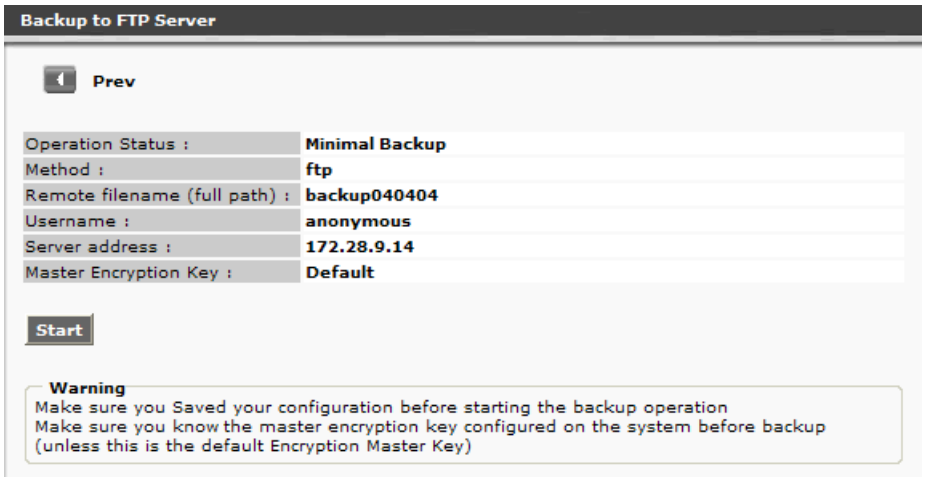
1 of 2

Table 5: Backup operation and contents (continued)

Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Trusted certificates	X	X	X	X
Unicode phone message files	X	X	X	X
				2 of 2

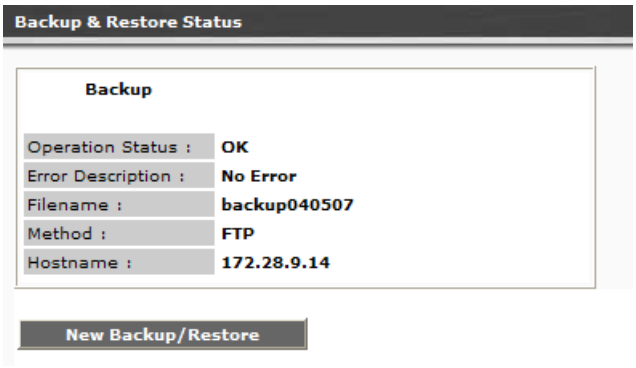
Click **Next.** A window appears as shown in example Figure 32 displaying the options that you selected for the backup and information that you entered for the FTP server.

Figure 32: Backup to FTP server



5. If the information is correct, click **Start**. A window appears as shown in example Figure 33 displaying the status of the backup.

Figure 33: Backup to FTP server complete



The Backup and Restore Status screen contains the following fields:

- Operation Status:
  - Executing: Executing displays while the operation is in progress.
  - OK: Displays if the operation is a success.
- Error Description: An error appears if there is a problem with the backup. For a list of the FTP backup errors and possible resolutions, see Table 6.
- Filename: This field displays the filename that you entered in the first assistant screen.
- Method: The field displays FTP server.
- Hostname: The IP address of the FTP server or the hostname as it is defined in the system's DNS servers.

Tip:

You can verify the files that were successfully backed up by accessing the backup directory on the FTP server and opening the readme.txt file.

Troubleshooting a failed FTP server backup

Use Table 6 to identify and troubleshoot problems with a failed FTP server backup.

Table 6: Backup errors and resolutions

Error message	Meaning	Resolution
Server unreachable	A PING to the FTP server failed.	Verify that the FTP server is accessible from Communication Manager Branch: 1. Using Branch Device Manager, click **Network Diagnostics** under Maintenance and Monitoring. 2. Click the radio button next to PING, enter the address of the FTP server and click **Start**. If PING fails, troubleshoot the network problems.
FTP error - invalid login parameters or configuration error	Incorrect configuration information such as a incorrect username, password, or wrong IP address.	Verify the username, password and IP address of the FTP server and try again.
Unable to create backup directories	The backup process failed to generate new directories on the FTP server.	The FTP account on the remote FTP server must have read and write permission. Verify that the account has read and write permission. If it does not, enable the read and write permission on the account and try the backup again.
Backup failed: Communication Manager Branch image	The backup process failed to copy the Communication Manager Branch image.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems. ● There is an invalid image running on the system or that the image is corrupted.
		1 of 4

Table 6: Backup errors and resolutions (continued)

Error message	Meaning	Resolution
Backup failed: service pack	The backup process failed to copy the service pack.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems. ● There is an invalid Service Pack running on the system or that the Service Pack image is corrupted.
Backup failed: Configuration Database	The backup process failed to copy the configuration database.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems. ● A configuration tool is being used. You cannot configure the system during a backup. Close all configuration tools and try the backup again.
Backup failed: Voice mail Configuration file	The backup process failed to copy the voice mail configuration file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems. ● Voice mail is down. If voice mail does not come back up, try rebooting Communication Manager Branch and try the backup again.
Backup failed: Setup help file	The backup process failed to copy the setup help file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Voicemail boxes	The backup process failed to copy the voice mail boxes.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
		2 of 4

Table 6: Backup errors and resolutions (continued)

Error message	Meaning	Resolution
Backup failed: Keytab file	The backup process failed to copy the keytab file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Installation task file	The backup process failed to copy the installation task file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Installation profile files	The backup process failed to copy the installation profile files.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Alarm client configuration file	The backup process failed to copy the alarm client configuration file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Trusted Certificate	The backup process failed to copy the Trusted Certificate.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Avaya Unicode file	The backup process failed to copy the Avaya Unicode file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: Custom Unicode file	The backup process failed to copy the Custom Unicode file.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
		3 of 4

Table 6: Backup errors and resolutions (continued)

Error message	Meaning	Resolution
Backup failed: IP phone image	The backup process failed to copy the IP phone image.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: IP phone script	The backup process failed to copy the IP phone script.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
Backup failed: System Language File 1	The backup process failed to copy the System Language File 1.	his error can indicate that: ● The FTP server does not have enough space to perform the backup. There are network problems.
Backup failed: System Language File 2	The backup process failed to copy the System Language File 2.	This error can indicate that: ● The FTP server does not have enough space to perform the backup. ● There are network problems.
		4 of 4

Procedure to backup to a USB flash disk

Use the following steps to backup to a USB flash disk:

1. Insert the USB flash disk in the USB port on the platform. Refer to Figure 34 and Figure 35 for the location of the USB port.

Figure 34: USB port on the i40

Figure notes:

1. **USB port**

Figure 35: USB port on the Communication Manager Branch i120

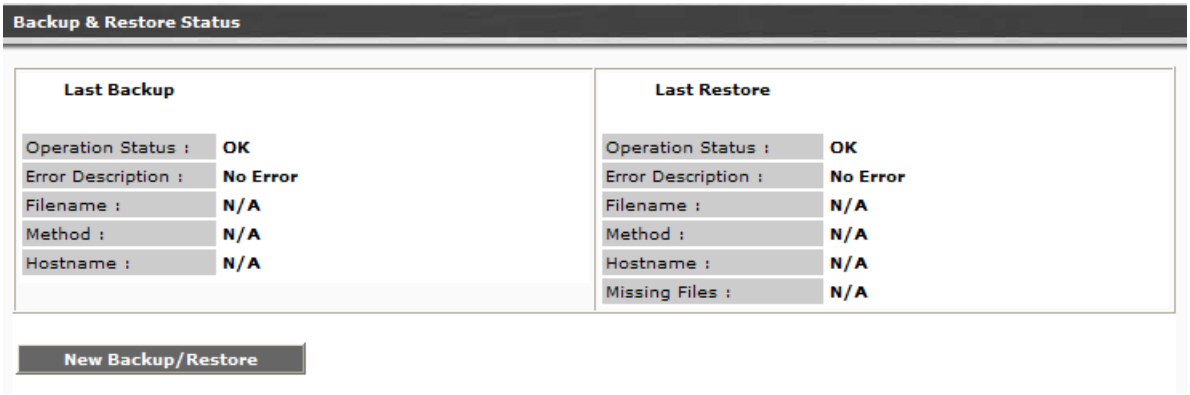
Figure 36: USB port on the Communication Manager Branch G450

Figure notes:
1. **USB port(s)**

2. Click **Backup and Restore** under the Maintenance and Monitoring > Configuration Administration.

   The **Backup and Restore Status** screen displays as shown in Figure 37. The Backup and Restore Status screen contains information on the last backup and the last restore.

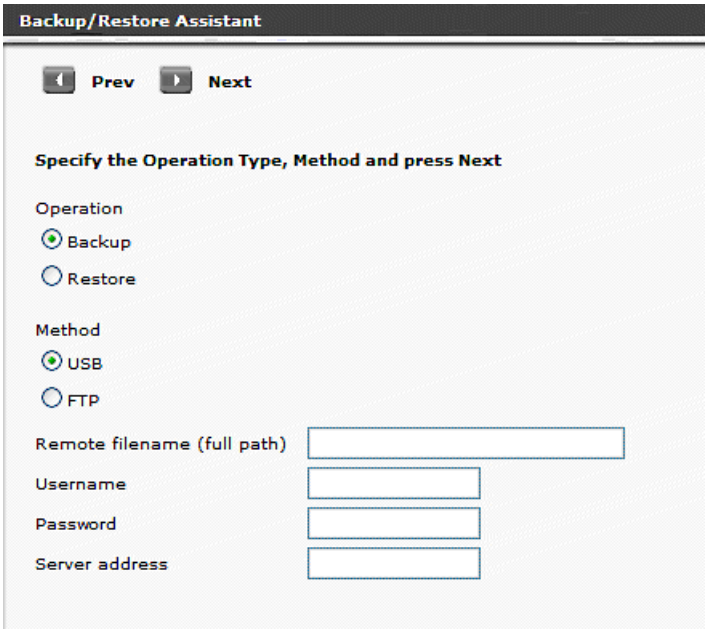
Figure 37: Backup and restore status screen



3. Click **New Backup/Restore**.

   The Backup and Restore Assistant screen appears as shown in Figure 38. The Backup and Restore Assistant steps you through the rest of the backup.

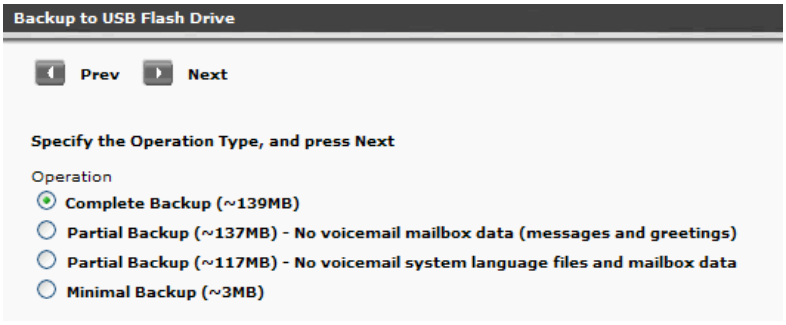
Figure 38: Backup and restore assistant screen



4. On the Backup/Restore Assistant screen choose:
   a. A backup operation by clicking the radio button next to **Backup**.
   b. The backup method by clicking the radio button next to **USB**. When USB is selected the Remote file name, User name, Password, and Server address fields are inactive.

   Click **Next**. The Backup to USB Flash Drive appears as shown in example Figure 39.

Figure 39: Backup and restore assistant - Backup to USB Flash Drive



5. Select the backup operation that you want to perform. The following is a detailed list of what is included in each backup operation. For a quick reference, see Table 7.

   - **Complete Backup**: A complete back contains the following data:
     - Configuration files:
       - Translations
       - Installation profiles
       - Platform configuration information (IP addresses, Vlans, etc.)
       - Services configuration (DHCP server, NTP server, etc.)
       - Voicemail and auto attendant configuration.
       - SES profile data
     - AES keytab file
     - Alarm client configuration file: This file is used to send alarms to Avaya Services.
     - Locally stored IP phone files: A total of 40MB is used with a maximum of:
       - 40 scripts including the setting file, language files, and upgrade scripts
       - 16 IP phone images
     - System announcements: A complete backup includes up to 256 files with a maximum size of 7MB.
     - Voice mail and system language files: A complete backup can include up to two files. Each file has a maximum size of 15MB.
     - Auto Attendant files such as announcements and menu prompts
     - Certificates: A maximum of 10 Trusted Certificates can be backed up. There is no backup and restore capability for the server certificate used for the HTTPS/SIP Proxy on the Communication Manager Branch. The server certificate is valid for a specific Communication Manager Branch only. A new server certificate must be generated if the Communication Manager Branch is changed.
     - Unicode phone message files: The Unicode phone message files are used on H.323 type phones to support languages other than the default system languages.
     - User voice mail boxes and greetings

   Note:

   The platform image, service pack, and media module firmware can be added to the backup directory creating a full backup. For more information, see Creating a full backup on page 221.

   - **Partial Backup**: This partial backup includes everything in the complete backup except for the voice mail data such as messages and greetings. Choosing this backup reduces the size and the time for the backup. Voice mail data can add 250MB for the i40, 560MB for the Communication Manager Branch i120, and 790MB for the G450 Communication Manager Branch.

Important:
There is no option available to backup the voice mail and the user greetings only. Use the Complete Backup option to backup voice mail and user greetings.

- **Partial Backup**: This partial backup includes everything in the complete backup except the voice mail system language files and mailbox data. Choosing this backup reduces the size and time for the backup. Each system language file can add up to 15MB to the backup.
- **Minimal Backup**: A minimal backup contains administrator data only such as:
  - Configuration files: installation profiles
  - AES configuration file
  - Unicode Phone message files
  - Locally stored IP phone files: Scripts and language files only. It does not include IP phone images.
  - System announcements
  - Auto Attendant files: Announcements and menu prompts
  - Trusted certificates
  - Alarm Client configuration file

Important:
A Minimal backup does not include user information stored in the voice mail configuration file and SIP Profile Data.

Use Table 7 as a quick reference for backup content information.

Table 7: Backup operation and contents

Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Translations	X	X	X	X
Installation profiles	X	X	X	X
Platform configuration information	X	X	X	X
Services configuration information	X	X	X	X
Voice mail and auto attendant configuration information	X	X	X	X

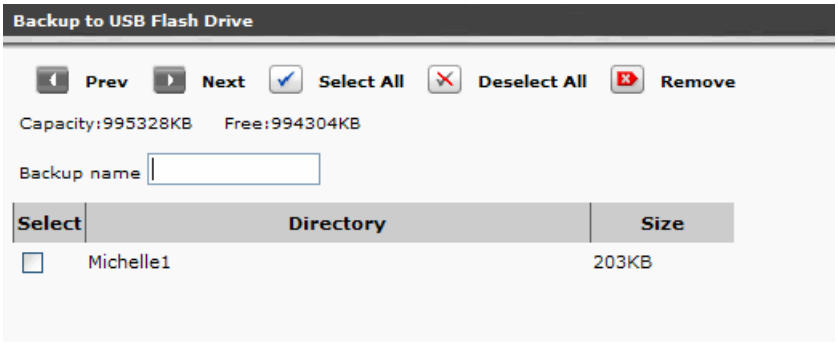
1 of 2

Table 7: Backup operation and contents (continued)

Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Voice mail user information	X	X	X	
SIP profile data	X	X	X	
AES keytab file	X	X	X	X
Alarm client configuration file	X	X	X	X
Locally stored IP phone files	X	X	X	
System announcements	X	X	X	X
Voice mail data such as messages and greeting	X			
System language files	X	X		
Auto Attendant files such as announcements and menu prompts	X	X	X	X
Trusted certificates	X	X	X	X
Unicode phone message files	X	X	X	X
				2 of 2

6. Click **Next**. A window appears as shown in example Figure 40. In this window you can:
   - Check the capacity and free space of the USB flash disk.
   - Remove any unnecessary directories: Removing unnecessary directories frees space on the flash disk for the backup. To remove a directory click the box associated with the directory name and then click **Remove**.
   - Select a directory to overwrite: To overwrite a directory, click the box associated with directory name.
   - Enter a name for the backup in the **Backup name** field.

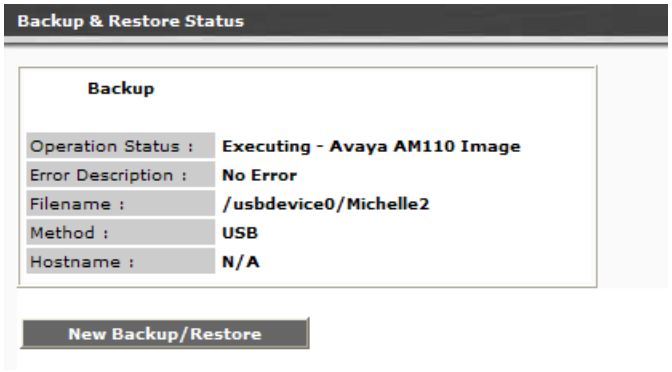
Figure 40: Backup to USB Flash Drive assistant



Click **Next**. A window appears showing the selected operation, the selected method, and the directory name for the backup.

7. If the information is correct, click **Start**. A window appears as shown in example Figure 41 displaying the status of the backup.

Figure 41: Backup and Restore Status screen



The **Backup and Restore Status** screen contains the following fields:

- Operation Status:
  - Executing: Executing displays while the operation is in progress.
  - OK: Displays if the operation is a success
- Error Description: An error appears if there is a problem with the backup. For a list of the USB backup errors and possible resolutions, see Table 8.
- Filename: This field displays the filename that you entered in the first assistant screen.
- Method: The Method field displays USB flash disk.
- Hostname: The IP address of the FTP server or the hostname as it is defined in the system's DNS servers.

Tip:

You can verify the files that were successfully backed up by accessing the backup directory on the USB flash disk and opening the readme.txt file.

Troubleshooting a failed USB backup

Use Table 8 to identify and troubleshoot problems with a failed USB backup.

Table 8: Backup errors and resolutions

Error message	Meaning	Resolution
Backup failed: Communication Manager Branch image	The backup process could not copy the Communication Manager Branch image.	This error can indicate that: • The USB does not have enough space to perform the backup. • There is an invalid image on the system or that the image on the system is corrupted.
Backup failed: service pack	The backup process could not copy the image.	This error can indicate that: • The USB does not have enough space to perform the backup. • There is an invalid service pack on the system or the service pack is corrupted.
Backup failed: Configuration Database	The backup process could not copy the Configuration Database	This error can indicate that: • The USB does not have enough space to perform the backup. • The system is being used by a configuration tool. You cannot perform configuration changes during a backup. Complete the configuration changes and try the backup again.
Backup failed: Voice mail Configuration file	The backup process could not copy the Voice mail Configuration file.	This error can indicate that: • The USB does not have enough space to perform the backup. • Voice mail is down. Try the backup again. If voice mail is still down, reboot the system and try again.
Backup failed: Setup help file	The backup process could not copy the Setup help file.	This error can indicate that the USB does not have enough space to backup the Setup help file.
		1 of 2

Table 8: Backup errors and resolutions (continued)

Error message	Meaning	Resolution
Backup failed: Voicemail boxes	The backup process could not copy the Voicemail boxes.	This error can indicate that the USB does not have enough space to backup the Voice mailboxes.
Backup failed: Keytab file	The backup process could not copy the Keytab file.	This error can indicate that the USB does not have enough space to backup the Keytab file.
Backup failed: Installation task file	The backup process could not copy the Installation task file.	This error can indicate that the USB does not have enough space to backup the installation task file.
Backup failed: Installation profile files	The backup process could not copy the Installation profile files.	This error can indicate that the USB does not have enough space to backup the profile files.
Backup failed: Alarm client configuration file	The backup process could not copy the Alarm client configuration files.	This error can indicate that the USB does not have enough space to backup the alarm client configuration file.
Backup failed: Trusted Certificate	The backup process failed to copy the Trusted Certificate.	This error can indicate that the USB does not have enough space to backup the Trusted Certificate.
Backup failed: Avaya Unicode file	The backup process failed to copy the Avaya Unicode file.	This error can indicate that the USB does not have enough space to backup the Avaya Unicode file.
Backup failed: Custom Unicode file	The backup process failed to copy the Custom Unicode file.	This error can indicate that the USB does not have enough space to backup the Custom Unicode file.
Backup failed: IP phone image	The backup process failed to copy the IP phone image.	This error can indicate that the USB does not have enough space to backup the IP phone image.
Backup failed: IP phone script	The backup process failed to copy the IP phone script.	This error can indicate that the USB does not have enough space to backup the IP phone script.
Backup failed: System Language File 1	The backup process failed to copy the System Language File 1.	This error can indicate that the USB does not have enough space to backup the System Language File 1.
Backup failed: System Language File 2	The backup process failed to copy the System Language File 2.	This error can indicate that the USB does not have enough space to backup the System Language File 2.
		2 of 2

Creating a full backup

To create a full backup you must first download the firmware for the platform, the firmware for the media modules and the service pack from the avaya Web site at http://support.avaya.com. After the service pack and firmware files have been downloaded you can manually add them to the backup directory where the complete backup is stored.

Restoring the System

This chapter contains information on how to restore Branch Central Manager and the local Communication Manager Branch system.

Restoring Branch Central Manager

Read the following information before performing a restore of Branch Central Manager:

- Branch Central Manager can be restored from backup files that are stored on the Branch Central Manager server or on the FTP server.
- Branch Central Manager verifies that the firmware at the time of the backup is the same version as the firmware on the restore device.
- A backup is restored to the active bank only. A backup can include the following information:
  - Administration data stored in the Main Configuration files:
    - All templates
    - All groups
    - All jobs in the job queue/log except the jobs that are running.
    - All system settings such as those for job queue/log retention and system log file size.
  - All profiles including SIP Profile Data: SIP user information such as contact lists, etc.
  - Voice mail configuration file: The voice mail configuration file contains voice mail user information such as passwords, etc.
  - System logs
- After the restore is complete, Avaya recommends that you reboot Branch Central Manager.
- The Configuration Manager utility is used to restore Branch Central Manager. For a procedure to restore Branch Central Manager, see the Branch Central Manager on-line help.

Restoring Communication Manager Branch without using Branch Device Manager

For new installations of Communication Manager Branch, a profile or a backup can be restored from a USB flash disk without using the Branch Device Manager interface.

Use the following steps to restore from a USB flash disk:

1. Insert the USB flash disk containing the profile or backup in the USB port on the platform.
2. Perform an NVRAM init command. The NVRAM init command deletes all configuration files including the IP addresses and restores the system to factory defaults.

   If there is only one profile or backup on the USB flash disk, the system automatically uses it to perform a restore.

   If there are multiple profiles and/or backups on the USB flash disk, the system does not automatically select which one to restore. You must connect to the Services port on the platform, log into Branch Device Manager and follow the system prompt to select either the install from profile or the install from scratch option. If install from profile is selected, later in the process you choose which profile to install.

Restoring Communication Manager Branch using Branch Device Manager

Overview

The platform, and the service pack on Communication Manager Branch have two boot banks, bank A and bank B. A boot bank is a partition in the flash disk that contains the version of Communication Manager Branch, configuration and administration information, etc. At any time, one boot bank is active while the other is inactive. It is possible that the boot banks may contain different information.

A complete restore, a partial restore, or a minimal restore operation is selected during the restore procedure. During a complete and partial restore operation, the data from the FTP server or the USB flash disk is loaded onto the inactive bank. When the restore includes the Main Configuration file the boot banks are swapped and the system automatically reboots. When the reboot is complete, the active bank contains the information from the restore. If there is an issue with the restore you can swap back to the inactive bank where the last old firmware and old Main Configuration files are stored.

While a complete restore contains all the files needed to restore the system on which the backup was performed, it does not contain all the files needed to duplicate the Communication Manager Branch system. To duplicate a Communication Manager Branch the platform image and the firmware files of the media modules must be downloaded from the support Web site and placed in the backup directory. The images, firmware, and service pack combined with a complete backup create a full backup. The platform image and media module firmware can be downloaded from the Avaya support Web site at http://rfa.avaya.com. For more information on creating a full backup, see Creating a full backup on page 221.

If a full backup is not available you can manually restore the firmware, images, and service pack using the information in Restoring the firmware, images, and service pack on page 242.

Read before you begin a restore

Read the following information before beginning a restore operation:

- Know what you are restoring: You can verify the files that will be restored by accessing the device containing the backup directory and opening the readme.txt file.
- A restore containing the Main Configuration file requires a reboot and is service affecting.
- You can restore only the SIP Profile Data using the **Configuration File Management** link on the Branch Device Manager interface. Restoring the SIP Profile Data requires a manual reboot.
- You can restore only the Main Configuration file using the **Configuration File Management** link on the Branch Device Manager interface. You can restore the Main Configuration file onto the same system type in which it was created. For example, a backup of the Main Configuration file on an i40 system can only be restored on an i40 system. You cannot backup one system type and use it to restore another system type.
- You must know the master key that is currently configured on Communication Manager Branch and the one that was configured during the time of the backup. They must be identical for the restore to be successful.
- The platform must have an IP address configured before a restore from a FTP server is executed.
  - An NVRAM init command deletes all configuration files including the IP addresses. After the NVRAM init command executes Branch Device Manager is used to configure the IP address for the platform. Once the IP addresses are configured the system reboots.

Supported FTP and SCP servers

The FTP and SCP servers listed in Table 9 are supported for Communication Manager Branch backups, restores, uploads and downloads.

Table 9: Supported FTP and SCP servers table

Server	Operating System	Version
FileZilla	Microsoft Windows	0.9.5
proFTPd	Linux	1.3.0
IIS	Microsoft Windows	5.0 and later
vsFTPd	Linux	2.0.3
wu-FTPd	Linux	2.6.2
PureFTP	Linux	1.0.21
Default FTP server	Solaris Sun OS	
OpenSSH	Microsoft Windows	3.8
OpenSSH	Linux Solaris Sun OS	4.6
WINSSHD	Microsoft Windows	4.23

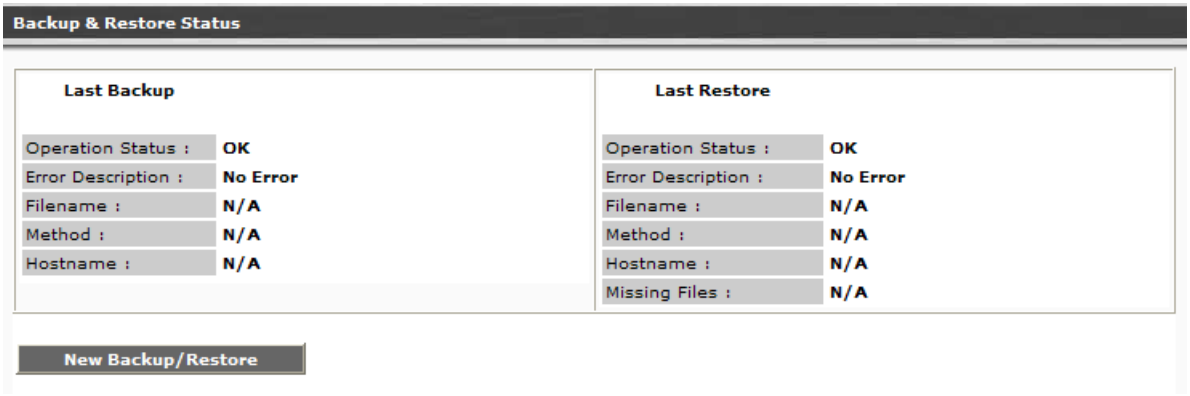
Procedure to restore from an FTP server

Using the Branch Device Manager interface, use the following steps to perform a restore from an FTP server:

1. Click **Backup and Restore** under the Maintenance and Monitoring > Configuration Administration.

   The **Backup and Restore Status** screen displays as shown in example Figure 42. The Backup and Restore Status screen contains information on the last backup and the last restore.

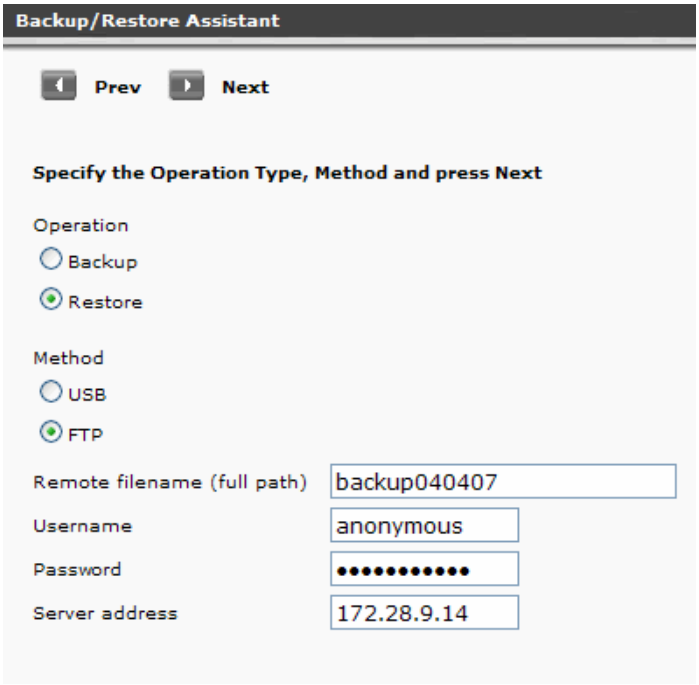
Figure 42: Backup and restore status screen



2. Click **New Backup/Restore**.

   The Backup and Restore Assistant screen appears as shown in example Figure 43. The Backup and Restore Assistant steps you through the restore operation.

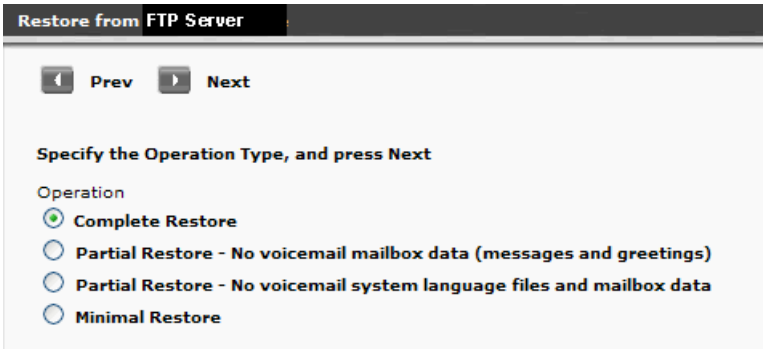
Figure 43: Backup and restore assistant screen



3. On the Backup/Restore Assistant screen choose:
   a. A restore operation by clicking the radio button next to **Restore**.
   b. **FTP** as the restore method: When FTP is selected, enter information in the following fields:
      - **Remote filename (full path)**: Enter a path of the FTP server that includes the filename of the backup to be restored. The path and file name can be up to 128 characters in length and cannot include illegal symbols such as *,:,?,|,{}, and a space.
      - **Username**: Enter the login for the FTP server. The Username can be up to 32 characters in length.
      - **Password**: Enter the password for the FTP server. The password can be up to 32 characters in length.
      - **Server address**: Enter the IP address of the FTP server or enter the hostname as it is defined in the system's DNS servers.
   c. Click **Next**.

   The **Restore from FTP Server** screen appears as shown in example Figure 44.

Figure 44: Restore Assistant - Restore from an FTP Server



4. Select the restore operation. The following is a detailed list of what is included in each restore operation. For a quick reference see Table 10.
   - **Complete Restore**: A complete restore can contain the following data:
     - Configuration files:
       - Translations
       - Installation profiles
       - Platform configuration information (IP addresses, Vlans, etc.)
       - Services configuration (DHCP server, NTP server, etc.)
       - Voice mail and auto attendant configuration.
       - SIP profile data
     - AES keytab file

- Alarm client configuration file: This file is used to send alarms to Avaya Services.
- Image files for the
- Locally stored IP phone files with a maximum size of 40MB that include the following:
  - A maximum of 40 scripts including the setting file, language files, and upgrade scripts
  - A maximum of 16 IP phone images
- System announcements: A complete restore includes up to 256 files with a maximum size of 7MB.
- Voice mail and system language files: A complete restore can include up to two files, with a maximum file size of 50MB for each file.
- Auto attendant files such as announcements and menu prompts
- Trusted certificates: A maximum of 10 trusted certificates can be restored. There is no backup and restore capability for the server certificate used for the HTTPS/SIP Proxy on the server. The server certificate is valid for a specific only. A new server certificate must be generated if the is changed.
- Unicode phone message files: The Unicode phone message files are used on H.323 type phones to support languages other than the default system languages.
- User voice mail boxes and greetings

Note:

The platform image, the service pack, and the media module firmware will be restored if they were added to the backup directory prior to the restore. For more information, see Creating a full backup on page 221.

- **Partial Restore**: This partial restore operation includes everything in the complete restore except for voice mail data such as messages and greetings. Choosing this restore reduces the size and the time for the restore. Voice mail data can add 250MB for the i40, 560MB for the Communication Manager Branch i120, and 790MB for the Communication Manager Branch G450.

Important:

There is no option available to restore only voice mail and user greetings. Choose the Complete Restore option to restore voice mail and user greetings.

- **Partial Restore**: This partial restore operation includes everything in the complete restore except for the voice mail system language files and the mailbox data. Choosing this restore reduces the size and time for the restore. Each system language file can add 10 to 50MB to the restore.
- **Minimal Restore**: A minimal restore contains administrator data only such as:
  - Configuration files: installation profiles
  - AES configuration file

- Unicode Phone message files
- Locally stored IP phone files for scripts and language files only. It does not include IP phone images.
- System announcements
- Auto Attendant files such as announcements and menu prompts
- Trusted certificates
- Alarm Client configuration file

Important:
A Minimal Restore does not include user information stored in the voice mail configuration file and SIP profile data.

Use Table 10 as a quick reference on what is included in each restore operation.

Table 10: Restore operation and contents

Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Translations	X	X	X	X
Installation profiles	X	X	X	X
Platform configuration information	X	X	X	X
Services configuration information	X	X	X	X
Voice mail and auto attendant configuration information	X	X	X	X
Voice mail boxes and greetings	X			
SIP profile data	X	X	X	
AES keytab file	X	X	X	X
Alarm client configuration file	X	X	X	X
Locally stored IP phone files	X	X	X	
System announcements	X	X	X	X
System language files	X			
Auto Attendant files such as announcements and menu prompts	X	X	X	X

1 of 2

Table 10: Restore operation and contents (continued)

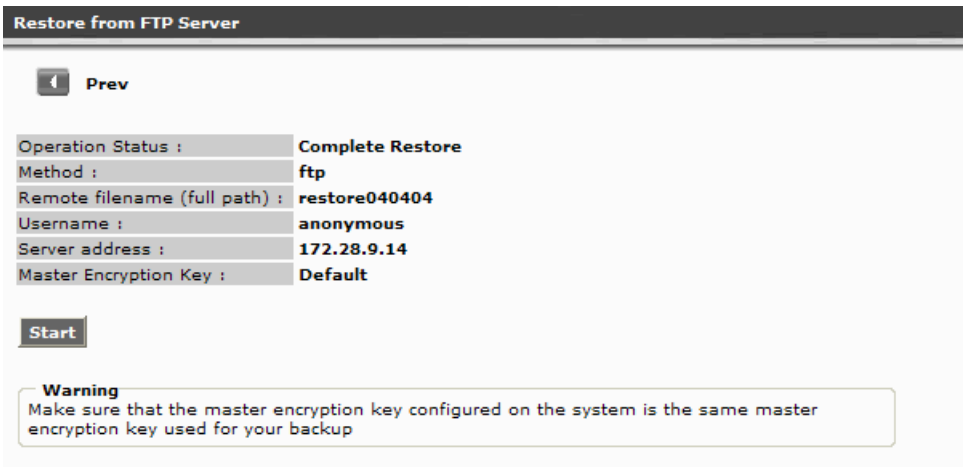
Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Trusted certificates	X	X	X	X
Unicode phone message files	X	X	X	X
				2 of 2

Important:

The voice mail configuration file, SIP profile data, and the Main Configuration file can be backed up and restored individually using **Configuration File Management** under Configuration Administration. If any of these files are restored to the active bank, a reboot must be performed.

Click **Next**. A window appears as shown in example Figure 45.

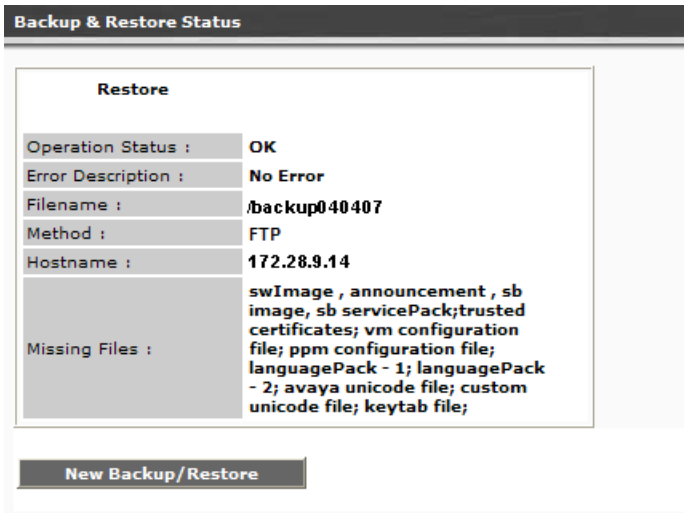
Figure 45: Restore from FTP Server - verify restore



5. Verify the restore operation, the method for the restore, and the directory name to be restored. If the information is correct, click **Start**.

   Before Communication Manager Branch starts the restore a message window appears. To continue with the restore, click **OK**. After clicking OK, the restore begins. A status window appears as shown in example Figure 46.

Figure 46: Backup and Restore Status screen



The Backup and Restore Status screen contains the following fields:

- Operation Status:
  - Executing: Executing displays while the operation is in progress.
  - OK: Displays if the operation is a success.
- Error Description: For a list of the restore errors and possible resolutions, see Table 12.
- Filename: This field displays the filename that you entered in the first assistant screen.
- Method: The method field displays FTP.
- Hostname: The IP address of the FTP server or the hostname as it is defined in the system's DNS servers.
- Missing Files: This field contains any files that were missing from the backup directory. This field is informational only and does not indicate that the restore was unsuccessful. You can obtain a copy of the missing file and restore the file at a later time.

During a restore operation information is written to the inactive bank. After the contents of the restore is verified the inactive bank is swapped with the active bank. If the restore contains the Main Configuration file, the system reboots.

Procedure to restore from a USB flash disk

Use the following steps to restore from a USB flash disk:

1. Insert the USB flash disk in the USB port on the platform. Refer to Figure 47 and Figure 48 for the location of the USB port.

Figure 47: USB port on the i40

Figure notes:

1. **USB port**

Figure 48: USB port on the Communication Manager Branch i120

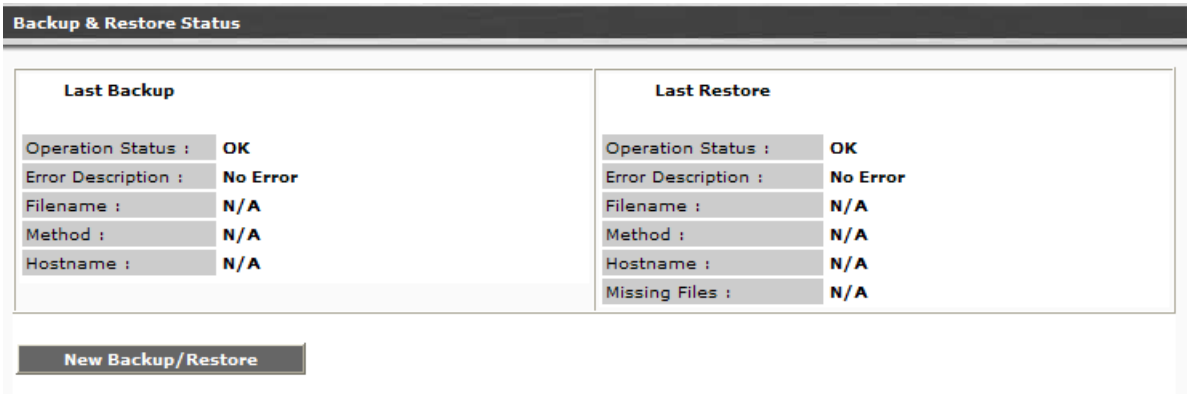
Figure notes:

1. **USB port**

2. Click **Backup and Restore** under the Maintenance and Monitoring > Configuration Administration.

   The **Backup and Restore Status** screen displays as shown in Figure 49. The Backup and Restore Status screen contains information on the last backup and the last restore.

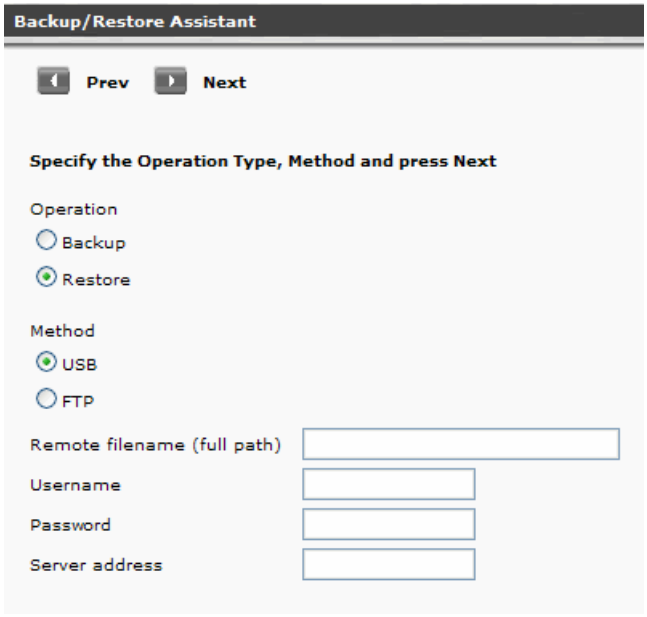
Figure 49: Backup and restore status screen



3. Click **New Backup/Restore**.

   The Backup and Restore Assistant screen appears as shown in Figure 50. The Backup and Restore Assistant steps you through the restore operation.

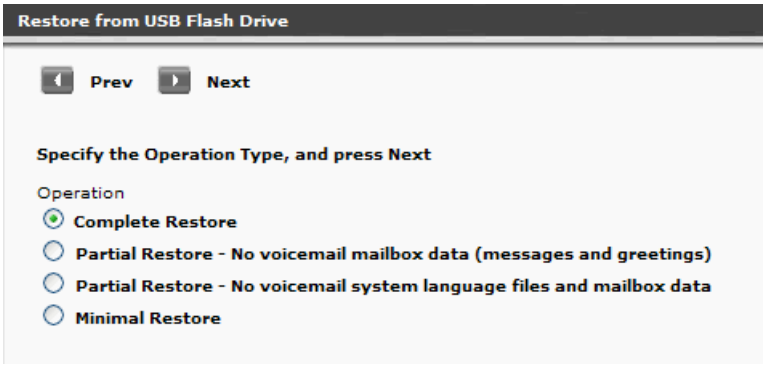
Figure 50: Backup/Restore Assistant screen



4. On the **Backup/Restore Assistant** screen choose:
   a. A restore operation by clicking the radio button next to **Restore**.
   b. **USB** as the restore method: When USB is selected the **Remote file name**, **Username**, **Password**, and **Server address** fields are inactive.

c. Click **Next**. The **Restore from USB Flash Drive** assistant appears as shown in example Figure 51.

Figure 51: Restore from USB Flash Drive



5. Select the restore operation. The following is a detailed list of what is included in each restore operation. For a quick reference see Table 11.

   - **Complete Restore**: A complete restore contains the following data:
     - Configuration files:
       - Translations
       - Installation profiles
       - Platform configuration information (IP addresses, Vlans, etc.)
       - Services configuration (DHCP server, NTP server, etc.)
       - Voice mail and auto attendant configuration.
       - SES profile data
     - AES keytab file
     - Alarm client configuration file: This file is used to send alarms to Avaya Services.
     - Locally stored IP phone files with a maximum size of 40MB that include the following:
       - A maximum of 40 scripts including the setting file, language files, and upgrade scripts
       - A maximum of 16 IP phone images
     - System announcements: A complete restore includes up to 256 files with a maximum size of 7MB.
     - Voice mail and system language files: A complete restore can include up to two files, with a maximum file size of 50MB for each file.
     - Auto Attendant files such as announcements and menu prompts

- Certificates: Up to 10 Trusted Certificates can be restored. There is no backup and restore capability for the server certificate used for the HTTPS/SIP Proxy on the server. The server certificate is valid for a specific only. A new server certificate must be generated if the is changed.
- Unicode phone message files: The Unicode phone message files are used on H.323 type phones to support languages other than the default system languages.
- User voice mail boxes and greetings

Note:

The platform image, the service pack, and the media module firmware will be restored if they were added to the backup directory prior to the restore. For more information, see Creating a full backup on page 221.

- **Partial Restore**: Choosing this restore reduces the size and the time for the restore by eliminating voice mail data such as messages and greetings. Voice mail data can add 250MB for the i40, 560MB for the Communication Manager Branch i120, and 790MB for the Communication Manager Branch G450.

Important:

There is no option available to restore only voice mail and user greetings. Use the Complete Restore operation to restore voice mail and user greetings.

- **Partial Restore**: Choosing this restore reduces the size and time for the restore by eliminating voice mail system language files and mailbox data. Each system language file can add 10 to 50MB to the restore.
- **Minimal Restore**: A minimal restore contains the following administrator data:
  - Configuration files and installation profiles
  - AES configuration file
  - Unicode Phone message files
  - Locally stored IP phone files of scripts and language files only. It does not include IP phone images.
  - System announcements
  - Auto Attendant files such as announcements and menu prompts
  - Trusted certificates
  - Alarm Client configuration file

Important:

A Minimal Restore does not include user information stored in the voice mail configuration file and SIP profile data.

Use Table 11 as a quick reference on what is included in each restore operation.

Table 11: Restore operation and contents

Files or directories	Complete	Partial w/o voice mail data	Partial w/o language files and mail boxes	Minimal
Translations	X	X	X	X
Installation profiles	X	X	X	X
Platform configuration information	X	X	X	X
Services configuration information	X	X	X	X
Voice mail and auto attendant configuration information	X	X	X	X
Voice mailboxes and greeting	X			
SIP profile data	X	X	X	
AES keytab file	X	X	X	
Alarm client configuration file	X	X	X	X
Locally stored IP phone files	X	X	X	X
System announcements	X	X	X	X
System language files	X			
Voice mail boxes and greetings	X	X		
Auto Attendant files such as announcements and menu prompts	X	X	X	X
Trusted certificates	X	X	X	X
Unicode phone message files	X	X	X	X

Important:

The voice mail configuration file, SIP profile data, and the Main Configuration file can all be backed up and restored individually using **Configuration File Management** under Configuration Administration. If any of these files are restored to the active bank, a reboot must be performed.

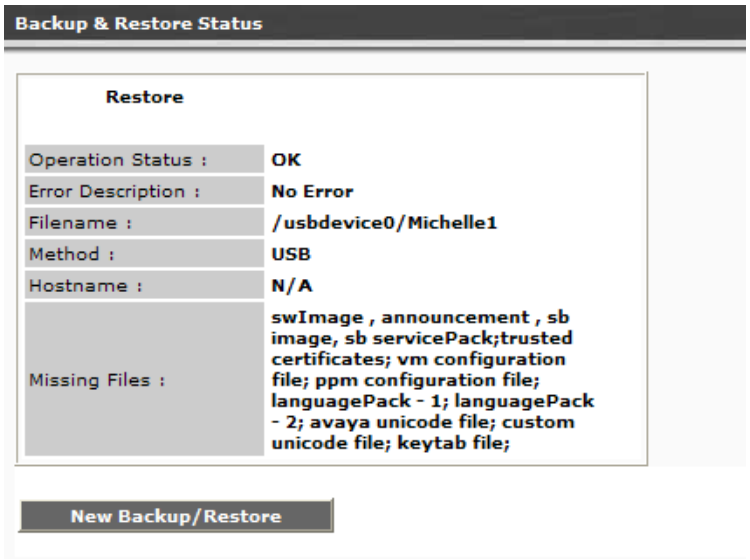
Click **Next**. A **Restore from USB Flash Disk** screen appears displaying the contents of the USB flash disk.

6. Use the Restore from USB Flash Drive screen shown in to:
   - View the contents of the USB flash disk: A list of directories on the flash disk appears under the Directories heading. The size of the directory appears under the Size heading.
   - Select one or more directories for the restore: To select to restore to an existing directory, click the box associated with the directory name and click **Next**.

     A window appears displaying the selections you have made for the restore.
7. Verify the restore operation, the method for the restore, and the directory name(s) to be restored. If the information is correct click **Start**.

   Before Communication Manager Branch starts the restore, a message window appears. To continue with the restore, click **OK**. After clicking OK the restore begins and a status window appears as shown in example Figure 52.

Figure 52: Backup and Restore Status screen



The **Backup and Restore Status** screen contains the following fields:

- **Operation Status**: This field can contain status information of:
  - **Executing**: Executing displays while the operation is in progress.
  - **OK**: Displays if the operation is a success
- **Error Description**: For a list of the restore errors and possible resolutions, see Table 12.
- **Filename**: This field displays the filename that you entered in the first assistant screen.
- **Method**: There are two methods of restores, FTP server and USB flash disk.
- **Hostname**: This field is not used if USB is selected.

- **Missing Files**: This field contains any files that were missing from the restore. This field is informational only and does not indicate that the restore was unsuccessful. You can obtain a copy of the missing file and restore the file at a later time.

During a restore operation, information is written to the inactive bank. After the contents of the restore is verified, the inactive bank is swapped with the active bank. If the restore contains the Main Configuration file, the system reboots.

Troubleshooting a failed restore

In general, a restore using an FTP server fails if there are network connectivity issues and all restores fail if the restore reaches the maximum size of 180MB.

Use the information in Table 12 for help troubleshooting restore error messages.

Table 12: Restore error messages and resolution table

Error message	Description	Resolution
Server unreachable	This error message appear when a PING to the FTP server fails.	Verify that the FTP server is accessible from Communication Manager Branch: 1. Using Branch Device Manager, click Network Diagnostics under Maintenance and Monitoring. 2. Click the radio button next to PING, enter the address of the FTP server and click Start. If PING fails, troubleshoot the network problems.
FTP error - invalid login parameters or configuration error	This error is caused by incorrect configuration information such as a incorrect username or password, or wrong IP address.	Verify the username, password and IP address of the FTP server and try again.
Restore directory does not exist	Wrong backup directory name	Verify the backup directory name and spelling.
		1 of 4

Table 12: Restore error messages and resolution table (continued)

Error message	Description	Resolution
Restore failed: image	The restore image did not pass validation. The backup image is not an Avaya signed image.	Find another backup with a valid backup image and use it for the restore.
Restore failed: service pack	The restore service pack did not pass validation. This could be because the restore service pack is not an Avaya signed service pack or that the service pack version is not compatible with the image that was restored.	Find another backup with a valid service pack and use it for the restore. If you changed the service pack version on the backup prior to the restore and you still have a copy of the old version, copy the old version back to the backup directory and remove the new version.
Restore failed: Configuration Database	This error can be caused by one of the following: ● Different Master encryption key was used to encrypt this file than the one that is being used on the system ● The file was modified or replaced ● The device was busy by another configuration tool such as Branch Device Manager or Branch Central Manager.	When creating a backup, you must ensure that the master encryption key used to create the file and the one currently on the system are identical. Modification or replacement of backup files is prohibited. If the system is busy with another configuration tool, terminate the configuration session and try the restore again. If the system incorrectly indicates that a configuration session exists, reboot the system.
Restore failed: Voice mail configuration file	The voice mail is configuration file is incompatible (it has been modified or replaced).	Modification or replacement of the voice mail file is prohibited.
Restore failed: SIP profile data	The SIP profile data file is incompatible (it has been modified or replaced).	Modification or replacement of the SIP profile data file is prohibited.
		2 of 4

Table 12: Restore error messages and resolution table (continued)

Error message	Description	Resolution
Restore failed: IP phone image	IP phone images can be installed by a user. Communication Manager Branch allows a maximum of 16 images. The combination of images and scripts cannot exceed 40MB in size.	This error message only occurs if IP phone files were manually added. If the total size of the IP phone images, the scripts, and the language files exceed 40MB, the restore operation will fail.
Restore failed: IP phone script	IP phone scripts can be installed by a user. Communication Manager Branch allows a maximum of 40 scripts. The combination of IP images and scripts cannot exceed 40 MB in size.	This error message only occurs if IP phone files were manually added. If the total size of the IP phone images, the scripts, and the language files exceed 40MB, the restore operation will fail.
Restore failed: System language file	This message appears if non-Avaya system language files have been installed.	Remove the non-Avaya system language files from the backup. You can download new language files from the Avaya support Web site at http://support.avaya.com.
Restore failed: Voicemail boxes	The voice mail boxes are incompatible or a size limit has been exceeded. The size of the voice mailboxes and user greeting is configurable.	Verify that the size limit was not exceeded. If additional files were installed in the VOICEMAILBOXES directory, remove the files and try the restore again.
Restore failed: Installation profile files	The installation profile files are incompatible.	The installation profile files are damaged. Find another backup and try the restore again.
Restore failed: Installation task file	The installation task file is incompatible.	The installation profile files are damaged. Find another backup and try the restore again.
Restore failed: alarm client configuration file	The alarm client configuration file is incompatible.	The alarm client configuration file is damaged. Find another backup and try the restore again.
Restore failed: Keytab file	The Keytab file is incompatible.	The Keytab file is damaged. Find another backup and try the restore again.
		3 of 4

Table 12: Restore error messages and resolution table (continued)

Error message	Description	Resolution
Restore failed: Trusted Certificate	The Trusted Certificate is incompatible.	Verify that the correct trusted certificate is being restored. Be sure to use certificates from trusted sources only.
Restore failed: Avaya Unicode file	Communication Manager Branch Communication Manager Branch could not validate the format of the Unicode file. The Avaya Unicode file may have been modified or replaced.	Obtain an new Unicode file from the Avaya support site at http://support.avaya.com.
Restore failed: Custom Unicode file	Communication Manager Branch could not validate the format of the Custom Unicode file. The Custom Unicode file may have been modified or replaced.	Obtain an new Unicode file from the Avaya support site at http://support.avaya.com.
		4 of 4

Restoring the firmware, images, and service pack

The platform and the media module firmware, and the service pack can be downloaded from the http://support.avaya.com Web site. After the files have been downloaded from the support web site use the steps outlined in this section to download/install the files onto Communication Manager Branch.

To download/install the platform image file and the service pack on Communication Manager Branch:

1. Click **Device** under Firmware Management in the Branch Device Manager interface.
2. Click the **Image Download Process** tab.
3. Select the image type and the download method. Additional fields may display as required by the download method. Fill in any additional fields and click **Start**.

To download/install the media module firmware:

1. Click **Media Module** under Firmware Management in the Branch Device Manager interface.
2. Select the media module by clicking the associated radio button.
3. Select the download method. Additional fields may display as required by the download method. Fill in any additional fields and click **Start**.

Rebooting Communication Manager Branch

In the rare event that Communication Manager Branch is not responding or where problems exist for all users at the location, you may need to reboot.

Reboots can be performed through the Branch Device Manager interface or by depressing the reset button on the system's hardware.

Before you reboot

It is important to understand that each image on Communication Manager Branch contains two boot banks, bank A and bank B. A boot bank is a partition in the flash disk that contains the version of Communication Manager Branch, configuration and administration information, etc. At any one given time, one boot bank will be active while the other is inactive. It is possible that the boot banks may contain different information. If the active boot bank becomes corrupted, you can swap boot banks and reboot Communication Manager Branch. The ability to swap banks is particularly important when you are upgrading to new versions of Communication Manager Branch. For information on swapping boot banks using Branch Device Manager, see Reboot using Branch Device Manager on page 244. For information on swapping boot banks using Communication Manager Branch hardware, see Reboot using Hardware on page 246.

In most cases, performing a reboot is service affecting. Rebooting the system should only be done in rare situations such as:

- An inability to make or receive calls
- During maintenance procedures like upgrades
- If you are instructed to do so by a procedure outlined in this book
- If you are instructed to do so by a support person

What happens when you reboot

This section explains what happens when you reboot the Communication Manager Branch system.

Rebooting the Communication Manager Branch system

Rebooting the platform is service affecting. You can expect the following things to happen during the reboot:

- New analog calls or Public Switched Telephone Network (PSTN): A user will not be able to place a new call.
- New H.323 calls: The user will not have dial tone and will not be able to place a new call.
- New SIP to SIP calls: During the reboot of the platform, the SIP user will not be able to place a new call.
- H.323, PSTN, or analog calls in progress: Any call in progress using H.323, PSTN, or an analog station will be terminated.
- Existing PSTN or analog calls: All established PSTN or analog calls will be terminated.
- Existing SIP to SIP calls: All established SIP to SIP calls will remain active.
- Existing H.323 to H.323 calls: All established H.323 to H.323 calls will remain active.
- Existing H.323 to SIP and H.323 to inter-branch calls: All established calls will be terminated.
- Calls using media gateway resources: Any call that is using media gateway resources will be terminated.
- Calls to voice mail: Any new calls, calls in progress, or established calls to voice mail will be terminated.
- Stations connected to the platform using PoE: All stations connected to the Communication Manager Branch i120 using PoE will be terminated. All stations connected to the i40 using PoE will remain active.

  Note:

  The Communication Manager Branch G450 platform does not support PoE.

To reboot the Communication Manager Branch i40, i120, or G450 using the reset button, see Reboot the Communication Manager Branch i40, 120, or G450 platform on page 247. To reboot the Communication Manager Branch i40, i120, or G450 using the Branch Device Manager interface, see Reboot using Branch Device Manager on page 244. To reboot the

Reboot using Branch Device Manager

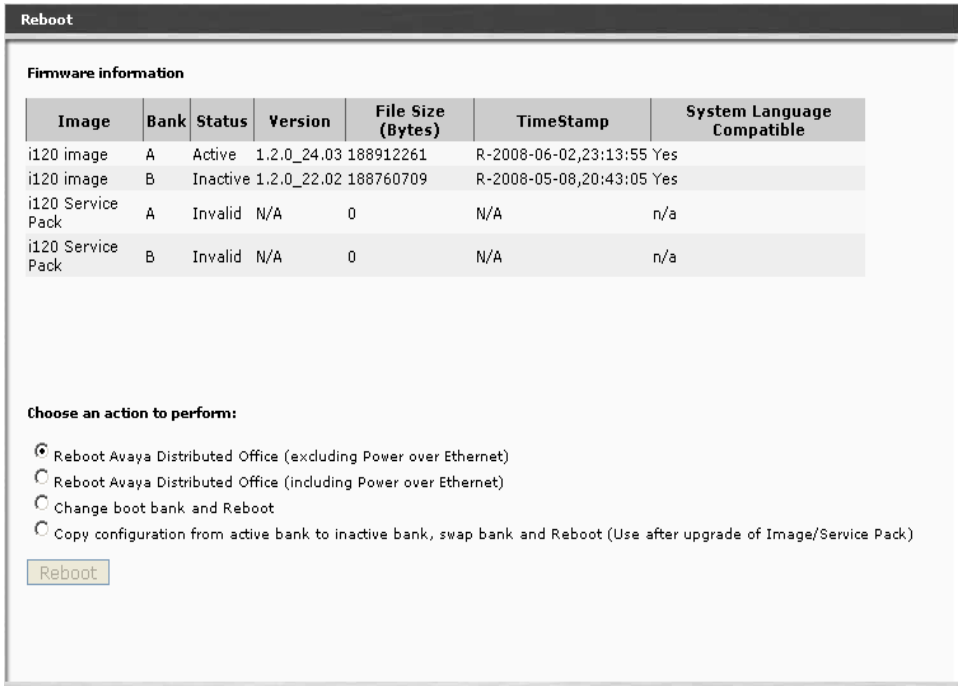
If at all possible, use the Branch Device Manager interface to reboot the platform. When Branch Device Manager is used to reboot the platform, a graceful shutdown is performed reducing the chances of software corruption.

Use the following steps to perform a reboot using Branch Device Manager:

1. Click **Reboot** under Maintenance and Monitoring.

   The Reboot screen displays as shown in example Figure 53.

Figure 53: Branch Device Manager Reboot screen



There are two sections to the Reboot screen, **Firmware information** and **Choose an action to perform**.

The **Firmware information** section displays the following information:

- **Image**: There are three images on Communication Manager Branch:
  - Platform
  - image.
  - SP: Service Pack
- **Bank**: The Bank column displays the banks on each image. There are two banks for each image, bank A and bank B.
- **Status**: The Status column displays the status of a bank. A bank can be either active or inactive.
- **Version**: The software version and service pack displays.
- **Size**: The size of the boot bank for the image displays in bytes.
- **Timestamp**: The time the image was loaded displays.
- **Is Lang. Pack Compatible**: Communication Manager Branch supports up to two language packs simultaneously. Language packs can contain different structures indicated by the version of the pack. The **Is Lang. Pack Compatible** field is used to display whether the image supports a language pack version that has been loaded. If the

image does not support the language pack version and a reboot to that image is performed, voice mail will not work.

2. In the **Choose an action to perform** section, select one of the following options:

Note:

Some reboot options affect service more than others. For information on the impact a reboot option has on the system, see What happens when you reboot on page 243.

- **Reboot Communication Manager Branch (excluding Power over Ethernet)**: This option reboots the entire system, but does not power down the PoE ports.
- **Reboot Communication Manager Branch (including Power over Ethernet)**: This option reboots the entire system and powers down the PoE ports.
- **Change the boot bank and reboot**: This option allows you to swap the active and inactive boot banks of the platform prior to rebooting the Communication Manager Branch. When the reboot is complete, the boot bank that was inactive prior to the reboot will be active.
- **Copy configuration from the active bank to inactive bank, swap bank and reboot**: You can use this option to copy the configuration information from the active bank of the Communication Manager Branch to the inactive bank of the Communication Manager Branch. This option allows you to copy the most current configuration information over to the inactive bank (that may contain older information), swap into the inactive bank and reboot.

  This option can be used when an upgrade is performed at the same time configuration or administration changes are being made. In this case, this option must be selected or all the latest changes will be lost.

3. Click **Reset**.

The system displays a status bar showing the reboot progress.

Reboot using Hardware

This section explains how to reboot the Communication Manager Branch i40, i120, and G450 using the hardware.

Reboot the Communication Manager Branch i40, 120, or G450 platform

Use this procedure if you want to reset Communication Manager Branch using the current active bank:

1. Press and hold the reset button.
2. Release the reset button.

Swap boot banks and Reboot the Communication Manager Branch i40, i120, or G450 platform

Use this procedure if you want to swap the active bank of the Communication Manager Branch i40, i120, or G450 to the inactive bank and reset the platform. To do this procedure you must depress both the reset (labeled RST on the platform) and the Alternate Software Bank (labeled ASB on the platform) buttons:

1. Press and hold the ASB button.
2. Press and hold the reset button.
3. Release the reset button.
4. Release the ASB button.

LEDs during the reboot of the Communication Manager Branch i40, i120, or G450

When rebooting the Communication Manager Branch i40, i120, or the G450:

- The system red ALM LED turns on
- The system green CPU LED turns off
- Various LEDs turn off and on or blink during the reboot process

After the Communication Manager Branch i40, i120, or the G450 has rebooted:

- The green ETR LED turns off
- The system red LED turns off
- The system CPU and PWR LEDS are on

Index

Numerical

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V