

Firmware Download Procedures

Firmware download procedures give you the capability to download new firmware to one or more programmable circuit packs of the same type residing within the same system. Programmable circuit packs have a “P” in their suffix. For example TN799DP is programmable, but TN799C is not. This programmable capability reduces the need to physically remove circuit packs and return them to Avaya for firmware updates.

This description contains the most accurate information available at the time of production. Go to the Avaya Support Web site (<http://www.avaya.com/support>) and click on **Downloads** for the most recent information about downloading firmware.

This document includes the following sections:

- [Overview of process and circuit packs](#) on page 1
- [Self and C-LAN-distributed download procedure](#) on page 4
- [Download from SCP-enabled file server procedure](#) on page 20
- [IPSI and SIPI download procedure](#) on page 28
- [Using Software Update Manager for centralized firmware download](#) on page 39
- [Troubleshooting firmware downloads](#) on page 39

Overview of process and circuit packs

Firmware download process

During the firmware download process, a firmware image is installed on a circuit pack in three steps:

1. The image is copied from an Avaya server over the Web to a local “staging area” — a PC or server on the customer LAN.
2. The image is copied from the local staging area to the **source** circuit pack or media server.
3. The image is downloaded from the **source** to the **target** with one of these methods:
 - **Self-download** ([Self and C-LAN-distributed download procedure](#)) - image is downloaded directly from RAM (the **source**) to flash memory (the **target**) on the same circuit pack
 - **C-LAN-distributed download** ([Self and C-LAN-distributed download procedure](#)) - image is downloaded from RAM (the **source**) on a C-LAN circuit pack to flash memory (the **target**) on one or more separate circuit packs of the same type

- **IPSI or SIPI download** ([IPSI and SIPI download procedure](#)) - image is downloaded from a **source** media server to one or all **target** IPSI circuit packs
- **Download from file server** - image is downloaded from an **SCP-enabled file server** to one or all **target** circuit packs

Circuit packs

Although different circuit packs have different potential roles in a firmware download, currently the following circuit packs can participate in a firmware-download procedure. Additional packs will be added in the future.

- Maintenance/Test (M/T-ANL) – TN771DP
- Control LAN (C-LAN) – TN799C or TN799DP
- 2-Wire Digital Line (DIG-LINE) – TN2214CP or TN2224CP
- IP Media Processor (IPMEDPRO) – TN2302AP
- IP Server Interface (IPSI) – TN2312AP, TN2312BP
- S8400 IP Interface (SIPI) – TN8412AP
- UDS1 – TN464GP, TN2464BP, and TN2313AP
- Voice Announcements over LAN (VAL) – TN2501AP
- IP Media Resource 320 (IPMEDRES) – TN2602AP

In a firmware download to IPSIs or a SIPI, the media server is the source and the IPSIs or SIPI are the targets. For downloads to all other circuit packs, the download from an SCP-enabled file server method is available, or see [Table 1](#) for each circuit pack's roles in other firmware download methods.

Table 1: Non-IPSI Circuit-Pack Roles in Firmware Downloads

Circuit Pack	TN Code	Role in Self Download	Role in C-LAN-distributed Download
Maintenance/Test	TN771DP		Target
C-LAN	TN799C ¹		Source
	TN799DP ²	Source and Target	Source
DIG-LINE (2-wire)	TN2214CP		Target
	TN2224CP		Target
<i>1 of 2</i>			

Table 1: Non-IPSI Circuit-Pack Roles in Firmware Downloads (continued)

Circuit Pack	TN Code	Role in Self Download	Role in C-LAN-distributed Download
IP Media Processor	TN2302AP ³		Target
IP Media Resource 320	TN2602AP	Source and Target	
VAL	TN2501AP	Source and Target	
UDS1	TN464GP		Target
	TN2464BP		Target
	TN2313AP		Target
2 of 2			

1. The TN799C C-LAN circuit pack can be the "source" for a C-LAN-distributed download but cannot be the "target" circuit pack for either a self or C-LAN-distributed download since it is not a programmable circuit pack (no "P" suffix).
2. The TN799DP can be both source and target for a self download and can be the source for a C-LAN-distributed download.
3. For TN2302AP circuit packs with a vintage less than 22, a different download procedure is required that is not described here. Go to the Avaya Support Web site (<http://www.avaya.com/support>). Under **Downloads**, click on the "D" under "Download by Product Name." Click on **DEFINITY ECS**, and then **TN2302AP (MedPro) Firmware Downloads**. Choose the firmware download needed. Open the Read_Me file for more information and the download procedure.

If you need to download new firmware to an IPSI or SIPI, use the [IPSI and SIPI download procedure](#) on page 28. Otherwise, use the [Self and C-LAN-distributed download procedure](#) on page 4.

Self and C-LAN-distributed download procedure

This section describes the procedures for either a self or C-LAN-distributed firmware download. These procedures will help you determine which method to use. The main differences between the two methods are:

- | | |
|----------------------------|---|
| C-LAN-distributed download | <ul style="list-style-type: none">● The “source” circuit pack is always a C-LAN, either TN799DP or TN799C.● Multiple “target” circuit packs of the same TN code can be scheduled for download at a time. |
| Self-download | <ul style="list-style-type: none">● The “source” and “target” circuit packs are the same.● Each circuit pack must be scheduled for download individually. |

The high-level procedures for a self or C-LAN-distributed firmware download are:

1. [Prepare for download](#) on page 5
2. [Upload image file from Web to staging area](#) on page 9
3. [FTP/SFTP the image file to the source circuit pack](#) on page 9
4. [Schedule the download](#) on page 11
5. [Verify the download schedule](#) on page 16
6. [Monitor download progress](#) on page 16
7. [Disable FTP/SFTP file system](#) on page 18

Note:

If you have any trouble with this procedure, refer to [Troubleshooting firmware downloads](#) on page 39.

Prepare for download

The following sub-sections contain procedures to prepare for the firmware downloads to target circuit packs. These sub-sections are:

- [Choose an appropriate source circuit pack](#) on page 5
- [Verify hardware/software requirements](#) on page 6
- [If DS1-C \(DS1 converter complex\), verify a clear channel](#) on page 6
- [Get circuit pack information](#) on page 7
- [Enable FTP/SFTP file system on source circuit pack](#) on page 8

Choose an appropriate source circuit pack

Given the type of target circuit pack to be upgraded, choose the source circuit pack from the following table ([Table 2](#)). The last column indicates which download method must be used with the target and chosen source.

Table 2: Download Method by Circuit Pack

Target Circuit Pack(s)	Source Circuit Pack	Download Method
TN464GP, TN2464BP, and TN2313AP (UDS1)	TN799C or TN799DP	C-LAN-distributed
TN2214CP or TN2224CP (DIG-LINE)	TN799C or TN799DP	C-LAN-distributed
TN771DP (Maintenance/Test)	TN799C or TN799DP	C-LAN-distributed
TN2302AP (IP Media Processor) ¹	TN799C or TN799DP	C-LAN-distributed
TN2602AP (IP Media Resource)	TN2602AP	Self
TN799DP (C-LAN)	TN799DP	Self
TN2501AP (VAL)	TN2501AP	Self

1. For TN2302AP circuit packs with a vintage less than 22, a different download procedure is required that is not described here. Go to the Avaya Support Web site (<http://www.avaya.com/support>). Under **Downloads**, click on the "D" under "Download by Product Name." Click on **DEFINITY ECS**, and then **TN2302AP (MedPro) Firmware Downloads**. Choose the firmware download needed. Open the Read_Me file for more information and the download procedure.

Verify hardware/software requirements

Before starting the upgrade procedure, you need several items.

✓	Item
	Superuser or Services login and password to DEFINITY or Communication Manager
	PC or other server with the following:
	● IP connectivity to the source board
	● IP connectivity to the World-Wide Web
	● File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) software program

Note:

Some GUI-based FTP applications are incompatible with Communication Manager/DEFINITY. Command-line FTP applications launched from a UNIX shell or DOS prompt work best.

If DS1-C (DS1 converter complex), verify a clear channel

If you need to distribute firmware from a source C-LAN to target boards on a DS1-C (DS1 converter complex) remote port network, then make sure there is a clear channel between the source C-LAN and those target boards.

To confirm this clear channel, follow these steps:

1. At the SAT prompt, enter `list fiber-link` and find the link between the source C-LAN and the target boards.
2. Enter `display fiber-link n`, where *n* is the fiber link's number.
The Fiber Link Administration screen displays.
3. Go to the second page of the Fiber Link Administration screen and verify that the **Line Coding** fields are set to **b8zs** for T1 facilities and **hdb3** for E1 facilities.
4. If they are not, then escalate before proceeding with the firmware download.

Get circuit pack information

To obtain system configuration information:

1. At the SAT, enter **list configuration all**.

The **System Configuration** screen ([Figure 1](#)) appears.

Figure 1: System Configuration screen

```
list configuration all
```

SYSTEM CONFIGURATION												
Board		Code	Vintage	Assigned Ports								
Number	Board Type			u=unassigned	t=tti	p=psa						
01A08	IP MEDIA PROCESSOR	TN2302AP	HW03 FW044	01	02	03	04	05	06	07	08	
01A04	CONTROL-LAN	TN799DP	HW00 FW005	u	u	u	u	u	u	u	u	u
				u	u	u	u	u	u	u	u	u
												17
01B04	DS1 Interface	TN464GP	HW02 FW006	01	02	03	04	05	06	07	08	
				09	10	11	12	13	14	15	16	
				17	18	19	20	21	22	26	24	
				u	u	u	u	u	u	u	u	u
01B05	DS1 Interface	TN464GP	HW02 FW006	01	02	03	04	05	06	07	08	
				09	10	11	12	13	14	15	16	
				u	u	u	u	u	u	u	u	u
				u	u	u	u	u	u	u	u	u
01B06	DS1 Interface	TN464F	000038	01	02	03	04	05	u	u	u	
				u	u	u	u	u	u	u	u	
				u	u	u	u	u	u	u	u	
				u	u	u	u	u	u	u	u	
01A10	VAL-ANNOUNCEMENT	TN2501AP	HW01 FW004	01	02	03	04	05	06	07	08	
				09	10	11	12	13	14	15	16	
				17	18	19	20	21	22	26	24	
				25	26	27	28	29	30	31	32	
												33

2. Check the target circuit pack(s). If the suffix in the **Code** field does not have a "P" (for example, TN2302AP), a firmware download is not possible.
3. Verify that a firmware download is needed by checking the firmware vintage(s) in the **Vintage** field of the target circuit pack(s).
4. Record the location in the **Board Number** field of each source and target circuit pack.
5. If a C-LAN is the source, make sure port 17 is assigned on that C-LAN. If it is not assigned, administer the port using the SAT command **add data-module UUC17**.

6. For a self download to a VAL board, make sure that port 33 is assigned on the VAL board. If it is not assigned, administer the port using the SAT command **add data-module UUC33**.
7. Determine the IP address of the source circuit pack. You can either ask the data systems administrator or enter the following SAT command sequence:
 - a. Type **display ip-interfaces**. Find the source circuit pack's **Slot** location and write down its **Node Name**.
 - b. Type **display node-names ip**. Find the source circuit pack's **Node Name** and write down its **IP Address**.

Enable FTP/SFTP file system on source circuit pack

Before files can be copied to the source circuit pack, you must set up an FTP/SFTP file system on the source circuit pack to accept the files.

1. Log into the SAT using a superuser or services login and password.
2. Enter **enable filexfer**.

The system displays the **Enable File Transfer** screen ([Figure 2](#)).

Figure 2: Enable File Transfer screen

enable filexfer	Page 1 of 1
ENABLE FILE TRANSFER	
Login: _____	
Password: _____	
Password: _____	
Secure? y	
Board Address: _____	

-
3. Type a 3-6 alphabetic character login in the **Login** field.
 4. Type a 7-11 character password (at least one letter and one number) in the first **Password** field.
 5. Retype the same password in the second **Password** field.
 6. In the **Secure** field:
 - if a C-LAN or VAL circuit pack, type **y** to enable SFTP.
 - if an IP Media Resource circuit pack, type **n** to enable FTP.
 7. Press **Enter**.

FTP/SFTP is now enabled on the circuit pack, and the login/password are valid until you disable the session.

This completes the preparation for a firmware download.

Upload image file from Web to staging area

For an upload from the Web, you need a temporary staging area to store the firmware images before downloading them to a circuit pack.

The staging area can be any of the following server types:

- PC platform
- UNIX platform
- Linux-based media server

To upload an image file from the Web:

1. Go to the Avaya Support Web site (<http://www.avaya.com/support>). Follow the **Downloads** link and the subsequent links for your product and the target circuit pack TN code.
2. Find the section for the firmware vintage you want. Unless otherwise instructed, choose the highest vintage.
3. Read that vintage's ReadMe file before downloading the image file(s).
4. Click on an image file name.
5. Save this file to a local staging area directory.
6. Write down the path to the local staging area and the filename of the firmware image. You will need to enter this information later.
7. Repeat steps 4 to 6 for each image file that the ReadMe file indicates should be downloaded for that circuit pack and vintage.

FTP/SFTP the image file to the source circuit pack

For VAL and C-LAN circuit packs, use SFTP to transfer the image file from the staging area to the source circuit pack. For the IP Media Resource circuit pack, use FTP to transfer the image file.

To FTP or SFTP the image file from the staging area to the source circuit pack:

1. Open a DOS interface or UNIX/Linux shell from the laptop, PC, UNIX, or Linux system (the local staging area).
2. Change the directory to the staging area using the command:

```
cd /your-staging-area
```

Verify that the new firmware image file is in the local staging area directory.

Firmware Download Procedures

3. List the contents of the directory showing the most recent files last using the following command:

`ls -ltr` on Linux/UNIX

or

`dir /od` on DOS.

4. Enter `ping ip_address` to verify a communication link to the source circuit pack, where `ip_address` is the IP address of the source circuit pack.
5. **For IP Media Resource:** Enter `ftp ip_address`, where `ip_address` is the IP address of the source circuit pack, to enter the FTP interface with a link to the source.

or

For VAL and C-LAN: Enter `sftp ip_address`, where `ip_address` is the IP address of the source circuit pack, to enter the SFTP interface with a link to the source.

6. Log into the FTP or SFTP session with the same login and password that you created in [Enable FTP/SFTP file system on source circuit pack](#) on page 8.
7. Enter `binary`. This requests that files be transferred in binary format.



CAUTION:

Files will be corrupted during transfer if you don't enter this `binary` command.

8. If you are self downloading to a VAL circuit pack, enter:

`cd /`

This command moves you from the announcement directory (default for an SFTP session on the VAL board) to the root directory ("/"), where firmware and other files reside. This will keep the firmware image file separate from the announcement files.

9. Enter `put filename.ext` to copy the new firmware image file to the source directory in RAM.
10. Repeat step 9 for each new firmware image file.
11. Enter `ls` to verify that the new firmware image file(s) is on the circuit pack.
12. Enter `bye` to end the FTP/SFTP session.

Schedule the download

You can schedule the download to occur immediately or at a later date and time. The procedures for self and C-LAN-distributed download methods differ at this step.

1. In a SAT session, enter **change firmware download**.

The **Firmware Download** screen displays, [Figure 3](#)

2. Fill in the fields on this screen. Field descriptions are described in [Table 3](#).

If you are performing a self download, enter only one target board location. This target board location is the same as the source board location. See [Figure 3: Firmware Download Screen for a Self Download](#) for an example of self download to a VAL board.

If you are performing a C-LAN-distributed download, enter a C-LAN location as the source and 1 - 50 target locations, where the target boards are all of the same type.

[Figure 4: Firmware Download Screen for a C-LAN-distributed Download](#) is an example of a C-LAN-distributed download to two UDS1 boards.

Figure 3: Firmware Download Screen for a Self Download

change firmware download				Page	1 of	1
FIRMWARE DOWNLOAD						
Source Board Location: 01A10						
File Retrieval Protocol: SCP Login: 8\$abc7& Password:						
Firmware Image File Name: tn2501ap_f05.bin						
Target Board Code: TN2501 Suffix: AP Firmware Vintage:						
Schedule Download? y Remove Image File After Successful Download? y						
Start Date/Time: 09/12/2005 13:30 Stop Date/Time: 09/12/2005 16:30						
Target Location	Target Location	Target Location	Target Location	Target Location	Target Location	Target Location
1. 01A10	11. _____	21. _____	31. _____	41. _____	51. _____	61. _____
2. _____	12. _____	22. _____	32. _____	42. _____	52. _____	62. _____
3. _____	13. _____	23. _____	33. _____	43. _____	53. _____	63. _____
4. _____	14. _____	24. _____	34. _____	44. _____	54. _____	64. _____
5. _____	15. _____	25. _____	35. _____	45. _____	55. _____	65. _____
6. _____	16. _____	26. _____	36. _____	46. _____	56. _____	66. _____
7. _____	17. _____	27. _____	37. _____	47. _____	57. _____	67. _____
8. _____	18. _____	28. _____	38. _____	48. _____	58. _____	68. _____
9. _____	19. _____	29. _____	39. _____	49. _____	59. _____	69. _____
10. _____	20. _____	30. _____	40. _____	50. _____	60. _____	70. _____
Enter 5 character board number; cabinet (1-30):carrier (A-E):slot (0-20)						

Figure 4: Firmware Download Screen for a C-LAN-distributed Download

change firmware download

FIRMWARE DOWNLOAD

Page 1 of 1

Source Board Location: 01A04

File Server:

File Retrieval Protocol: SCP

Login:

Password:

Firmware Image File Name: usd1v22r1

Target Board Code: TN464

Suffix: GP

Firmware Vintage:

Schedule Download? y

Remove Image File After Successful Download? y

Start Date/Time: 10/08/2005 22:00

Stop Date/Time: 10/08/2005 22:30

Target Location	Target Location	Target Location	Target Location	Target Location
1. 01B04	11. _____	21. _____	31. _____	41. _____
2. 01B05	12. _____	22. _____	32. _____	42. _____
3. _____	13. _____	23. _____	33. _____	43. _____
4. _____	14. _____	24. _____	34. _____	44. _____
5. _____	15. _____	25. _____	35. _____	45. _____
6. _____	16. _____	26. _____	36. _____	46. _____
7. _____	17. _____	27. _____	37. _____	47. _____
8. _____	18. _____	28. _____	38. _____	48. _____
9. _____	19. _____	29. _____	39. _____	49. _____
10. _____	20. _____	30. _____	40. _____	50. _____

Enter 5 character board number; cabinet (1-30):carrier (A-E):slot (0-20)

See [Table 3: Firmware Download fields and descriptions](#) for the field descriptions for the Firmware Download screens.

Table 3: Firmware Download fields and descriptions

Field	Description	Notes
Source Board Location	The location of the source circuit pack.	For a self download, the same board is the source board and target board. For a C-LAN-distributed download, this is the source C-LAN location.
Firmware Image File Name	The complete filename of the new firmware image file. If the list directory board command showed that the file had an extension, such as .bin, include the extension.	

1 of 3

Table 3: Firmware Download fields and descriptions (continued)

Field	Description	Notes
Target Board Code	The circuit pack ID. For example, TN2501 Do not type the suffix, such as AP, D", or GP in this field (type the suffix in the Suffix field).	Enter the TN code of the target circuit pack(s). For a self download, the target is the same as the source circuit pack.
Suffix	Type the suffix. Examples: • For VAL (TN2501AP), AP. • For C-LAN (TN799DP), DP. • For DS1 (TN464GP), GP.	
Firmware Vintage	This field is blank.	You can view the firmware vintage on the Firmware Download screen. Use the command display firmware download or status firmware download to display the Firmware Download screen.
Schedule Download	Type y to schedule the firmware download for another time. Type n to start the firmware download immediately after completing the screen.	Once the firmware download begins, you cannot make any changes to this screen. You can only disable this schedule using the disable firmware download command and then start a new one. (See Aborting a firmware download on page 40 for instructions.) If you type n , then the Start Date/Time and Stop Date/Time fields disappear. The download begins as soon as you press Enter .
2 of 3		

Table 3: Firmware Download fields and descriptions (continued)

Field	Description	Notes
Remove Image File After Successful Download	Type y if you want the procedure to automatically remove the new firmware image file [default]. Type n if you do not want the new firmware image file removed.	If the field is set to y , at the completion of a successful download, the procedure automatically removes the new firmware image file from the source file system, freeing up the memory on the source circuit pack. Avaya recommends using this default setting. If field is set to n , you must manually remove the new firmware image file from the source file system after the download has completed. See the Caution statement on page 15 for information. See Disable FTP/SFTP file system on page 18 for instructions.
Start Date/Time	Type the date and time that you want the firmware download to begin.	
Stop Date/Time	Type the date and time that you want the firmware download to end.	If the scheduled stop time is reached before the new firmware image file has been downloaded to every circuit pack, the system finishes downloading to the circuit pack in progress before aborting the remainder of the download schedule.
Target Location	Type the location of the circuit pack that you are updating.	For a self download, this circuit pack must reside in the same location as the source pack. For a C-LAN-distributed download, enter up to 50 locations — these must all be the same type of circuit pack.
3 of 3		

3. Press **Enter** to close the window and submit the download schedule.

If you set the **Schedule Download** field to **n**, the download starts as soon as you submit the schedule.

Note:

The target circuit packs are automatically removed from service while the firmware is downloaded to them and automatically returned to service after the download is completed. While a circuit pack is removed from service, any active calls through that circuit pack are dropped.

 CAUTION:

Unless the **Remove Image File After Successful Download** field is set to **y**, the SFTP login and password remain on the C-LAN circuit packs either until they are reset or until you enter the **disable filexfer** command. The same is true for the VAL circuit pack, except as noted below.

4. For VAL circuit packs running Communication Manager Release 1.1 (see Note below), reseat the VAL circuit pack to reset the board after the download is complete by following these steps:

Note:

In systems running on DEFINITY R9.5, or R10 software loads older than R10 field trial load 40 (R010.01.040.0), or any Communication Manager 1.1, the VAL circuit pack must be re-seated in the carrier/slot in order for the board firmware upgrade to take effect. Re-seating of the circuit pack is NOT necessary in any Communication Manager 1.2 or later systems.

 WARNING:

To prevent electrostatic discharge (ESD), be sure to wear a grounding strap while handling the circuit pack.

 CAUTION:

Ensure that both the top green and top amber LEDs on the VAL circuit pack are out.

- a. Release the latch handle to free the VAL circuit pack from the carrier.
- b. Pull the circuit pack out approximately 1 – 2 inches (3 – 5 cm).
- c. Re-insert the circuit pack into the same carrier/slot position.
- d. Close the latch securely.

Primary/secondary sync circuit pack

If you are scheduling firmware downloads for a circuit pack that is designated as primary/secondary sync (timing) source (for example, TN464GP), the previous download procedure automatically redesignates a local timing source during the download. After the download is complete and the circuit pack is returned to service, the procedure designates the original circuit pack as the timing source.

Firmware download error message

If you receive a SAT error message asking you to use the command, **test firmware download**, this means that there was a problem with a previous firmware download. Run the test before proceeding.

Verify the download schedule

If you scheduled the download for later, ensure that the download will run as you intend.

1. In a SAT session, type `test firmware download` and press **Enter**.

If the download has already begun, the test will be denied.

If the download has not already begun, the **Test Results** screen [Figure 5](#) appears.

Figure 5: Test Results screen

test firmware download						SPE A
TEST RESULTS						
Port Code	Maintenance Name	Alt. Name	Test No.	Result	Error	
	FW-DWNLD		1413	PASS		

-
2. Look in the **Result** field for **PASS** or **FAIL** conditions.
 3. If the test does not pass, refer to [Testing firmware download](#) on page 40. Resolve every error and re-run the test using the `test firmware download` command.

When the test passes, every specified resource is *currently* available for the scheduled download. Note, however, that this does *not* guarantee the resource will still be available at the time of the download.

Monitor download progress

You can check the progress of a firmware download with the following procedure.

1. In a SAT session, type `status firmware download` and press **Enter**.

The **Status Firmware Download** screen displays.

2. If this screen is blank after issuing the command, the download has completed. Go to Step 4.
3. Check the **St** (status) field immediately to the right of the **Target Location** field to view the progress of the firmware update:
 - **(P)**ending
 - **(C)**ompleted
 - **(F)**ailed
 - **(A)**borted

4. Type **status firmware download last** and press **Enter**.

The **Status Firmware Download** screen appears ([Figure 6](#)).

This screen allows you to view the progress of the last completed firmware update or the entire schedule if it is completed. Notice that the **Start** and **Stop** times now reflect the actual start and stop times of the download schedule and the **Firmware Vintage** now reflects the vintage that was downloaded.

Figure 6: Status Firmware Download screen

```
status firmware download last

                                STATUS FIRMWARE DOWNLOAD

Source Board Location: 01A04
Firmware Image File Name: usdlv22r1
Target Board Code: TN464   Suffix: GP   Firmware Vintage: 8
Schedule Download? y Remove Image File After Successful Download? y
Start Date/Time: 10/08/2002 22:00   Stop Date/Time: 10/08/2002 22:02

Target      Target      Target      Target      Target
Location St Location St Location St Location St Location
St
1. 01B04   C   11.                21.                31.                41.
2. 01B05   C   12.                22.                32.                42.
3.          13.                23.                33.                43.
4.          14.                24.                34.                44.
5.          15.                25.                35.                45.
6.          16.                26.                36.                46.
7.          17.                27.                37.                47.
8.          18.                28.                38.                48.
9.          19.                29.                39.                49.
10.         20.                30.                40.                50.
Status: Pending(P) Completed(C) Failed(F) Aborted(A)
```

5. If one or more downloads fail, type **test firmware download** to resolve the errors and clear the alarms. For more information about the test that is run and the troubleshooting procedures to use if the test does not pass, see [Test Firmware Download \(#1413\)](#) on page 54.
6. If you are upgrading firmware on a VAL circuit pack running Communication Manager Release 1.1, you must reseal the circuit pack (see Note below). Proceed to step 7.
- If you are not upgrading firmware on a VAL circuit pack running Communication Manager Release 1.1, proceed to step 8.

7. Reseat the VAL circuit pack to reset the board after the download is complete by following these steps:

Note:

In systems running on DEFINITY R9.5, or R10 software loads older than R10 field trial load 40 (R010.01.040.0), or any Communication Manager 1.1, the VAL circuit pack must be re-seated in the carrier/slot in order for the board firmware upgrade to take effect. Re-seating of the circuit pack is NOT necessary in any Communication Manager 1.2 or later systems.



WARNING:

To prevent electrostatic discharge (ESD), be sure to wear a grounding strap while handling the circuit pack.



CAUTION:

Ensure that both the top green and top amber LEDs on the VAL circuit pack are out.

- a. Release the latch handle to free the VAL circuit pack from the carrier.
 - b. Pull the circuit pack out approximately 1 – 2 inches (3 – 5 cm).
 - c. Re-insert the circuit pack into the same carrier/slot position.
 - d. Close the latch securely.
8. If you set the **Remove Image File After Successful Download?** field on the **Firmware Download** screen to **y**, then the download procedure is now complete.

If you set the field to **n**, then proceed to the next section, [Disable FTP/SFTP file system](#), to disable FTP/SFTP and manually remove the firmware image.

Disable FTP/SFTP file system

Perform the following steps on the C-LAN, VAL, and IP Media Resource circuit packs to disable FTP/SFTP and disable the login and password you created. The allocated memory for the file system remains reserved for the session.

To free up resources on the source circuit pack, you must delete the new firmware image files and disable the FTP/SFTP file system.

1. In a SAT session, type `remove file board location filename.ext` and press **Enter** to remove the image file from the source board.
2. Type `list directory board location` and press **Enter**.
The **List Directory** screen appears.
3. Verify that the new firmware image file is **not** listed in the **File/Directory Name** field.

4. At the SAT, type **disable filexfr board *location*** and press **Enter**.

The FTP/SFTP file system is disabled on the circuit pack.

Note:

This command is successful only if no files remain on the source circuit pack.

You have completed the self and C-LAN-distributed download procedures.

Download from SCP-enabled file server procedure

This section describes the procedures for installing firmware from a file server that is enabled for Secure Copy (SCP) and is on the customer's network.

Note:

This capability is available only on Communication Manager Release 3.1 or higher.

Hardware/software requirements

The procedures in this section describe how to use a central firmware depository on an SCP-enabled file server to update one or all of your non-self-downloadable circuit packs and the following versions of self-downloadable circuit packs:

- TN799DP CLAN circuit pack, firmware version 17 or higher
- TN2602AP IP Media Resource 320, firmware version 20 or higher
- TN2501AP VAL circuit pack, firmware version 10 or higher

If the previously-identified self-downloadable circuit packs do not have the minimum firmware version, you must upgrade them manually first using the procedure in [Self and C-LAN-distributed download procedure](#) on page 4.

Signed files

In order to upgrade circuit packs using firmware from a file server, the firmware images that you install must be signed according to SCP encryption guidelines. Signed firmware images have filenames with the format **tnXXXXXX_fXX_sig.bin**, where **_sig** indicates the firmware is signed. For example, **tn2602AP_f212_sig.bin** would be the name of a signed firmware images for the TN2602 circuit pack.

Signed firmware image files may also be installed using the manual process. Signed firmware image files for non-self-downloadable circuit packs may be installed on the target circuit pack regardless of the version of the previous firmware image.

Checking the firewall settings

To check the firewall settings, perform the following steps:

1. On the Maintenance Web page menu, under **Security**, select **Firewall**.

The Firewall Web page appears.

2. Verify that the **Input to Server** and **Output from Server** check boxes are selected for **snmp** and **snmptrap**.

3. Access the SAT screen on the media server whose circuit packs you are upgrading.
4. At the SAT command line, type **change permissions acpsnmp**, and press **Enter**.

The screenshot shows a terminal window titled "change permissions acpsnmp" with "Page 1 of 1" in the top right. The main content is titled "COMMAND PERMISSION CATEGORIES" and shows the "Login Name: acpsnmp". It lists three categories of commands with their respective settings:

- COMMON COMMANDS**
 - Display Admin. and Maint. Data? **y**
 - System Measurements? **y**
 - System Mgmt Data Transfer Only? **n**
- ADMINISTRATION COMMANDS**
 - Administer Stations? **n**
 - Administer Trunks? **n**
 - Administer Features? **y**
 - Administer Permissions? **n**
 - Additional Restrictions? **n**
- MAINTENANCE COMMANDS**
 - Maintain Stations? **n**
 - Maintain Trunks? **y**
 - Maintain System? **n**
 - Maintain Switch Circuit Packs? **y**
 - Maintain Process Circuit Packs? **y**
 - Maintain Enhanced DS1? **n**

At the bottom, a legend indicates: ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh.

5. Check that the following fields are set to **y**:
 - **Display Admin and Maint. Data?**
 - **System Measurements?**
 - **Administer Features?**
6. Exit the Command Permission Categories screen.
7. At the SAT command line, type **save translations** to save any changes you made to the Command Permission Categories screen.

Upload image file from Web to file server

To upgrade TN circuit packs from an SCP-enabled file server, you need to download the appropriate circuit pack firmware image files to the file server.

To upload an image file from the Web:

1. Go to the Avaya Support Web site (<http://www.avaya.com/support>). Follow the **Downloads** link and the subsequent links for your product and the target circuit pack TN code.
2. Find the section for the firmware vintage you want. Unless otherwise instructed, choose the highest vintage and be sure the filename ends with **_sig.bin**.
3. Read that vintage's ReadMe file before downloading the image file(s).
4. Click on an image file name.

5. Save this file to the file server's remote directory for SCP.
6. Write down the IP address of the SCP file server and the filename of the firmware image. You will need to enter this information later.
7. Repeat steps 4 to 6 for each image file that the ReadMe file indicates should be downloaded for that circuit pack and vintage.

Get circuit pack information

To obtain system configuration information:

1. At the SAT, enter `list configuration all`.

The **System Configuration** screen ([Figure 7](#)) appears.

Figure 7: System Configuration screen

```
list configuration all
```

SYSTEM CONFIGURATION											
Board		Code	Vintage	Assigned Ports							
Number	Board Type			u=unassigned	t=tti	p=psa					
01A08	IP MEDIA PROCESSOR	TN2302AP	HW03 FW044	01	02	03	04	05	06	07	08
01A04	CONTROL-LAN	TN799DP	HW00 FW005	u	u	u	u	u	u	u	u
				u	u	u	u	u	u	u	u
											17
01B04	DS1 Interface	TN464GP	HW02 FW006	01	02	03	04	05	06	07	08
				09	10	11	12	13	14	15	16
				17	18	19	20	21	22	26	24
				u	u	u	u	u	u	u	u
01B05	DS1 Interface	TN464GP	HW02 FW006	01	02	03	04	05	06	07	08
				09	10	11	12	13	14	15	16
				u	u	u	u	u	u	u	u
				u	u	u	u	u	u	u	u
01B06	DS1 Interface	TN464F	000038	01	02	03	04	05	u	u	u
				u	u	u	u	u	u	u	u
				u	u	u	u	u	u	u	u
				u	u	u	u	u	u	u	u
01A10	VAL-ANNOUNCEMENT	TN2501AP	HW01 FW004	01	02	03	04	05	06	07	08
				09	10	11	12	13	14	15	16
				17	18	19	20	21	22	26	24
				25	26	27	28	29	30	31	32
											33

2. Check the target circuit pack(s). If the suffix in the **Code** field does not have a "P" (for example, TN2302AP), a firmware download is not possible.

3. Verify that a firmware download is needed by checking the firmware vintage(s) in the **Vintage** field of the target circuit pack(s). Also, verify that the following self-downloadable circuit packs have a high enough vintage or version to permit the upgrade from an SCP-enabled file server:

- TN799DP CLAN circuit pack, firmware version 17 or higher
- TN2602AP IP Media Resource 320, firmware version 20 or higher
- TN2501AP VAL circuit pack, firmware version 10 or higher

If any circuit packs of these three types has a version below the requirement, you cannot upgrade that circuit pack by downloading firmware from a file server using SCP.

4. Record the location in the **Board Number** field of each target circuit pack.

Check filename of current firmware on C-LAN

You should check the firmware file name format of the file currently loaded on the C-LAN source board. To check the firmware filename, perform the following steps:

1. At the SAT, enter **list directory board UUCSS**, where **UUCSS** is the slot location of the C-LAN source circuit pack.

The List Directory screen for the specified C-LAN appears.

list directory board 1C12				Page	1
LIST DIRECTORY					
Board	File/Directory	Creation		Size	
Location	Name	Date	Time	Kb	
01C12	F:fwdlimg464gv01	2000/01/01	00:00:00	367	
D = Directory F = File					

2. Check the Name field for the file name. If there is an extension, that extension will need to appear on the file name you use in the Firmware Download screen.

Preventing dropped calls on the TN2602AP circuit pack

A TN2602AP circuit pack drops active calls when you download firmware to it. Therefore, if you are performing firmware downloads for one or more than one TN2602AP circuit pack, you need to take measures to prevent calls from dropping. Use one of the following procedures to prevent dropped calls.

For single or load-balancing TN2602AP circuit packs

By using the `campon-busyout media-processor` command, a TN2602AP circuit pack can be busied out without dropping calls, and then upgraded.

If you determined that you must upgrade the firmware on existing TN2602AP circuit packs, do so now.

1. Type `campon-busyout media-processor UUCSS`, where *UUCSS* is the location of a TN2602AP circuit pack you are converting, and press **Enter**.
2. Wait until all calls the circuit pack is carrying have ended.
3. Schedule the firmware download. See [Schedule the download](#) on page 24.
4. When the firmware has been installed, type `release board UUCSS`, and press **Enter**.
5. Repeat steps 1 through 4 for the other TN2602AP circuit pack, if it exists.

For duplicated TN2602AP circuit packs

With duplicated TN2602AP circuit packs, the standby TN2602AP circuit pack can be upgraded first, and then the circuit packs interchanged. The active circuit pack becomes the standby and can then be busied out and upgraded without dropping calls.

Use `set media-processor <location>`, where *<location>* is the slot location of the TN2602AP circuit pack, to request a demand interchange of duplicated circuit packs.

Schedule the download

You can schedule the download to occur immediately or at a later date and time.

1. In a SAT session, enter `change firmware download <schedule_number>`, where *<schedule_number>* is a number from 1 to 4.

Note:

With four firmware download schedules available for setup, you can have upgrade schedules for four different circuit pack types active at the same time.

The **Firmware Download** screen displays, [Figure 8](#)

2. Fill in the fields on this screen. Field descriptions are described in [Table 4](#).

[Figure 8: Firmware Download Screen for Download from an SCP-enabled file server](#) is an example of a download to two UDS1 boards from an SCP-enabled file server.

Figure 8: Firmware Download Screen for Download from an SCP-enabled file server

change firmware download		Page 1 of 1	
FIRMWARE DOWNLOAD			
Source Board Location: auto		File Server: 135.9.22.104	
File Retrieval Protocol: SCP		Login: acme-user Password:	
Firmware Image File Name: tn799DP_f145_sig.bin			
Target Board Code: TN799		Suffix: DP Firmware Vintage: 140	
Schedule Download? y Remove Image File After Successful Download? y			
Start Date/Time: 10/08/2005 22:00		Stop Date/Time: 10/08/2005 22:30	
Target Location	Target Location	Target Location	Target Location
1. 01B04	11. _____	21. _____	31. _____
2. 01B05	12. _____	22. _____	32. _____
3. _____	13. _____	23. _____	33. _____
4. _____	14. _____	24. _____	34. _____
5. _____	15. _____	25. _____	35. _____
6. _____	16. _____	26. _____	36. _____
7. _____	17. _____	27. _____	37. _____
8. _____	18. _____	28. _____	38. _____
9. _____	19. _____	29. _____	39. _____
10. _____	20. _____	30. _____	40. _____
			41. _____
			42. _____
			43. _____
			44. _____
			45. _____
			46. _____
			47. _____
			48. _____
			49. _____
			50. _____

See [Table 4: Firmware Download fields and descriptions](#) for the field descriptions for the Firmware Download screens.

Table 4: Firmware Download fields and descriptions

Field	Description	Notes
Source Board Location	The location of a C-LAN source circuit pack.	For a download from an SCP-enabled file server, this is a source C-LAN location. You may also enter auto, which enables Communication Manager to use any available C-LAN circuit pack. For a self downloadable circuit pack type, you can enter self, and then add target locations for multiple self-downloadable circuit packs of the same type. This allows simultaneous firmware downloads to multiple circuit packs.
1 of 3		

Table 4: Firmware Download fields and descriptions (continued)

Field	Description	Notes
File Server	The IP address or node name of the SCP-enabled file server	If a node name is used, this name must already be identified in the Node Names screen.
File Retrieval Protocol	This is a display-only field that should read SCP .	SCP stands for Secure Copy.
Login	The login name for the SCP-enabled server.	
Password	The password for the SCP-enabled server.	
Firmware Image File Name	The complete filename of the new firmware image file. If the list directory board command showed that the file had an extension, such as .bin, include the extension.	The firmware image that you install must be signed according to SCP encryption guidelines. Signed firmware images have filenames with the format tnXXXXXX_fXX_sig.bin , where _sig indicates the firmware is signed. For example, tn2602AP_f212_sig.bin would be the name of a signed firmware images for the TN2602 circuit pack.
Target Board Code	The circuit pack ID. For example, TN2501 Do not type the suffix, such as AP, D", or GP in this field (type the suffix in the Suffix field).	Enter the TN code of the target circuit pack(s).
Suffix	Type the suffix. Examples: • For VAL (TN2501AP), AP. • For C-LAN (TN799DP), DP. • For DS1 (TN464GP), GP.	
Firmware Vintage	This field is blank.	You can view the firmware vintage on the Firmware Download screen. Use the command display firmware download or status firmware download to display the Firmware Download screen.
2 of 3		

Table 4: Firmware Download fields and descriptions (continued)

Field	Description	Notes
Schedule Download	Type y to schedule the firmware download for another time. Type n to start the firmware download immediately after completing the screen.	Once the firmware download begins, you cannot make any changes to this screen. You can only disable this schedule using the disable firmware download command and then starting a new one. (See Aborting a firmware download on page 40 for instructions.) If you type n , then the Start Date/Time and Stop Date/Time fields disappear. The download begins as soon as you press Enter .
Remove Image File After Successful Download	Type y if you want the procedure to automatically remove the new firmware image file [default]. Type n if you do not want the new firmware image file removed.	If the field is set to y , at the completion of a successful download, the procedure automatically removes the new firmware image file from the source file system, freeing up the memory on the source circuit pack. Avaya recommends using this default setting. If field is set to n , you must manually remove the new firmware image file from the source file system after the download has completed. See the Caution statement on page 15 for information. See Disable FTP/SFTP file system on page 18 for instructions.
Start Date/Time	Type the date and time that you want the firmware download to begin.	
Stop Date/Time	Type the date and time that you want the firmware download to end.	If the scheduled stop time is reached before the new firmware image file has been downloaded to every circuit pack, the system finishes downloading to the circuit pack in progress before aborting the remainder of the download schedule.
Target Location	Type the location of the circuit pack or circuit packs that you are updating.	Enter up to 50 locations — these must all be the same type of circuit pack.
3 of 3		

3. Press **Enter** to close the window and submit the download schedule.

If you set the **Schedule Download** field to **n**, the download starts as soon as you submit the schedule.

Note:

The target circuit packs are automatically removed from service while the firmware is downloaded to them and automatically returned to service after the download is completed. While a circuit pack is removed from service, any active calls through that circuit pack are dropped.

Primary/secondary sync circuit pack

If you are scheduling firmware downloads for a circuit pack that is designated as primary/secondary sync (timing) source (for example, TN464GP), the previous download procedure automatically redesignates a local timing source during the download. After the download is complete and the circuit pack is returned to service, the procedure designates the original circuit pack as the timing source.

Firmware download error message

If you receive a SAT error message asking you to use the command, **test firmware download**, this means that there was a problem with a previous firmware download. Run the test before proceeding.

Verify the download schedule

See [Verify the download schedule](#) on page 16.

Monitor download progress

See [Monitor download progress](#) on page 16.

IPSI and SIPI download procedure

This procedure allows you to update one or all of your TN2312AP/BP (IPSI) or TN8412AP (SIPI) target circuit packs using a new firmware image file that is loaded from the Web onto the media server.

Note:

You can download firmware for a TN2312BP to a TN2312AP IPSI circuit pack., though environmental maintenance is not available on the TN2312AP.

You can download firmware to one or more TN2312BP IPSI circuit packs from either the active or the standby S8700-series Media Server because the process only requires IP connectivity to the IPSIs, which both media servers have.

After the firmware download completes and the IPSI or SIPI resets, the IPSI/SIPI automatically activates the new firmware, regardless of how the IPSI/SIPI reset was initiated (as a scheduled event, by demand, or spontaneously by system software). You can schedule the firmware activation using the Activate IPSI Upgrade screen, although the new firmware might activate earlier if the IPSI/SIPI is reset for other reasons.

**CAUTION:**

Make sure that you want to upgrade the IPSI or SIPI firmware before you initiate the download. Once you have successfully downloaded the new firmware into an IPSI or SIPI, you cannot cancel the upgrade. However, after an upgrade, you can revert back to an older vintage ([Reverting to an older TN2312AP \(IPSI\) or TN8412 \(SIPI\) vintage](#)) by downloading the older vintage onto the circuit pack.

To update firmware on an IPSI or SIPI, follow these procedures

1. [Verify hardware and software prerequisites](#) on page 29
2. [Determine current IPSI or SIPI firmware](#) on page 30
3. [Pre-upgrade tasks](#) on page 30
4. [Upgrade tasks](#) on page 33
5. [Interchange the IPSIs \(S8700-series duplicated control network only\)](#) on page 38
6. [Post-upgrade task](#) on page 38

Verify hardware and software prerequisites

Before starting the upgrade procedure, you need several items.

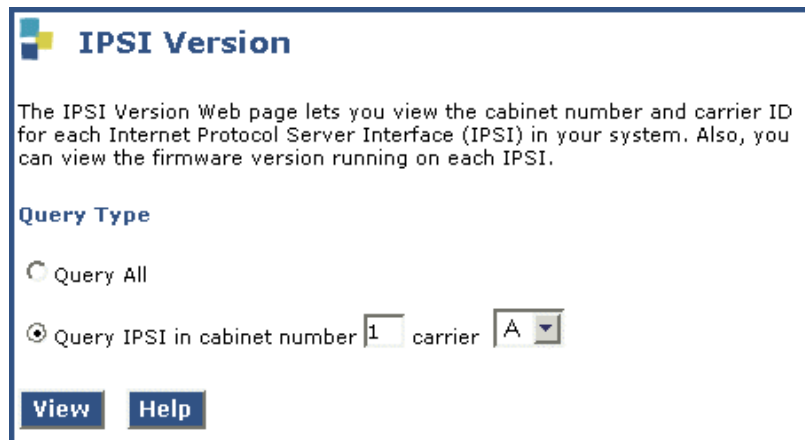
Make sure you have the following:

✓	Item
	Superuser or Services login and password to DEFINITY or Communication Manager
	A computer with the following:
	● IP connectivity to the media server
	● IP connectivity to the World-Wide Web
	● MS Internet Explorer 5.5 or later
	The latest IPSI or SIPI firmware, which is available at the Avaya Support Web site (http://www.avaya.com/support). Click Downloads and select your product (S8400, S8500, S8700, S8710, or S8720). To find out the firmware that is currently on the SIPI or IPSIs, see Determine current IPSI or SIPI firmware on page 30

Determine current IPSI or SIPI firmware

The following steps determine the firmware version on the SIPI or each IPSI.

1. Under IPSI Firmware Upgrades click **IPSI Version** and select **Query All** to see the firmware version of the SIPI circuit pack or every IPSI circuit pack.



IPSI Version

The IPSI Version Web page lets you view the cabinet number and carrier ID for each Internet Protocol Server Interface (IPSI) in your system. Also, you can view the firmware version running on each IPSI.

Query Type

☐ Query All

☒ Query IPSI in cabinet number carrier

View **Help**

The output looks something like this:

IP address	IPSI Name	IPSI Board	HW#	FW#
135.9.77.28	ipsi-A01e	TN2312	32	7

The last column shows the firmware version.

2. Print the page.
3. Determine which IPSIs, or if the SIPI, needs new firmware.

Pre-upgrade tasks

- [Access the Maintenance Web Interface](#) on page 31
- [Copy firmware files to media server](#) on page 32
- [Determine active IPSIs \(S8700-series duplicated control network only\)](#) on page 33
- [Busy out standby IPSIs \(S8700-series duplicated control network only\)](#) on page 33

Access the Maintenance Web Interface

The following steps allow you to access the Maintenance Web Interface.

Note:

If duplicated media servers, you must connect to the *active* media server.

1. If on site, connect to the services port (default 2 [Eth1]) on the back of the media server.

If off site, log into the media server using the IP address of the media server.

2. Launch the Web browser.
3. If connected directly to the media server, type **192.11.13.6** in the Address field to bring up the logon Web page.

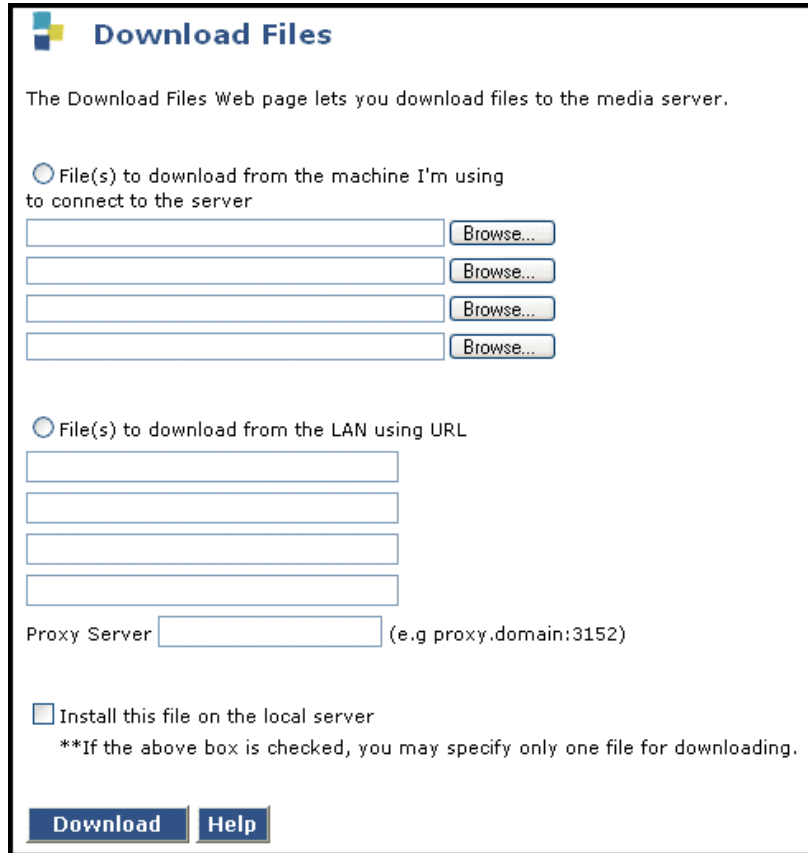
If connected through the network, type in the host name or IP address of the media server.

4. Log in as **craft** or **dadmin**.
5. When asked whether to suppress alarms, click **yes**.
6. Click **Launch Maintenance Web Interface** to get to the Main Menu.

Copy firmware files to media server

To copy files to the media server, complete the following steps:

1. On the Maintenance Web Interface, under Miscellaneous, click **Download Files**.



The screenshot shows a web page titled "Download Files" with a blue header bar. Below the header, a text box explains: "The Download Files Web page lets you download files to the media server." There are two radio button options. The first option, "File(s) to download from the machine I'm using to connect to the server", is selected. It has four text input fields, each with a "Browse..." button to its right. The second option, "File(s) to download from the LAN using URL", is unselected and has four text input fields. Below these is a "Proxy Server" label followed by a text input field and the text "(e.g proxy.domain:3152)". At the bottom, there is a checkbox labeled "Install this file on the local server" with a note below it: "**If the above box is checked, you may specify only one file for downloading." At the very bottom are two buttons: "Download" and "Help".

2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the **Choose File** window on your computer. Find the files that you need to copy to the media server.
4. Click **Download** to copy the file(s) to the media server.

The files are automatically copied to the default file location.

Determine active IPSIs (S8700-series duplicated control network only)

Note:

With a duplicated control network it is acceptable to download new firmware to an active IPSI. However, whenever possible, activate the new firmware to a standby IPSI.

The following step displays all the IPSIs.

1. In a SAT session, type `list ipserver-interface` and press **Enter** to determine which IPSIs in port networks are active.
2. Print the page, which shows the board locations (**Bd Loc**) and which IPSIs are active or standby (**Control State**) or write down the information.

Busy out standby IPSIs (S8700-series duplicated control network only)

You can busy out the standby IPSIs using the following procedure.

1. In a SAT session, type `busyout ipserver-interface standbyIPSI`, where *standbyIPSI* is an IPSI in standby mode, and press **Enter** to busy it out.
2. Repeat for each IPSI circuit pack in standby mode.

Upgrade tasks

- [Download firmware to IPSI or SIPI](#) on page 33
- [Activate the new firmware](#) on page 36
- [Release standby IPSIs \(S8700-series with duplicated control network only\)](#) on page 37
- [Verify the health of the IPSIs or SIPI](#) on page 37

Download firmware to IPSI or SIPI



CAUTION:

These steps will *not* disrupt call service unless a reset (for example, power failure) of the SIPI or active IPSI occurs. A reset activates the new firmware image and may disrupt call service. To avoid that possibility, perform these steps during a low traffic period or, if duplicated IPSIs, perform these steps on the standby IPSIs only, interchange the IPSIs, then perform them on the remainder of the IPSIs.

Firmware Download Procedures

The following steps download the firmware to the SIPI or to each or all IPSIs in the Maintenance Web Interface:

1. Under IPSI Firmware Upgrades, click **Download IPSI Firmware**.

The Download IPSI Firmware Web page appears.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The left sidebar contains a navigation menu with categories: Alarms, Diagnostics, Server, Server Configuration, Server Upgrades, and IPSI Firmware Upgrades. The main content area is titled "Download IPSI Firmware" and includes the following sections:

- Start Time for Download:** Two radio buttons: "Start Download Now" and "Start Download at" followed by input fields for mm/dd and hh:mm.
- IPSI Target(s):** Three radio buttons: "All IPSIs with board code" (with a dropdown menu showing "TN8412AP"), "IPSI cabinet number" (with input fields for "01" and "A"), and "All standby IPSIs (applies to duplicated control networks only)".
- Select File to Download:** Three radio buttons: "No valid ipsi firmware image found in the /var/home/ftp/pub directory.", "Use This File" (with an input field), and "Use File on Remote server." (with input fields for "Server IP", "Login", "Protocol" (set to "SCP"), and "Password").
- A checkbox: "Continue with download even if version is older than the version currently installed."
- Buttons: "Download Firmware" and "Help".

The top of the page shows the Avaya logo, the title "Integrated Management Maintenance Web Pages", and the server information "This Server: [1] aiws8400".

2. Select the time when you want the firmware download to begin. You can do it immediately or schedule a time.

3. For a SIPI, select **All IPSIs** with board code TN8412AP.

For IPSIs, select either an individual IPSI by providing its cabinet number and carrier location or select **All IPSIs**.

**CAUTION:**

Select **All IPSIs** only if the media server is shut down during an upgrade or on a new installation. *Never* select **All IPSIs** if IPSIs are duplicated.

4. Select the firmware file to download using one of the following options:
 - Select the appropriate file name if the file is already listed as available in the /var/home/ftp/pub directory
 - In the **Use This File** field, type the full path to the file if the file is on your laptop
 - Type in the Remote Server information:
 - In the **Use This File** field, type the file name if the file is in the SCP server's home directory. If the file is not in the home directory, type the full directory path including the file name.
 - In the **Server IP** field, type the IP address of the SCP file server.
 - In the **Login** field, type the login name to log into the SCP file server.
 - In the **Password** field, type the password to log into the SCP file server.
5. Click **Download Firmware** to download the firmware to the SIPI, all IPSIs, or an individual IPSI.
6. If you have more than one IPSI to upgrade, repeat for each IPSI.

**Important:**

The firmware download is first stored in RAM on the IPSI. After the entire download file has been successfully sent to the IPSI, the IPSI burns the firmware image into ROM. The firmware download is not permanent until the image has been completely burned into ROM. If for any reason the download process is interrupted (for example, a break in the network connection, a failure of the IPSI, power loss to the IPSI, and so forth), you must initiate the download again.

7. Click **Download Status** to view
 - Scheduled firmware downloads
 - History and status of previous downloads.
8. If necessary, cancel scheduled downloads from this screen. If you cancel, you cancel all the scheduled downloads, not just an individual one, unless you are only downloading to one IPSI.

Note:

If you have trouble with these procedures, you can use an alternate [Linux procedure for downloading IPSI firmware](#) on page 41 that uses Linux commands.

Activate the new firmware

**CAUTION:**

This causes a brief service interruption in a single control network configuration (the IPSIs are not duplicated). Schedule the activation for off hours.

**CAUTION:**

If an S8700-series duplicated control network, schedule the activation for the IPSIs in a busied-out, standby mode only.

Once the firmware is downloaded to the SIPI or IPSI, you must activate it. The new firmware could activate earlier if the SIPI or IPSIs are reset for other reasons. When you manually reset IPSIs, the command resets the IPSIs one at a time. When a particular IPSI's turn arrives, it is reset even if it is busy handling calls.

1. Under **IPSI Firmware Upgrades**, click **Activate IPSI Upgrade**.
2. Select either **All IPSIs** (if non-duplicated control network) or an individual IPSI by providing its cabinet number and carrier location. For the SIPI, select **All IPSIs**.
3. Select the time when you want to start activating the firmware. You can do it immediately or schedule a time.
4. Select the time when you want to stop the activation. If the activations have not completed by the stop time, they will stop, and you must activate them at another time.
5. Click **Activate IPSI Upgrade** to start the activation or the clock for the activation schedule.
6. Click **Activation Status** to view:
 - Scheduled firmware resets
 - History and status of the resets
7. If necessary, cancel the resets from this screen.

Cancellation affects only the IPSIs that have not yet been reset. The information displayed on this screen applies only to resets initiated from this screen. It does not display the status for resets initiated through Avaya Communication Manager or from other events such as board removal, power loss, and so forth. Canceling the resets means some IPSIs will have newer firmware than others.

Note:

If you have trouble with these procedures, you can follow an alternate [Linux procedure for activating new IPSI or SIPI firmware](#) on page 43 that uses Linux commands.

Release standby IPSIs (S8700-series with duplicated control network only)

Note:

The following steps are done using SAT commands.

The following steps release the IPSIs from busyout mode.

1. Type **release ipserver-interface *busyIPSI***, where *busyIPSI* is a busied-out IPSI and press **Enter** to release it.
2. Repeat for each busied-out IPSI circuit pack.

Verify the health of the IPSIs or SIPI

Note:

The following steps are done using SAT commands.

The following steps verify the health of the SIPI or standby IPSIs.

1. Type **list ipserver-interface** and press **Enter**.

The system displays the **IP Server Interface Information** screen ([Figure 9](#)).

Figure 9: IP Server Interface Information screen

list ipserver-interface								Page 1
IP SERVER INTERFACE INFORMATION								
Port Ntwk Num	Pri/ Sec Bd Loc	Primary/ Secondary IP Address	Primary/ Secondary Host Name	Primary/ Secondary DHCP ID	Serv State	Control State	State of Health C P E G	
1	1A01	172.22.22.174	172.22.22.174	ipsi-A01a	IN	actv-aa	0.0.0.0	
	1B01	172.22.22.175	172.22.22.175	ipsi-A01b	IN	standby	0.0.0.0	
26	26A01	172.22.22.244	172.22.22.244	ipsi-A26a	IN	actv-aa	0.0.0.0	
	26B01	172.22.22.243	172.22.22.243	ipsi-A26b	IN	standby	0.0.0.0	

2. Make sure that each standby IPSI has a **State of Health** of **0.0.0.0**.

C = Clock functionality

P = Packet interface

E = EAL

G = Tone detectors/Generators

3. If any parameter has a number other than **0**, view the active alarms.

Type **display alarms** and press **Enter** to resolve the alarms before proceeding.



CAUTION:

If an IPSI has health problems, you should **not** interchange to that IPSI. Interchanging to an unhealthy IPSI could bring down all the calls on that port network.

Interchange the IPSIs (S8700-series duplicated control network only)

The following steps interchange the IPSIs.

1. Type **set ipserver-interface *location***, where *location* is the location of the standby IPSI to set the standby IPSI as the new active IPSI. This forces an interchange from the active to the standby IPSI.
2. Type **list ipserver-interface** again to make sure the new active IPSI is still healthy. The **State of Health** field should still be **0.0.0.0**.

All the IPSIs should now be interchanged so that the newly active IPSIs are running the new version of firmware and the newly standby IPSIs are still running the old version.

3. Repeat the steps in [Busy out standby IPSIs \(S8700-series duplicated control network only\)](#) on page 33 through [Verify the health of the IPSIs or SIPI](#) on page 37 for each new standby IPSI.

Post-upgrade task

Verify IPSI or SIPI firmware version

The following steps in the Maintenance Web Interface list the SIPI or all the IPSIs and their firmware version.

1. Under IPSI Firmware Upgrades click **IPSI Version**.
2. Select **Query All** to verify that the IPSI circuit packs have the required firmware version.

Using Software Update Manager for centralized firmware download

You can use the Software Update Manager (SUM) to download firmware to one or all of your non-self-downloadable circuit packs and the following versions of self-downloadable circuit packs:

- TN799DP CLAN circuit pack, firmware version 17 or higher
- TN2602AP IP Media Resource 320, firmware version 20 or higher
- TN2501AP VAL circuit pack, firmware version 10 or higher
- TN2312BP IPSI circuit pack, any firmware version
- TN8412 SIPI circuit pack, any firmware version

If the previously-identified self-downloadable circuit packs do not have the minimum firmware version, you must download firmware to them manually first using the procedure in [Firmware download process](#) on page 1.

This capability is available only with Communication Manager Release 3.1 and Integrated Management (IM) Release 3.1 Network Management.

For more information, see *Job Aid: Firmware Download Procedures, Communication Manager Integrated Management Release 3.1, How to centrally manage and upgrade your TN boards*, 14-600853, Issue 1, February 2006.

Troubleshooting firmware downloads

This section contains these troubleshooting subsections:

- [Aborting a firmware download](#) on page 40
- [Testing firmware download](#) on page 40
- [Linux procedure for downloading IPSI firmware](#) on page 41
- [Linux procedure for activating new IPSI or SIPI firmware](#) on page 43
- [Backing out of firmware download](#) on page 44

Aborting a firmware download

You can only abort (disable/cancel) a scheduled download that has not yet started. Any download currently in progress will finish. For example, say you scheduled a C-LAN distributed download to multiple targets. Then, you disabled the download while it was in progress to the first circuit pack. The download will stop after the completion of the first circuit pack's download. The remainder of the circuit packs do not receive the download.

To abort a self or C-LAN-distributed firmware download

1. Open a SAT session.
2. Enter the command `disable firmware download`.

To abort an IPSI or SIPI firmware download:

1. Access the Maintenance Web Interface.
2. Under **IPSI Firmware Upgrades**, select **View Download Status**.
3. Click **Cancel Downloads**.

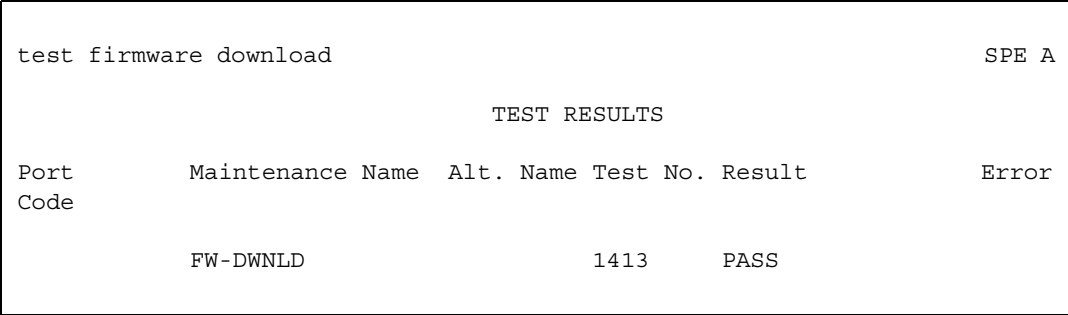
Testing firmware download

You can test a self or C-LAN-distributed firmware download either before a scheduled download has begun or after an attempted download has reported errors:

1. At the SAT, enter `test firmware download`.

The **Test Results** screen ([Figure 10](#)) appears.

Figure 10: Test Results screen



The screenshot shows a terminal window with the command 'test firmware download' and the output 'SPE A'. Below this is a table titled 'TEST RESULTS' with columns: Port Code, Maintenance Name, Alt. Name, Test No., Result, and Error. The table contains one row with the following data: Port Code is empty, Maintenance Name is 'FW-DWNLD', Alt. Name is empty, Test No. is '1413', Result is 'PASS', and Error is empty.

test firmware download						SPE A
TEST RESULTS						
Port Code	Maintenance Name	Alt. Name	Test No.	Result	Error	
	FW-DWNLD		1413	PASS		

The example in [Figure 10](#) shows **PASS** in the **Result** field, indicating a successful test of the firmware download circuitry.

2. If the test does not pass (**FAIL** appears in the **Result** field), refer to [Test Firmware Download \(#1413\)](#) on page 54.

Linux procedure for downloading IPSI firmware

The recommended method for downloading firmware from a media server to IPSIs or a SIPI is through the media server Web interface procedure described in [Download firmware to IPSI or SIPI](#) on page 33. If you have trouble using that procedure, you can follow this alternate procedure that uses Linux commands instead:

1. In a SAT session, type `go shell` and press **Enter** to access the Linux command line.
2. Log into the media server's Linux shell with a services- or superuser-level login ID and password.
3. Change directory to the default location using `cd /var/home/sftp`.
4. Enter the `loadipsi` command to invoke SFTP either to copy a firmware image or to schedule a copy operation.
 - To copy the firmware image from its default location on the server to either:
 - one IPSI circuit pack enter:


```
loadipsi -f ./filename -c location
```
 - or
 - every IPSI (one at a time, in the order recorded in the server's `/etc/hosts` file) enter:


```
loadipsi -f ./filename -a
```
 - To schedule an IPSI copy operation using the `-s` option, enter:


```
loadipsi -f ./filename -a -s mmddyyyyhh:mm
```

Note:

Enter `loadipsi -?` for more information about this command's syntax and options.

5. You will see:

Burning flash may take several minutes...

When the download is complete, you will see:

Burning flash may take several minutes.....done

All done: Success

If the download failed, you may see one of the errors listed in [Table 5: IPSI/SIPI firmware download error messages](#) on page 42:

Table 5: IPSI/SIPI firmware download error messages

Error Message from loadipsi Command	Description/Recommendation
IPSI/SIPI Related Error: Higher/same version for IPSI board. Download Stop.	Occurs after trying to download a file with a lower firmware version than the file currently on the IPSI or SIPI board. Only a higher or the same version is allowed unless the <code>-r</code> option is used with the <code>loadipsi</code> command. 1. If you intended to download an older vintage, then use the <code>-r</code> option with the <code>loadipsi</code> command as described in Reverting to an older TN2312AP (IPSI) or TN8412 (SIPI) vintage on page 44. 2. If you did not intend to download an older vintage, then perform the steps again using the vintage you intended.
IPSI/SIPI Related Error: copy2flash: FAIL	The file could be corrupted perhaps due to forgetting to use SFTP's binary mode. If you used Upload Files to Server on the Web interface, then the <code>binary</code> command is automatically used. 1. Upload the files from the server to the IPSI or SIPI again. If you think that the image files on the server may also be corrupted, then redo all the steps starting with copying firmware from the Web to the staging area. 2. If you are <i>not</i> using Upload Files to Server on the Web interface, but are manually SFTP'ing the files to the server, then be sure to use the <code>binary</code> command before the <code>get</code> command.
System Error: Connect to check IPSI board version: Error firmware version xx, board version: yy	Occurs when the IPSI or SIPI is resetting. 1. Wait until the IPSI or SIPI comes back up. 2. Re-enter the <code>loadipsi</code> command
1 of 2	

Table 5: IPSI/SIPI firmware download error messages (continued)

Error Message from loadipsi Command	Description/Recommendation
System Error: Image file: No such file or directory. System Error: Image file error.	Occurs when the specified file is not in the specified directory. 1. Make sure the current directory is /var/home/sftp or type cd /var/home/sftp to change to that directory. 2. Make sure the image file is in /var/home/ftp. Type ls -ltr on Linux or dir /od on DOS to list the files in the current directory with the most recent file last. 3. Re-enter the loadipsi command.
2 of 2	

Linux procedure for activating new IPSI or SIPI firmware

The recommended method for activating new firmware on the SIPI or IPSIs is through the media server Web interface procedure described in [Activate the new firmware](#) on page 36. If you have trouble using that procedure, you can follow this alternate procedure that uses Linux commands instead:

For an S8400, S8500 or an S8700-series duplex-reliability configuration, perform the following steps for the SIPI or all IPSIs during a low traffic period. For S870-series high- and critical-reliability configurations, perform the following on each of the standby IPSIs only.

1. In a SAT session, enter **go shell** to access the Linux command line.
2. Log into the media server's Linux shell with a services- or superuser-level login ID and password.
3. Enter a Linux **resetipsi** command to either:
 - reset **one** standby IPSI at a time, using **resetipsi -c location**,
 - reset the SIPI or **every** IPSI, using **resetipsi -a**,
 - or
 - schedule a reset of the SIPI or all IPSIs using the **-s** option:


```
resetipsi -a -s mmddyyyyhh:mm
```



CAUTION:

On duplex-reliability systems, stable calls will be moved to an EI EAL fallback configuration, but unstable calls will be dropped.

Note:

Enter `resetipsi -?` for more information about this command's syntax and options.

4. Check that the IPSI or SIPI has the new firmware version with the following command:

```
ipsiversion -c location
```

5. Check the health of the IPSI or SIPI by entering the following command:

```
list ipserver-interface
```

The **State of Health** field should be **0.0.0.0**. Resolve any health problems.

This completes the IPSI download procedure for duplex-reliability configurations. For a high- or critical-reliability configuration, you still need to upgrade the active IPSIs. Follow the steps outlined in [Interchange the IPSIs \(S8700-series duplicated control network only\)](#) on page 38.

Backing out of firmware download

To back out of a completed firmware download and revert to the previous image, for all circuit packs except IPSI, SIPI, C-LAN, and VAL, you follow the same download procedure you did before, except use the previous firmware vintage instead.

For backing out of an IPSI or SIPI download, see [Reverting to an older TN2312AP \(IPSI\) or TN8412 \(SIPI\) vintage](#) on page 44. For backing out of a C-LAN or VAL download, see [Reverting to an older TN799DP \(C-LAN\) or TN2501AP \(VAL\) vintage](#) on page 45.

Reverting to an older TN2312AP (IPSI) or TN8412 (SIPI) vintage

As the server copies firmware to an IPSI or SIPI during a firmware download, the previous firmware is overwritten. Therefore, the old firmware must be downloaded in order to restore the previous firmware image file.

At a high level, copying, downloading and activating a previous image of firmware has the same steps as an [IPSI and SIPI download procedure](#). However, the additional steps include the following procedure:

1. When downloading a previous firmware image from the Web to a directory on the active media server, follow the steps described in [Copy firmware files to media server](#) on page 32. Be sure to select the firmware image that was on the IPSI or SIPI before the upgrade.
2. When copying the previous image from the server to the IPSI(s) or SIPI, follow the steps described in [Download firmware to IPSI or SIPI](#) on page 33.
3. If using the media server's Maintenance Web Interface, select the **Download IPSI Firmware** page. On the **Download IPSI Firmware** page, select the following:

Continue with download even if version is older than the version currently installed

4. If using the alternate Linux command line method, be sure to use the `-r` option with the `loadipsi` command to download without comparing the new version with the existing version.

For instance, to copy the previous image to every IPSI or to the SIPI, you would enter

```
loadipsi -f /var/home/sftp/filename -a -r
```

Activate the IPSI or SIPI as described in [Activate the new firmware](#) on page 36.

Reverting to an older TN799DP (C-LAN) or TN2501AP (VAL) vintage

To revert back to the old firmware image file on a C-LAN or VAL circuit pack:

1. In a SAT session, enter `get boot-image location` to check the status of the firmware images on the target circuit pack.

The **Display Firmware Image(s)** screen ([Figure 11](#)) appears.

Figure 11: Display Firmware Image(s) screen

get boot-image 1C07	
DISPLAY FIRMWARE IMAGE(S)	
Image 1	Image 2
Board Type: TN2501	TN2501
FW Vintage: 02	01
HW Signature: 02	02
Suffix: A	A
Date: 09/13/02	05/06/02
Timestamp: 10:30:50	12:42:18
CRC Checksum: Good	Good
Active Image: Yes	No
Reboot Image: Yes	No

2. Check **Image 1** and **Image 2** fields to see where the active image resides.
3. Check the **Date** and **Timestamps** fields to determine whether to revert back to **Image 1** or **Image 2**.

In the following example, we are reverting back to **Image 2**, because it has the older date and time stamp.

Note:

In most cases, the image with the more recent date and time stamp is the new firmware image file.

4. Type `set boot-image board location image 1 | 2` and press **Enter**.

Example: `set boot-image board 1C07 image 2`

The system responds with:

Command Successfully Completed

5. Type `get boot-image location` and press **Enter** to check the status of the firmware images on the target circuit pack.

The **Display Firmware Image(s)** screen [Figure 12](#) appears.

Figure 12: Display Firmware Image(s) screen

get boot-image 1C07		
DISPLAY FIRMWARE IMAGE(S)		
	Image 1	Image 2
Board Type:	TN2501	TN2501
FW Vintage:	02	01
HW Signature:	02	02
Suffix:	A	A
Date:	09/13/02	05/06/02
Timestamp:	10:30:50	12:42:18
CRC Checksum:	Good	Good
Active Image:	Yes	No
Reboot Image:	No	Yes

Note that the value in the **Reboot Image** field has changed.

6. Reseat the circuit pack to activate the new firmware image:



WARNING:

To prevent electrostatic discharge (ESD), be sure to wear a grounding strap while handling the circuit pack.



CAUTION:

For a VAL circuit pack, ensure that both the top green and top amber LEDs are out.

- Release the latch handle to free the circuit pack from the carrier.
 - Pull the circuit pack out approximately 1 – 2 inches (~ 3 – 5 cm).
 - Re-insert the circuit pack into the carrier.
 - Close the latch securely.
7. Wait until all three of the top LEDs (red, green, and amber) are out.

8. In the SAT session, type `get boot-image location` and press **Enter** to check the status of the firmware images on the target circuit pack.

The **Display Firmware Image(s)** screen [Figure 13](#) appears.

Figure 13: Display Firmware Image(s) screen

get boot-image 1C07		
DISPLAY FIRMWARE IMAGE(S)		
	Image 1	Image 2
Board Type:	TN2501	TN2501
FW Vintage:	02	01
HW Signature:	02	02
Suffix:	A	A
Date:	09/13/02	05/06/02
Timestamp:	10:30:50	12:42:18
CRC Checksum:	Good	Good
Active Image:	No	Yes
Reboot Image:	No	Yes

9. Verify that the **FW Vintage** field displays the correct vintage.
10. Ensure that both the **Active Image** and the **Reboot Image** fields are as you expect.

Error Log Entries and Test to Clear Values

[Table 6: FW-DWNLD Maintenance Error Log Entries](#) on page 48 shows the error log entries and tests apply to self- and C-LAN distributed downloads, *not to IPSI or SIPI downloads*.

Table 6: FW-DWNLD Maintenance Error Log Entries

Error Type	Aux Data	Cause of Error	Alarm Level	On/Off Board	Test to Clear Value
257 (a)	See associated note	Download failure	MIN	OFF	<code>test firmware download location</code>
258 (b)	See associated note	Download failure	MIN	OFF	<code>test firmware download location</code>
259 (c)	See associated note	Download failure	MIN	OFF	<code>test firmware download location</code>
513 (a)	See associated note	Download failure	MIN	OFF	<code>test firmware download location</code>
769 (2)	See associated note	Firmware download request	MIN	OFF	<code>test firmware download location</code>

Notes:

- a. **Error Type 257** — A log-only error indicating that a certain software resource was not available. Such an error very seldom occurs and usually produces a `proc_err`. However, in the firmware download feature, the file cannot be downloaded and/or the schedule can also abort/fail. To resolve the error, use the `test firmware download` command. The Aux Data specifies the unavailable resource that caused the error. See [Table 7](#) for more details.

Table 7: Aux Data for Error Type 257

Aux Data	Description of Failure
1	Source board query failed. 1. Check for system-wide problems. 2. Clear every error, and retry the download.
1 of 2	

Table 7: Aux Data for Error Type 257 (continued)

Aux Data	Description of Failure
2	Target board query failed. 1. Check for system-wide problems. 2. Clear every error, and retry the download.
3	Allocating resources failed. 1. Check for system-wide problems. 2. Clear every error, and retry the download.
4	Firmware Download Information table query failed. 1. Check for system-wide problems. 2. Clear every error, and retry the download.
5	Header message failed. 1. Check for system-wide problems. 2. Clear every error, and retry the download.
6	Download Map timer expired. 1. Check for system-wide problems. 2. Clear every error, and retry the download.
2 of 2	

- b. **Error Type 258** — A log-only error indicating that a source board-related error occurred. The download schedule can also abort/fail. To resolve the error, use the command `test firmware download`. The Aux Data specifies the error. See [Table 8](#) for more details.

Table 8: Aux Data for Error Type 258

Aux Data	Description of Failure
1	Download image file specified on the <code>change firmware download</code> screen not present on the source board. 1. Use the <code>list directory board location</code> command to verify file system's contents.
2	The image on the source board has an invalid header. 1. Retry the test. 2. If error recurs, then escalate.
3	Bad CRC on image file on source board. 1. Retry the test. 2. If error recurs, then escalate.
1 of 2	

Table 8: Aux Data for Error Type 258 (continued)

Aux Data	Description of Failure
4	File name too long. 1. Rename the file, and try again.
5	Invalid TN code on the change firmware download screen does not match TN code of image on the source board. 1. Verify screen, and make sure the correct image is being used.
6	Invalid suffix on the change firmware download screen does not match suffix of image on the source board. 1. Verify screen, and make sure the correct image is being used.
7	Source board is not present. 1. Compare board's entered location on the change firmware download screen with its actual location.
8	Incorrect source board 1. Verify that the source board has a valid TN code and suffix (for example, AP).
9	PPP ports not available 1. Use another source board, or reschedule the download for off hours.
10	DL Setup message to source failed. 1. Retry the download. 2. If error recurs, then escalate.
2 of 2	

- c. **Error Type 259** — A log-only error indicating that the target board failed to download. To resolve the error, use the command **test firmware download**. The Aux Data specifies the error. See [Table 9](#) for more details.

Table 9: Aux Data for Error Type 259

Aux Data	Description of Failure
1	Target board is not present / responding. 1. Check board's location and translations, and retry download.
2	Incorrect target board for download schedule. 1. Verify board's location and download schedule.
3	Target failed to go into DL Mode. 1. Retry the download.
1 of 3	

Table 9: Aux Data for Error Type 259 (continued)

Aux Data	Description of Failure
4	Target received bad file header. 1. Get a new image, and retry download.
5	Bad checksum on source board's image. 1. Get a new image, and retry download.
6	TFTP protocol error – One reason for this type of failure may be that the target board is located in a DS1-C remote PN using ami-zcs line coding to communicate with the Media Server. To have a successful firmware download you must have a clear channel between the source and target board, or the source and target must reside in the remote PN. Some examples of the correct type of line coding for this feature are: b8zs and hdb3.
7	File transfer timer expired. 1. Check the board's location and translations, and retry download.
8	Target failed to reset after transfer. 1. Check the board's location and translations, and retry download.
10	Download of target failed. 1. Check the board's location and translations, and retry download.
13	The target board rejected the download image. 1. Check the board's translations. 2. Verify the image file. 3. Retry the download, and escalate if it still fails.
20	Could not open the requested file – Internal firmware error on target board. 1. Retry the download, and escalate if it still fails.
21	Problem reading the requested file – Internal firmware error on target board. 1. Retry the download, and escalate if it still fails.
22	The download file has a bad CRC – Internal firmware error on target board. 1. Retry the download, and escalate if it still fails.
24	A download is already in progress – Internal firmware error on target board. 1. Retry the download, and escalate if it still fails.
30	A start download sequence error – Internal firmware error on target board. 4. Retry the download, and escalate if it still fails.
2 of 3	

Table 9: Aux Data for Error Type 259 (continued)

Aux Data	Description of Failure
32	The file name is too long – Internal firmware error on target board. 1. Retry the download, and escalate if it still fails.
40	FLASH programming failed on firmware – Internal firmware error on target board. 1. Retry the download, and escalate if it still fails.
All other Aux Data values	TFTP protocol error 1. Retry the download and escalate if it still fails.
3 of 3	

a. **Error Type 513** — Indicates that the schedule has failed. A schedule failure can result from:

- Any of the previously mentioned log-only errors (257 – 259)
- An expiration of the schedule timer
- An execution of `disable firmware download` command

To resolve the error and clear the alarm, use the `test firmware download` command. The Aux Data specifies the reason why the schedule failed. See [Table 10](#) for more details.

Table 10: Error Type 513 Aux Data

Aux Data	Description of Failure
1	Software resources not available; see Error Type 257 (a).
2	Source board-related failure; see Error Type 258 (b).
3	A target board failed; see Error Type 259 (c). 1. Check image, translations and retry.
4	Two consecutive target boards failed, download schedule aborted. 1. Verify download image, translations, and retry.
5	Schedule timer expired 1. Schedule unfinished target boards, and retry.
6	<code>disable firmware download</code> command executed.

2. **Error Type: 769** — Indicates that a downloadable board image is bad and that a good image needs to be downloaded. This error may be a result of a failed download attempt or a board that is in an unstable condition. The Aux Data indicates the location of the circuit pack requesting the firmware download and is in the form UUAAA, where UU is the port network number (cabinet) and AAA is the angel number.

The angel number can be converted into the carrier and slot number by using the following table. Continuing with the example of Aux Data 1080, you look for angel number 80 in [Table 11](#). You can find it in the column of carrier B and in the row of slot 15, so the target board is located in 1B15.

Table 11: Converting an angel number into carrier and slot

	Carrier				
	A	B	C	D	E
Slot #	Angel Number				
1	28	66	98	34	02
2	29	67	99	35	03
3	30	68	100	36	04
4	31	69	101	37	05
5	56	70	102	38	06
6	57	71	103	39	07
7	58	72	104	40	08
8	59	73	105	41	09
9	60	74	106	42	10
10	61	75	107	43	11
11	62	76	108	44	12
12	63	77	109	45	13
13	88	78	110	46	14
14	89	79	111	47	15
15	90	80	112	48	16
16	91	81	113	49	17
17	92	82	114	50	18
1 of 2					

Table 11: Converting an angel number into carrier and slot (continued)

	Carrier				
	A	B	C	D	E
Slot #	Angel Number				
18	93	83	115	51	19
19	94	84	116	52	20
20	95	85	117	53	21
21	NA	86	118	54	22
22	NA	87	119	55	23
<i>2 of 2</i>					

System Technician-Demanded Tests: Descriptions and Error Codes

Like the FW-DWNLD (Firmware Download) MO, its associated test, [Test Firmware Download \(#1413\)](#) on page 54, is non-traditional. Maintenance software automatically executes this test as part of scheduling, verifying, and running a firmware-download schedule.

This MO provides no on-demand tests for system technicians.

Test Firmware Download (#1413)

This test is **destructive**.

This test has two functions and can only be executed if there is a download schedule to verify or there are FW-DWNLD errors to resolve and alarms to clear.

1. This test verifies that the information on the **Firmware Download** screen is correct. It also verifies that the source board is of the correct type, that the file to be downloaded is present on that source board, and that the file is error free. In addition it verifies that the target board code and suffix are correct. It also retrieves the new firmware vintage for the target board and populates the appropriate field in the firmware download table.

2. If this test is executed after a firmware download schedule has run, and there are firmware download alarms/errors, it resolves the errors, clears the alarms, copies the current download status table to the last table, and clears out the current table.

Table 12: TEST #1413 Firmware Download Test

Error Code	Test Result	Description / Recommendation
	ABRT	Internal system error 1. Retry the command at 1-minute intervals up to 5 times.
2100	ABRT	System resources required for this test are not available. 1. Retry the command at 1-minute intervals up to 5 times.
1	FAIL	The firmware image file entered on the change firmware download screen is not present on the source board specified in the screen. 1. Execute the list directory board location command, and verify that: ● A file system is enabled on the board ● The file is present 2. If the file system is not enabled: a. Execute the enable filesystem command. b. FTP the correct firmware image to the source board. If the correct image file is present, then the name entered on the screen is incorrect. 3. Execute the change firmware download command, and enter the correct file name.
2	FAIL	The image file header on the source board is invalid. 1. FTP a good firmware image file to the source board.
3	FAIL	Firmware image file on the source board has a bad CRC. 1. FTP a good firmware image file to the source board.
4	FAIL	Firmware image file name is too long. 1. Rename the image file to a file name of the correct size. 2. FTP the new image file to the source board. 3. Execute the change firmware download command, and enter the new file name on the screen.
1 of 3		

Table 12: TEST #1413 Firmware Download Test (continued)

Error Code	Test Result	Description / Recommendation
5	FAIL	The TN code of the firmware image file on the source board does not match the TN code entered on the screen. The firmware file is incorrect for the board type entered on the screen. 1. Execute the list directory board location command, and verify that a file system is enabled on the board and the file is present. 2. If the file system is not enabled, execute the enable filesystem command, and FTP the correct firmware image to the source board. 3. Execute the change firmware download command, and enter the new file name on the screen.
6	FAIL	The suffix of the firmware image file on the source board does not match the suffix entered on the screen. The firmware image file is incorrect for the board types entered on the screen. 1. Execute the list directory board location command, and verify that a file system is enabled on the board and the file is present. 2. If the correct firmware image is not present, FTP the correct firmware image to the source board. 3. Execute the change firmware download command, and enter the new file name on the screen.
7	FAIL	The source board entered on the screen is not present. 1. Execute the display firmware download command, and verify the source board's location. 2. Verify the source board's translations. 3. If the location is incorrect, execute the change firmware download command, and enter the correct location on the screen.
8	FAIL	The source boards entered on the screen are incorrect. The board could have been changed after the schedule was entered. 1. Execute the list configuration command. Verify the source board's location. 2. Execute the change firmware download command, and enter the correct location on the screen.
	PASS	Firmware download to this circuit pack is successful.
2 of 3		

Table 12: TEST #1413 Firmware Download Test (continued)

Error Code	Test Result	Description / Recommendation
0	NO BOARD	The test could not relate the internal ID to the port (no board). This could be due to incorrect translations, no board is inserted, an incorrect board is inserted, or an insane board is inserted. 1. Ensure that the board's translations are correct. 2. If the board was already administered correctly, check the error log to determine whether the board is hyperactive. If so, the board was shut down. Reseat the board to reinitialize it. 3. If the board was found to be correctly inserted in step 1, then: a. Enter the <code>busyout board location</code> command. b. Enter the <code>reset board location</code> command. c. Enter the <code>release board location</code> command. d. Enter the <code>test board location long</code> command. This should re-establish the linkage between the internal ID and the port.
3 of 3		