FUJITSU

shaping tomorrow with you

FLASHWAVE® 7500

Metro/Regional Multiservice ROADM

Release 9.1
Issue 2, October 2013

Compatible with:

NETSMART® 1500 Version 8
NETSMART® 500 Version 5.2
NETSMART® 2000 Version 6

FNC-7500-0091-273

Upgrades and Migrations

Compliance

FCC

This equipment has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interferences when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio energy and if not installed in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, which the user will be required to correct at his/her expense.

Industry Canada

This digital apparatus does not exceed the Class A limits for noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications to ICES-003.

Cet appareil numérique ne dépasse pas les limites d'émission de bruit pour les appareils numériques de Classe A tel que définit dans le document NMB-003 publié par le Département Canadien de Communications.

Important

Observe all warnings in the text or on equipment labels regarding high-voltage or high-temperature conditions. The following warnings and figures apply to most Fujitsu products.

Plug-In Unit Cautions

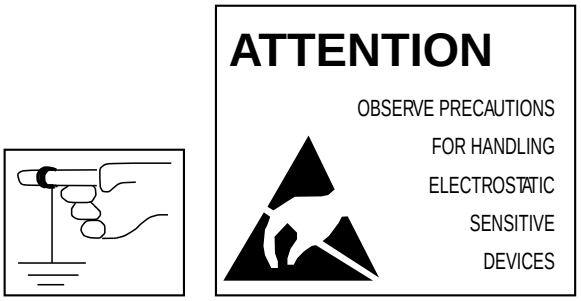
Observe the following precautions when handling plug-in units:

- Hold the plug-in unit only by its edges.
- Slowly and firmly push a plug-in unit into its slot to avoid damaging the unit. Do not force the unit. A slow insertion method minimizes power surges during installation. The longer ground connector pins ensure the ground circuit is connected first.

ESD Cautions

Units are stamped with anti-electrostatic markings (shown at right). Observe the following precautions to avoid damage from ESD:

- Always transport and store the unit in an ESD approved shipping bag.
- Always wear an ESD wrist strap, with a minimum 1-megohm resistance, that is connected to safety ground. Do not use a damaged wrist strap.

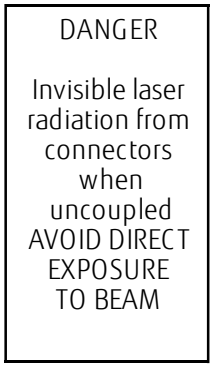


Anti-Electrostatic Markings

Fiber Warnings

Danger: Invisible laser radiation. Avoid direct exposure to the beam. Never look into the end of a fiber, fiber cord, or fiber pigtail. Permanent eye damage or blindness can occur quickly when laser radiation is present. The label on the right is attached to laser-emitting and receiving units as a reminder. Use of controls, adjustments, or procedures other than those specified may result in hazardous laser radiation exposure.

Danger: Never handle exposed fiber with your bare hands or touch it to your body. Fiber fragments can enter the skin and are difficult to detect and remove.



Laser Radiation Label

Avertissements de Fibre

La Danger: Le rayonnement laser Invisible. Eviter l'exposition directe au rayon. Jamais le regard dans la fin d'une fibre, une corde de fibre, ou la natte de fibre. Les dommages permanent d'oeil ou la cécité peut arriver rapidement quand le rayonnement laser est actuel.

La Prudence: L'Usage de contrôles ou d'ajustements ou l'exécution ou les procédures autrement que ces spécifié en ceci ont pour résultat l'exposition de rayonnement hasardeuse.

La Danger: Jamais la poignée a exposé la fibre avec vos mains nues ou le touche à votre corps. Les fragments de fibre peut entrer la peau et sont difficiles de détecter et enlever.

Installation Restrictions

The following guidelines apply when installing this equipment:

- Systems shall be installed only in restricted access areas (for example, dedicated equipment rooms or equipment closets) in accordance with the National Electrical Code, ANSI/NFPA 70.
- Equipment suitable for mounting over non-combustible surface ONLY.
- ***Caution:*** To de-energize the equipment, all input power circuits (-48Vdc battery) must be removed prior to maintenance/servicing or upgrading.
- Care should be taken not to compromise the stability of the rack by the installation of this equipment
- This equipment has a maximum operating ambient of 50 Deg C. The ambient temperature where the equipment is installed shall not exceed 50 Deg C.
- A minimum air clearance of 1.75" (1U) below the equipment must be maintained after the installation into the rack. the equipment can be installed at the very top location if desired.
- Care should be taken not to overload the supply circuit
- For the input power harness; Use only UL-Listed, dual closed loop, connectors.
- Suggested Vendor: Thomas and Betts - P/N:54205.
- Use Crimp Tool: Thomas and Betts P/N TBM25S for 6-AWG copper conductors.

Reliable earthing of the equipment must be maintained when installed in the rack. Use only UL-Listed, dual closed loop, connectors. Suggested Vendor and Part Number:

- Thomas and Betts - P/N: 256-30695-1070
- Use Crimp Tool: Thomas and Betts P/N TBM25S for 6-AWG copper connectors.

For the output distribution harness; Use only UL-Listed dual closed loop connectors. Suggested Vendor and Part Number:

- Thomas and Betts - P/N:256-30695-1298PH
- Use Crimp Tool: Thomas and Betts P/N TBM25S for 10-AWG copper connectors.

Restrictions d'Installation

Les indications suivantes s'appliquent en installant cet équipement:

- Les systémes seront seulement installés dans les secteurs d'accËs limités (par exemple, les piËces d'équipement dédié ou les placards d'Équipement) conformément au Code Electrique National, ANSI/NFPA 70.
- L'équipement convenable pour monter par-dessus la surface incombustible seulement
- ***La prudence:*** A de-stimule l'équipement, toute pile de (-48Vdc de circuits de pouvoir d'entrée) doit être enlevé avant entretien/entretenir ou avant améliorer.
- Le soin devrait être pris pour ne pas compromettre la stabilité de l'étagère par l'installation de cet équipement.
- Cet équipement a un maximum fonctionnant ambiant de 50 Deg C. La température ambiante où l'équipement est n'installé dépassera pas 50 Deg C.
- Un dégagement minimum d'air de 1.75" (1U) au dessous de l'équipement doit être maintenu après l'installation dans l'étagère. l'équipement peut être installé tout en haut l'emplacement si désiré.
- Le soin devrait être pris pour ne pas surcharger le circuit de provision
- Pour l'harnais d'entrée de pouvoir; seulement UL-LISTED les connecteurs de boucle fermés doubles seront utilisés.
- Le Vendeur suggéré: Thomas et Betts - P/N:54205.
- L'outil: Thomas et Betts - P/N:TBM25S pour les conducteurs de cuivre 6-AWG.

Earthing fiable de l'équipement doit être maintenu quand installé dans l'étagère. Utiliser la boucle fermée, double et seulement UL-ENUMERE, les connecteurs. Le Vendeur suggérés et Nombre de Partie:

- Thomas et Betts - P/N:256-30695-1070
- et utilise l'outil: Thomas et Betts - numéro de partie TBM25S pour 6-AWG connecteurs de cuivre.

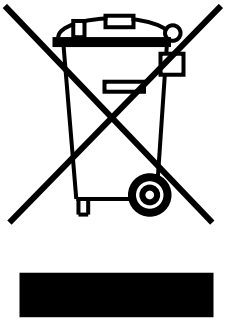
Pour l'harnais de distribution de production; seulement UL-LISTED les connecteurs de boucle fermés doubles seront utilisés. Le Vendeur et numéro de partie suggérés:

- Thomas et Betts - P/N: 256-30695-1298PH
- L'outil: Thomas et Betts P/N: TBM25S pour 10-AWG connecteurs de cuivre

Flammable Liquids Warning

Danger: Do not use flammable liquids or sprays, such as those used for cleaning optical connectors, around telecommunications equipment. Electrical fan motors and other potential ignition sources within the equipment might ignite the flammable material and cause personal injury or damage to the equipment. If uncertain about whether a liquid or spray is flammable, contact the manufacturer

Proper Disposal Procedures for Information Technology Equipment within the EU



All electrical and electronic equipment or units must be disposed of in accordance with European Directive 2001/96/EC for Waste Electrical and Electronic Equipment (WEEE).

Network communications or commercial equipment customers can dispose of Fujitsu equipment by contacting the Fujitsu regional office in their country. Customers can locate regional offices at http://www.fujitsu.com/global/.

Fujitsu will ensure the proper recycling, reuse, and other forms of recovery of WEEE. Potential hazardous substances in WEEE can harm the environment. You can contribute to the elimination of these effects through your cooperation.

Additional WEEE disposal information may be found at: http://www.fujitsu.com/global/about/environment/apporach/policy/

Document Change Notice

This notice lists the reasons for, location of, and a description of document changes. When the changes are extensive, a general statement giving the nature of the revisions is provided.

Reason for Document Change:	Updated for Release 9.1, Issue 2
Location of Change	**Description of Change**
Chapter 2	Updated Section 2.5, Upgrading Firmware on Equipment, Table 10.
Chapter 3	Updated Section 3.5.1, Identify Firmware Expansion Pack Files to Transfer subsection procedure. Updated Section 3.5.3, Copy Expansion Pack File to Target NE Standby NVM subsection procedure.
Chapter 4	Updated Section 4.2, Upgrading the Processor Unit procedure.
Chapter 9	Updated Section 9.3.3, Changing System Type procedure. Made the following changes in Section 9.3.6, Making Fiber-Optic Cable Connections: • Added eight new graphics throughout. • Updated Pass-Through Connections between Amplifiers subsection procedure. • Updated Table 135 in Pass-Through Connections between Amplifiers subsection. • Updated Table 136 in Install Mux/Demux Connections to Amplifier in Slot 1 subsection. • Updated Table 137 in Install Mux/Demux Connections to Amplifier in Slot 11 subsection.

Contents

1
About Upgrades and Migrations Procedures

In this chapter:

This practice provides upgrade procedures for the FLASHWAVE® 7500 system. Individuals involved with upgrading or expanding service should consult this practice.

This practice contains the following chapters:

- About Upgrades and Migrations Procedures– Provides an overview to upgrading a FLASHWAVE 7500 system
- Upgrading System Software from Release 4.1– Provides procedures for upgrading the Core Configuration from Release 4.1 to Release 4.2.
- Upgrading System Software from Release 4.2 or Later– Provides procedures to upgrade the Core/Small/ETSI Configurations from Release 4.2 through 5.2 to Release 6.1 or later.
- Upgrading to the Enhanced NEM–Provides upgrade procedures for upgrading the FLASHWAVE® 7500 system to the Enhanced NE Management (NEM) Processor plug-in unit (MPMA-SHP4)
- Adding or Deleting a Node in a Network– Describes how to add or delete a node in a FLASHWAVE 7500 ring network
- Adding or Deleting a Tributary Shelf– Describes how to add or delete a Tributary shelf in FLASHWAVE 7500 NE
- Converting Linear Network, Core Configuration– Describes how to convert a FLASHWAVE 7500 Core Configuration linear network to a ring network
- Upgrading Nodes, Core Configuration–Provides procedures for upgrading nodes in a FLASHWAVE 7500 Core Configuration network.
- Upgrading Nodes, Small/ETSI Configuration–Provides procedures for upgrading nodes in a FLASHWAVE 7500 Small/ETSI Configuration network.

1.1 Provisioning Hierarchy

In this section:

1.1.1 Service Provisioning Hierarchy

The following table lists the facility AIDTYPEs and SFP/XFP modules for each type of OLC. It is used to resolve ambiguity within subsequent provisioning hierarchy diagrams.

Table 1: Facility AIDTYPEs for OLCs and SFP/XFP Modules

Equipment Type				Facility AIDTYPEs						
OLC	SFP/XFP Module			Client Facility		Network-Side Facilities			DCC Facility	
	Name	Type	ACTTYPE	Optical	STS	STS	Network	Edge Facility	Client[1]	Network[2]
IFMA-SB				OCN				OCN		
				OC48				OC48	SDCC	
				1GE				1GE		
				1FC				1FC		
IFMA-HG IFMA-HL				OC192			OC192	OCH107	SDCC	
				OCN				OCH107		
IFMA-LE IFMA-LL				10GE				OCH111		
IFMA-U1 IFMA-U2 IFMA-U3 IFMA-U4				OC192			OC192	OCH107	SDCC	GCC0
				OCN				OCH107		
				10GE				OCH111		
				STM64			STM64	OCH107	SDCC[3]	
IFMA-U12 IFMA-U22 IFMA-U32				OC192			OC192	OCH107	SDCC	GCC0
				OCN				OCH107		
				10GE				OCH111		
IFMA-U52	XFP1-1410 XFP1-D420 XFP1-D430	10GELR 10GEER 10GEZR		10GE				OCH107		GCC0

1 Client SDCC is supported on the client SONET/SDH facility.
2 GCC0 is supported on the OCHxxx edge facility. Network SDCC is supported on the network SONET facility.
3 DCC for SDH is supported on the client STM-64 facility.

Table 1: Facility AIDTYPEs for OLCs and SFP/XFP Modules (Cont.)

Equipment Type				Facility AIDTYPEs						
OLC	SFP/XFP Module			Client Facility		Network-Side Facilities			DCC Facility	
	Name	Type	ACTTYPE	Optical	STS	STS	Network	Edge Facility	Client[1]	Network[2]
	XFP1-1410 XFP1-D420 XFP1-D430	OC192SR1 OC192IR1 OC192IR2 OC192LR2		OC192			OC192	OCH107	SDCC	GCC0
	XFP1-1410 XFP1-D420 XFP1-D430	OC192SR1 OC192IR1 OC192IR2 OC192LR2		OCN				OCH107		GCC0
	XFP1-1410 XFP1-D420 XFP1-D430	OC192SR1 OC192IR1 OC192IR2 OC192LR2		STM64			STM64	OCH107	SDCC	GCC0
	XFP1-1410 XFP1-D420 XFP1-D430	OTU2P1I12D1 OTU2P1S12D1 OTU2P1S12D2B OTU2P1L12D2		OCH107				OCH107	GCC0	GCC0
	XFP1-1410 XFP1-D420 XFP1-D430	OTU2EP1I12D1 OTU2EP1S12D1 OTU2EP1S12D2B OTU2EP1L12D2		OCH111				OCH111	GCC0	GCC0
IFMA-QU				OC768			OC768	OCH430		GCC0
				STM256			STM256			
				OCH430						
IFMA-QU2				OC768			OC768	OCH430	SDCC	GCC0
				STM256			STM256			
IFMA-8T IFMA-8T2	SFP1-0080 SFP1-0160	OC48SR1		OC48				OCH107		GCC0
	SFP1-0090 SFP1-0170	OC48IR1								
	SFP1-0100 SFP1-0180	OC48LR1								
	SFP1-0110 SFP1-0190	OC48LR2								
	SFP1-B40A...H	OC48C8L	OC48MC8L[4]							
IFMA-GU	SFP1-5000	1GESX		1GE			OC192	OCH107		GCC0
	SFP1-5010 SFP1-5200	1GELX								
	SFP1-5051	1GEZX								
	SFP1-5220	1GEBX10U								
	SFP1-5230	1GEBX10D								
	SFP1-B50A...H	1000C8L								
IFMA-QM IFMA-QM2	XFP1-1410 XFP1-D420 XFP1-D430	10GELR 10GEER 10GEZR		10GE			OCH107	OCH430		GCC0
	XFP1-1410 XFP1-D420 XFP1-D430	OC192SR1 OC192IR1 OC192IR2 OC192LR2		OC192 STM64			OCH107	OCH430	SDCC	GCC0

1 **Client SDCC is supported on the client SONET/SDH facility.**
2 **GCC0 is supported on the OCHxxx edge facility. Network SDCC is supported on the network SONET facility.**
4 ACTTYPE applies to multirate SFP modules only. It indicates the value returned by RTRV-EQPT, which is different from the type value used in provisioning. For example, in the IFMA-8T muxponder unit, the SFP module SFP1-B40A can be entered using equipment types OC48C8L. However, the RTRV-EQPT command will return OC48MC8L for this SFP module.

Table 1: Facility AIDTYPEs for OLCs and SFP/XFP Modules (Cont.)

Equipment Type				Facility AIDTYPEs						
OLC	SFP/XFP Module			Client Facility		Network-Side Facilities			DCC Facility	
	Name	Type	ACTTYPE	Optical	STS	STS	Network	Edge Facility	Client[1]	Network[2]
	XFP1-1410 XFP1-D420 XFP1-D430	OTU2P1I12D1 OTU2P1S12D1 OTU2P1S12D2B OTU2P1L12D2		OCH107			OCH107	OCH430		GCC0
	Any mix of client interfaces[5]			10GE OC192 STM64 OCH107			OCH107	OCH430	SDCC	GCC0
IFMA-BX (Digital Wrapper Mode)	SFP1-5000	1GESX		1GE FOSPORT	STS1 STS3/3C	STS1 STS3/3C	OC192	OCH107	SDCC	GCC0
	SFP1-5010 SFP1-5200	1GELX								
	SFP1-5220	1GEBX10U								
	SFP1-5230	1GEBX10D								
	SFP1-5051	1GEZX								
	SFP1-0020 SFP1-0021	OC3IR1		OC3	STS1 STS3/3C	STS1 STS3/3C				
	SFP1-0030 SFP1-0031	OC3LR1								
	SFP1-0050 SFP1-0051	OC12IR1		OC12	STS1 STS3/3C STS12/12C	STS1 STS3/3C STS12/12C				
	SFP1-0060 SFP1-0061	OC12LR1								
	SFP1-0080 SFP1-0160	OC48SR1		OC48	STS1 STS3/3C STS12/12C STS48/48C	STS1 STS3/3C STS12/12C STS48/48C				
	SFP1-0090 SFP1-0170	OC48IR1								
	SFP1-0100 SFP1-0180	OC48LR1								
	SFP1-0110 SFP1-0190	OC48LR2								
	SFP1-B40A...H	10008CL	OC48MC8L	1GE	STS1 STS3/3C	STS1 STS3/3C				
		OC3C8L		OC3	STS1 STS3/3C	STS1 STS3/3C				
		OC12C8L		OC12	STS1 STS3/3C STS12/12C	STS1 STS3/3C STS12/12C				
		OC48C8L		OC48	STS1 STS3/3C STS12/12C STS48/48C	STS1 STS3/3C STS12/12C STS48/48C				
IFMA-BX (Native OC-192 Mode)	SFP1-5000	1GESX		1GE[6] FOSPORT	STS1 STS3/3C	STS1 STS3/3C	OC192		SDCC	SDCC
	SFP1-5010 SFP1-5200	1GELX								
	SFP1-5220	1GEBX10U								
	SFP1-5230	1GEBX10D								
	SFP1-5051	1GEZX								

1 **Client SDCC is supported on the client SONET/SDH facility.**
2 **GCC0 is supported on the OCHxxx edge facility. Network SDCC is supported on the network SONET facility.**
5 Type OCH430 edge facility supports type OCH107 network facilities only.
6 Each 1GbE SFP inserted in the 10G Flexponder unit (IFMA-BX) supports two client facilities, types 1GE and FOSPORT, simultaneously.

Table 1: Facility AIDTYPEs for OLCs and SFP/XFP Modules (Cont.)

Equipment Type				Facility AIDTYPEs						
OLC	SFP/XFP Module			Client Facility		Network-Side Facilities			DCC Facility	
	Name	Type	ACTTYPE	Optical	STS	STS	Network	Edge Facility	Client[1]	Network[2]
	SFP1-0020 SFP1-0021	OC3IR1		OC3	STS1 STS3/3C	STS1 STS3/3C				
	SFP1-0030 SFP1-0031	OC3LR1								
	SFP1-0050 SFP1-0051	OC12IR1		OC12	STS1 STS3/3C STS12/12C	STS1 STS3/3C STS12/12C				
	SFP1-0060 SFP1-0061	OC12LR1								
	SFP1-0080 SFP1-0160	OC48SR1		OC48	STS1 STS3/3C STS12/12C STS48/48C	STS1 STS3/3C STS12/12C STS48/48C				
	SFP1-0090 SFP1-0170	OC48IR1								
	SFP1-0100 SFP1-0180	OC48LR1								
	SFP1-0110 SFP1-0190	OC48LR2								
	SFP1-B40A...H	10008CL	OC48MC8L	1GE FOSPORT	STS1 STS3/3C	STS1 STS3/3C				
		OC3C8L		OC3	STS1 STS3/3C	STS1 STS3/3C				
		OC12C8L		OC12	STS1 STS3/3C STS12/12C	STS1 STS3/3C STS12/12C				
		OC48C8L		OC48	STS1 STS3/3C STS12/12C STS48/48C	STS1 STS3/3C STS12/12C STS48/48C				
IFMA-SM	SFP1-5000	1GESX		1GE	ODU0 ODU1	ODU0 ODU1		OCH[7] (Rate=10. 71) OTU2 ODU2	SDCC GCC0	GCC0
	SFP1-5010	1GELX								
	SFP1-5220	1GEBX10U								
	SFP1-5230	1GEBX10D								
	SFP1-0021	OC3IR1		OC3 STM1	ODU0 ODU1	ODU0 ODU1				
	SFP1-0030 SFP1-0031	OC3LR1								
	SFP1-0051	OC12IR1		OC12 STM4	ODU0 ODU1	ODU0 ODU1				
	SFP1-0061	OC12LR1								
	SFP1-0080	OC48SR1		OC48 STM16	ODU0 ODU1	ODU0 ODU1				
	SFP1-0090	OC48IR1								
	SFP1-0100 SFP1-0180	OC48LR1								
	SFP1-0110 SFP1-0190	OC48LR2								
	SFP1-B40A...H	10008CL		1GE	ODU0 ODU1	ODU0 ODU1				

1 Client SDCC is supported on the client SONET/SDH facility.
2 GCC0 is supported on the OCHxxx edge facility. Network SDCC is supported on the network SONET facility.
7 Creation or deletion of a OCH facility (rate=10.71) will auto create/delete OTU2 and ODU2 facility.

Table 1: Facility AIDTYPEs for OLCs and SFP/XFP Modules (Cont.)

Equipment Type				Facility AIDTYPEs						
OLC	SFP/XFP Module			Client Facility		Network-Side Facilities			DCC Facility	
	Name	Type	ACTTYPE	Optical	STS	STS	Network	Edge Facility	Client[1]	Network[2]
		OTU1C8L		OCH[8] (Rate=2.67) OTU1 ODU1	ODU0 ODU1	STS1 STS3/3C				
		OC3C8L		OC3	ODU0 ODU1	ODU0 ODU1				
		OC12C8L		OC12	ODU0 ODU1	ODU0 ODU1				
		OC48C8L	OC48MC8L	OC48	ODU0 ODU1	ODU0 ODU1				
IFMA-RG IFMA-RG3								OCH107 OCH111		GCC0
IFMA-QR IFMA-QR2								OCH430		GCC0

Pass-Through Channel Provisioning

Proceed to the applicable provisioning hierarchy listed as follows:

Core	WSS	Figure 1
	2D-ROADM	Figure 1
	ILA	Not applicable
Small/ETSI	40-Ch WSS without Raman Amplifier	Figure 1
	40-Ch WSS with Raman Amplifier	Figure 2
	2D-ROADM	Figure 1
	ILA	Not applicable
Small	32-Ch ROADM	Figure 1
	32-Ch FOADM	Figure 3
Extension		Not applicable

1 Client SDCC is supported on the client SONET/SDH facility.
2 GCC0 is supported on the OCHxxx edge facility. Network SDCC is supported on the network SONET facility.
8 Creation or deletion of a OCH facility (rate=2.67) will auto create/delete OTU1 and ODU1 facility.

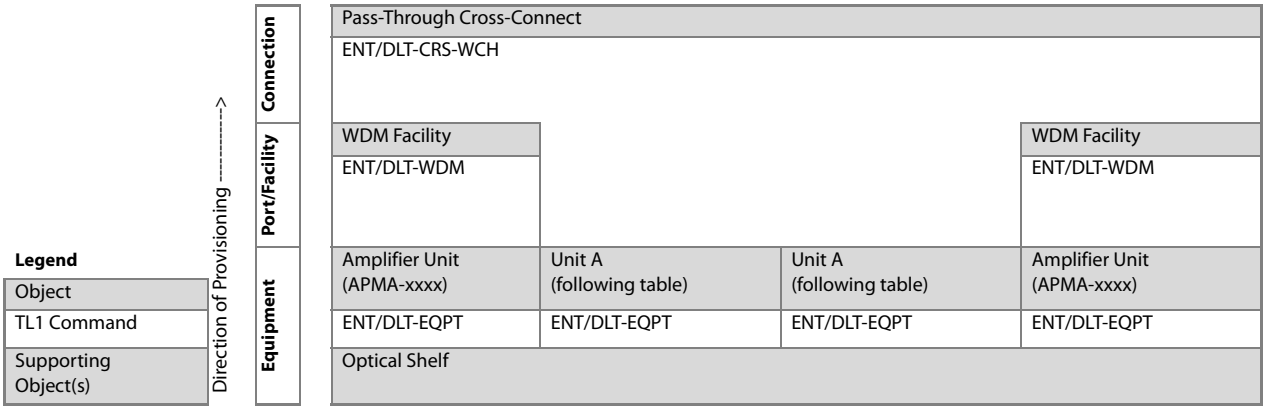


Figure 1: Pass-Through Channel Service Provisioning Hierarchy (All ROADM Configurations without Raman Amplifier)

The figure referenced in the previous table refers to a plug-in unit that varies depending on the system configuration. The following table lists the unit for each configuration.

Table 2: Configuration-Dependent Details

Configuration		Unit A
Core	WSS	WSS Core Switch Unit (SFMA-CMC1)
	2D-ROADM	2D-ROADM Unit (SFMA-RDC1)
Small/ETSI	40-Ch WSS without Raman Amplifier	WSS Core Switch Unit (SFMA-CMC1)
	2D-ROADM	2D-ROADM Unit (SFMA-RDC1)
Small	32-Ch ROADM	Mux/Demux Unit (MDXP-MDC3) and Switch Fabric (SWXP-SWC1)

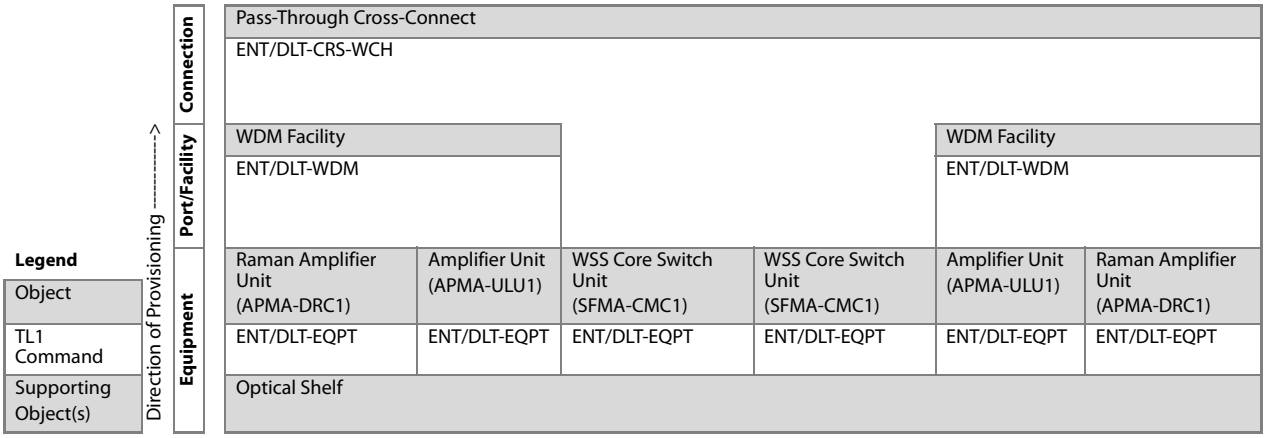


Figure 2: Pass-Through Channel Service Provisioning Hierarchy (Small/ETSI Configurations with Raman Amplifiers)

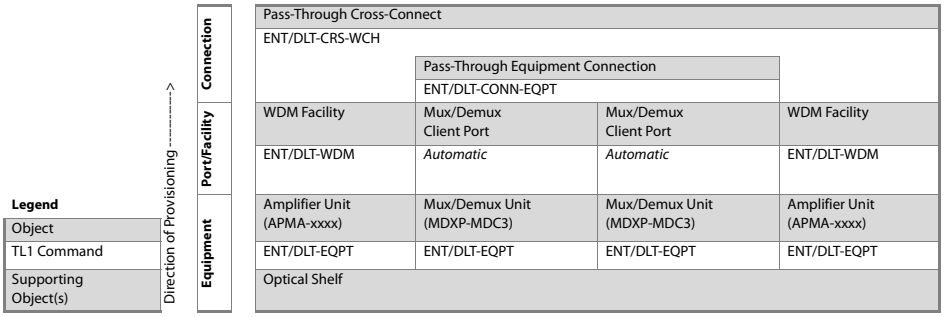


Figure 3: Pass-Through Channel Service Provisioning Hierarchy (32-Ch FOADM Small)

Channel Add/Drop with OCh-DPRING Protection

Proceed to the applicable provisioning hierarchy listed as follows:

Core	WSS	Figure 4
	2D-ROADM	Figure 4
Small/ETSI	40-Ch WSS without Raman Amplifier	Figure 4
	40-Ch WSS with Raman Amplifier	Figure 5
	2D-ROADM	Figure 4
Small	32-Ch ROADM	Figure 4
	32-Ch FOADM	Figure 4
Extension		Figure 6

The following table applies to all configurations except the Extension Configuration and the Small /ETSI Configuration with Raman Amplifiers. It shows the provisioning hierarchy for a channel add/drop with OCh-DPRING protection. The following table begins with creation of the OLC equipment entity and finishes with provisioning of the OCh-DPRING protection group. In the following table , the caveat **if applicable** indicates that the entity may or may not be required. Use Table 1, which lists the facilities and SFP/XFP modules applicable to each type of OLC, to resolve this ambiguity.

Note: *The following table generalizes TL1 commands for creating/deleting OLC facilities (ENT/DLT-**AIDTYPE**). Use Table 1 to determine the applicable AIDTYPEs for each type of OLC. For example, the TL1 command for entering the client facility on the IFMA-LE (LAN PHY Transponder) is ENT-10GE.*

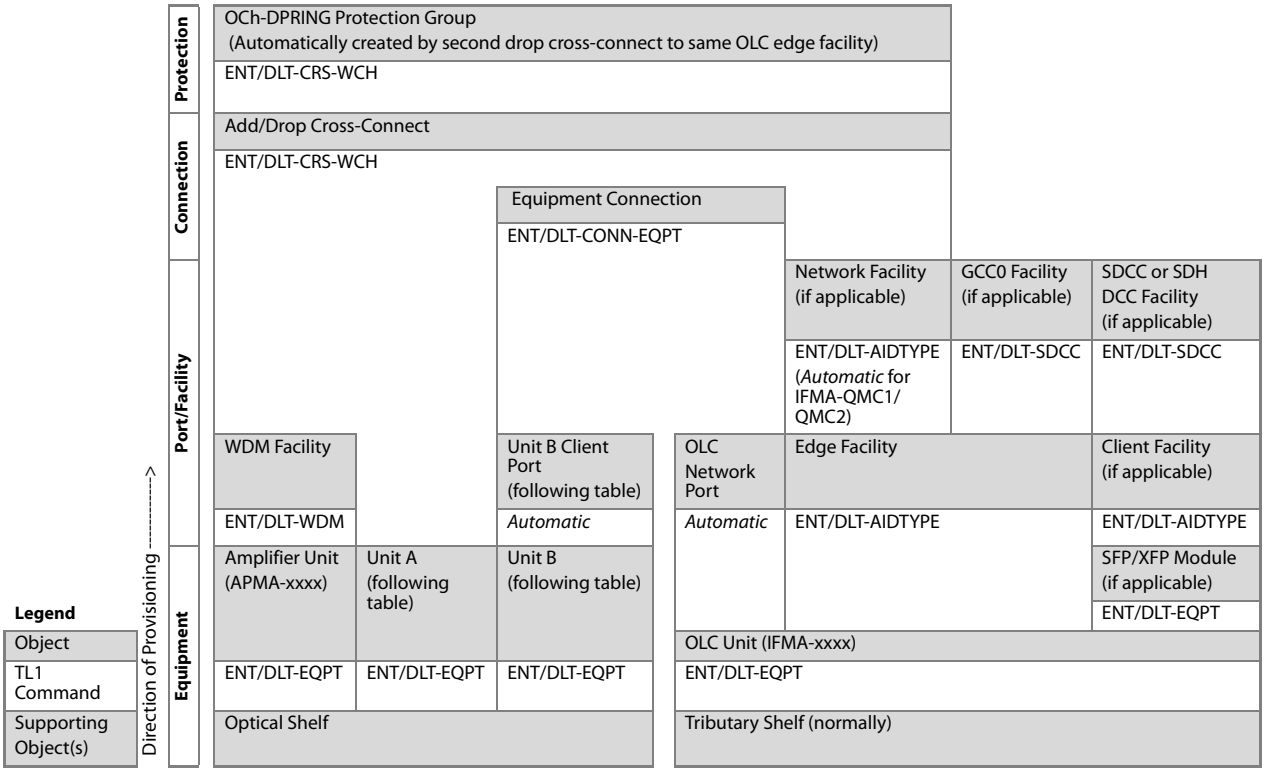


Figure 4: Service Provisioning Hierarchy–Channel Add/Drop with OCh-DPRING Protection (All OADM Configurations without Raman Amplifier)

The following table lists these units for each configuration listed in the previous table.

Table 3: Configuration-Dependent Details for Service Provisioning Hierarchy–Channel Add/Drop with OCh-DPRING Protection (All OADM Configurations without Raman Amplifier)

Configuration		Unit A	Unit B	Unit B Client Port
Core	WSS	WSS Core Switch Unit (SFMA-CMC1)	Mux/Demux Unit (MDMA-RMC1)	Mux/Demux Client Port (MDMA-RMC1)

Table 3: Configuration-Dependent Details for Service Provisioning Hierarchy–Channel Add/Drop with OCh-DPRING Protection (All OADM Configurations without Raman Amplifier) (Cont.)

Configuration		Unit A	Unit B	Unit B Client Port
	2D-ROADM	Not applicable	2D-ROADM Unit (SFMA-RDC1)	2D-ROADM Client Port (SFMA-RDC1)
Small/ ETSI	40-Ch WSS without Raman	WSS Core Switch Unit (SFMA-CMC1)	Mux/Demux Unit (MDMA-RMC1)	Mux/Demux Client Port (MDMA-RMC1)
	2D-ROADM	Not applicable	2D-ROADM Unit (SFMA-RDC1)	2D-ROADM Client Port (SFMA-RDC1)
Small	32-Ch Small, FOADM	Not applicable	Mux/Demux Unit (MDXP-MDC3)	Mux/Demux Client Port (MDXP-MDC3)
	32-Ch Small ROADM	Mux/Demux Unit (MDXP-MDC3)	Switch Fabric Unit (SWXP-SWC1)	Switch Fabric Client Port (SWXP-SWC1)

applies to the Small/ETSI Configuration with Raman Amplifiers. It shows the provisioning hierarchy for a channel add/drop with OCh-DPRING protection. The following figure begins with creation of the OLC equipment entity and finishes with provisioning of the OCh-DPRING protection group. In the following table, the caveat **if applicable** indicates that the entity may or may not be required. Use Table 1, which lists the facilities and SFP/XFP modules applicable to each type of OLC, to resolve this ambiguity.

Note: *The following table generalizes TL1 commands for creating/deleting OLC facilities (ENT/DLT-**AIDTYPE**). Use Table 1 to determine the applicable AIDTYPEs for each type of OLC. For example, the TL1 command for entering the client facility on the IFMA-LE (LAN PHY Transponder) is ENT-10GE.*

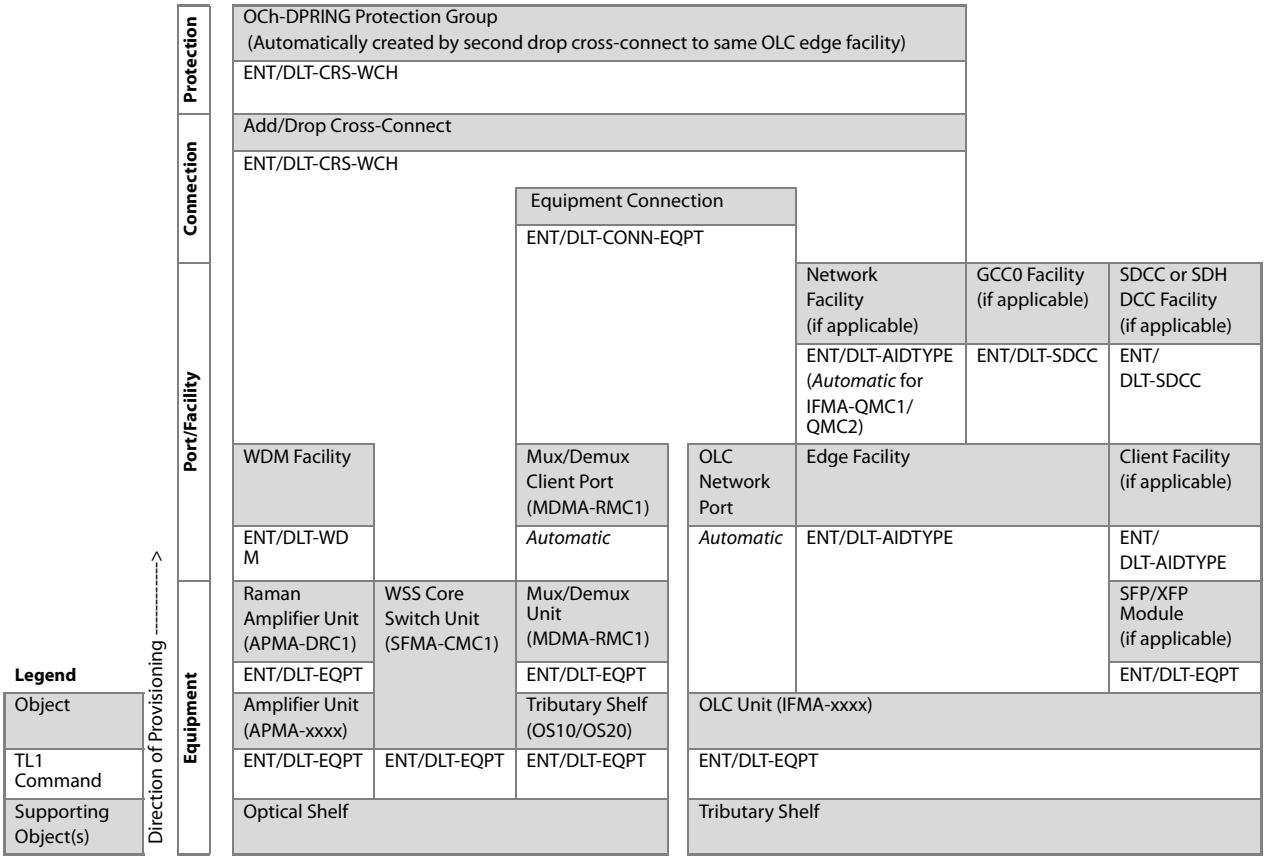


Figure 5: Service Provisioning Hierarchy–Channel Add/Drop with OCh-DPRING Protection (Small/ETSI Configuration with Raman Amplifiers)

The following table applies to the Extension Configuration. It shows the provisioning hierarchy for a channel add/drop with OCh-DPRING protection. The following table begins with creation of the OLC equipment entity and finishes with provisioning of the OCh-DPRING protection group. In the following table , the caveat **if applicable** indicates that the entity may or may not be required. Use Table 1, which lists the facilities and SFP/XFP modules applicable to each type of OLC, to resolve this ambiguity.

Note: *The following table generalizes TL1 commands for creating/deleting OLC facilities (ENT/DLT-**AIDTYPE**). Use Table 1 to determine the applicable AIDTYPEs for each type of OLC. For example, the TL1 command for entering the client facility on the IFMA-LE (LAN PHY Transponder) is ENT-10GE.*

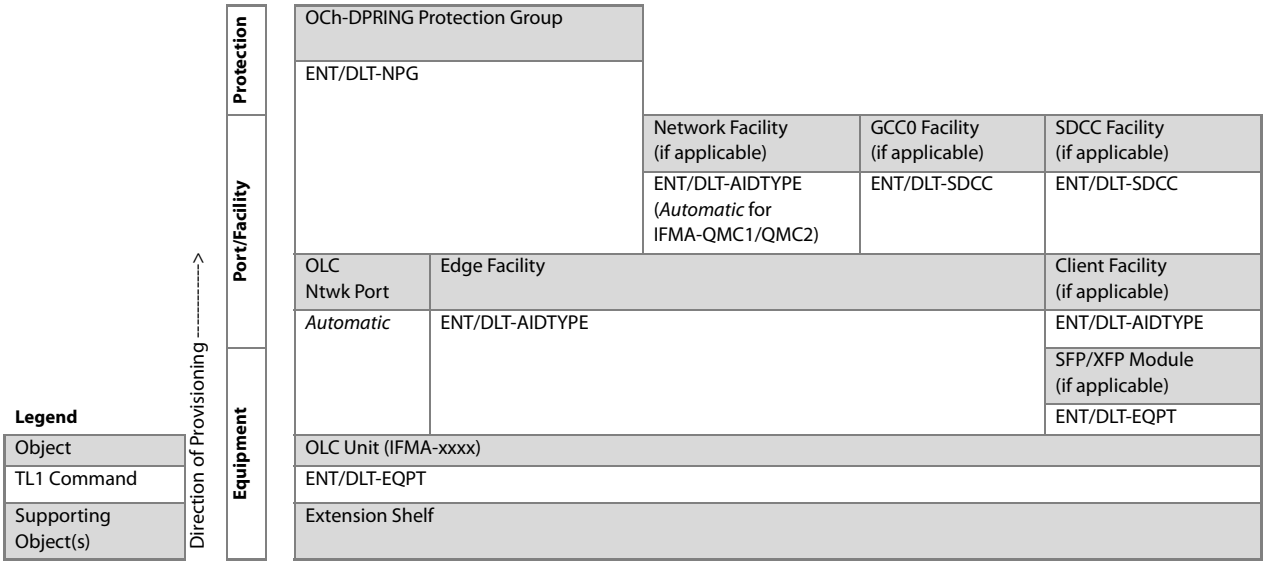


Figure 6: Service Provisioning Hierarchy–Channel Add/Drop with/without OCh-DPRING Protection (Extension Configuration)

Channel Add/Drop without OCh-DPRING Protection

Provisioning for an unprotected add/drop is identical to an OCh-DPRING–protected add/drop but does not include the protection level. Proceed to the applicable hierarchy that follows, but ignore the protection level of the diagram:

Core	WSS	Figure 4
	2D-ROADM	Figure 4
Small/ETSI	40-Ch WSS without Raman Amplifier	Figure 4
	40-Ch WSS with Raman Amplifier	Figure 5
	2D-ROADM	Figure 4
Small	32-Ch ROADM	Figure 4
	32-Ch FOADM	Figure 4
Extension		Figure 6

FLASHWAVE LIGHTGUARD Protection

The following table presents the provisioning hierarchy for FLASHWAVE LIGHTGUARD protection, which is applicable to transponders and muxponders only. It begins with creation of the OLC and FLASHWAVE LIGHTGUARD unit equipment entities and finishes with creation of the FLASHWAVE LIGHTGUARD protection group. As indicated in the following table , SFP/XFP modules are applicable only to muxponders.

Note: *The following table generalizes TL1 commands for creating/deleting the OLC client facilities (ENT/DLT-**AIDTYPE**). Use Table 1 to determine the applicable AIDTYPEs for each type of OLC. For example, the TL1 command for entering the client facility on the IFMA-LE (LAN PHY Transponder) is ENT-10GE.*

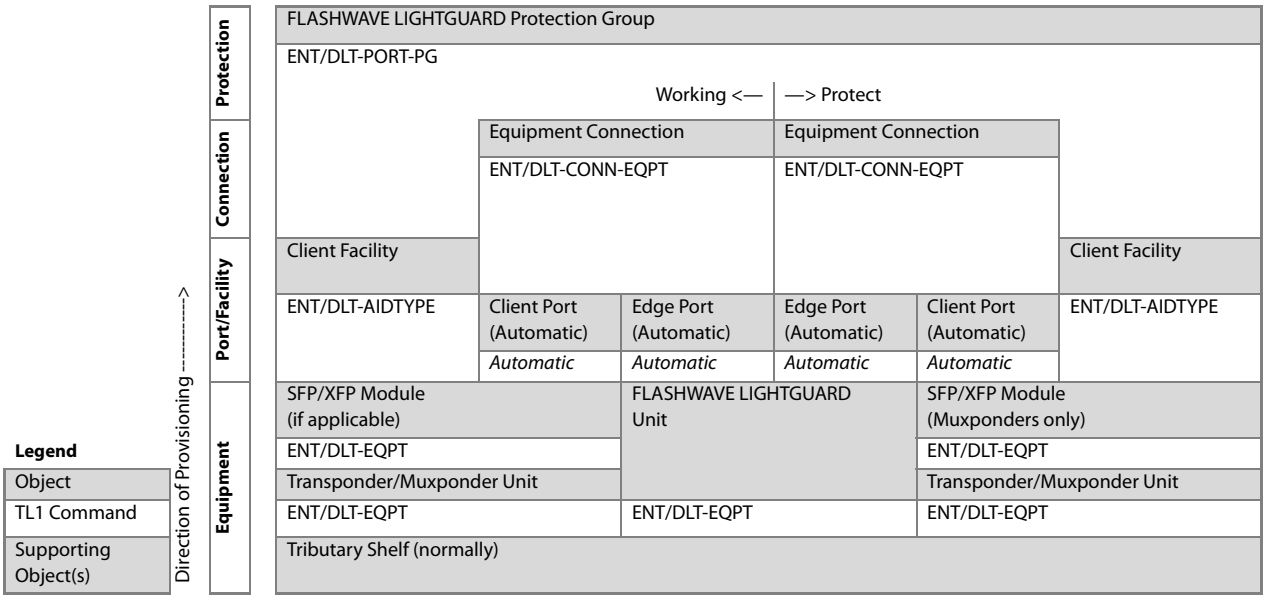


Figure 7: Service Provisioning Hierarchy–FLASHWAVE LIGHTGUARD Protection

Flexponder with Client 1+1 Protection

The following table presents the provisioning hierarchy for client 1+1 protection for the 10G Flexponder (IFMA-BX). It begins with creation of working and protect Flexponder units and finishes with creation of the 1+1 fiber facility protection group.

Note: *An SDCC can be associated with the working client facility only.*

Note: *The following table generalizes TL1 commands for creating/deleting the client facilities (ENT/DLT-**AIDTYPE**). Use Table 1 to determine the applicable AIDTYPEs for each type of SFP/XFP module. For example, the TL1 command for entering an OC-48 client facility is ENT-OC48.*

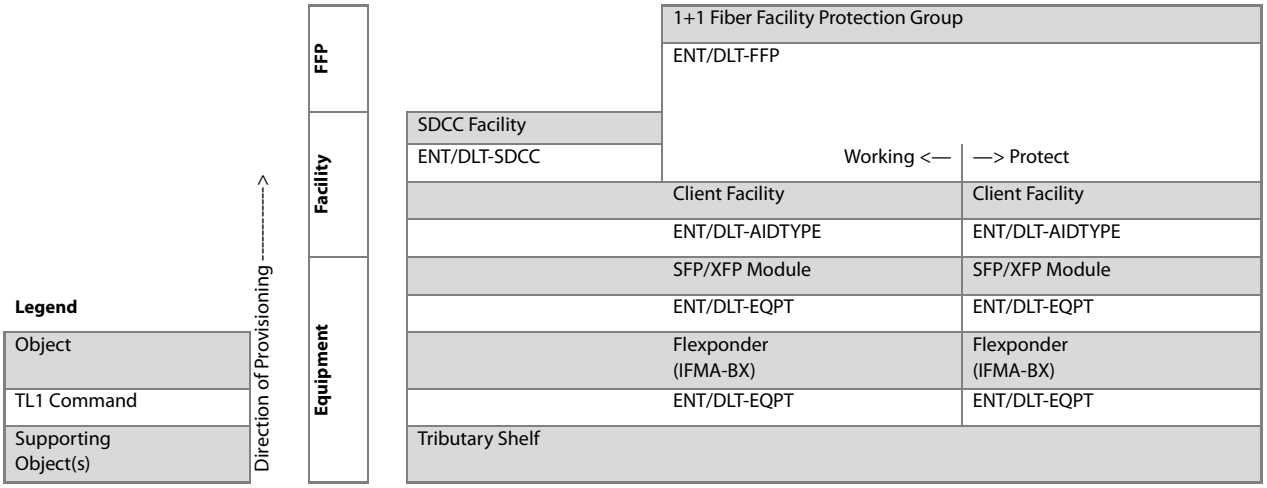


Figure 8: Service Provisioning Hierarchy–Flexponder Pair with Client 1+1 Protection

The following table builds on the provisioning hierarchy indicated in the previous table, adding edge, network, and GCC0 facilities and STS time slots. The following table includes two sets of *network* STS time slots, one for each Flexponder, but only one set of *client* STS time slots, and this set is associated with the working Flexponder. Client STS time slots are not shown for the protect Flexponder because they are not used in provisioning operations; the client 1+1 FFP group ensures that any cross-connect made to/from a working client STS time slot is automatically mirrored on the protect side. The following tables are similar, except with Flexponder B provisioned for native OC-192.

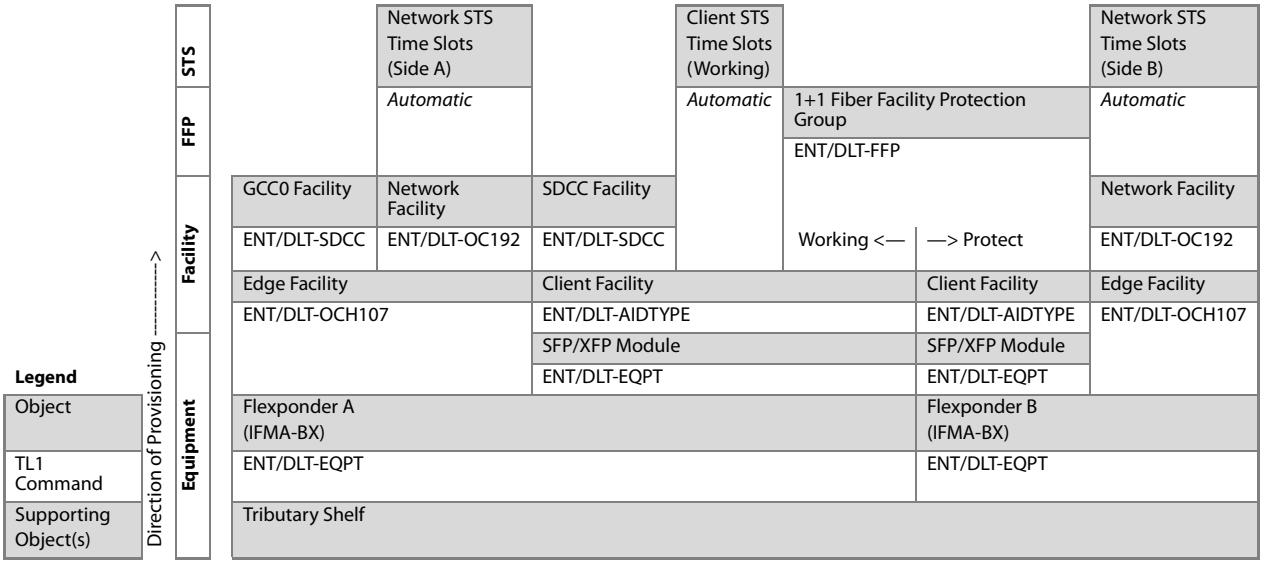


Figure 9: Service Provisioning Hierarchy–STS Time Slots for Flexponder Pair with Client 1+1 Protection

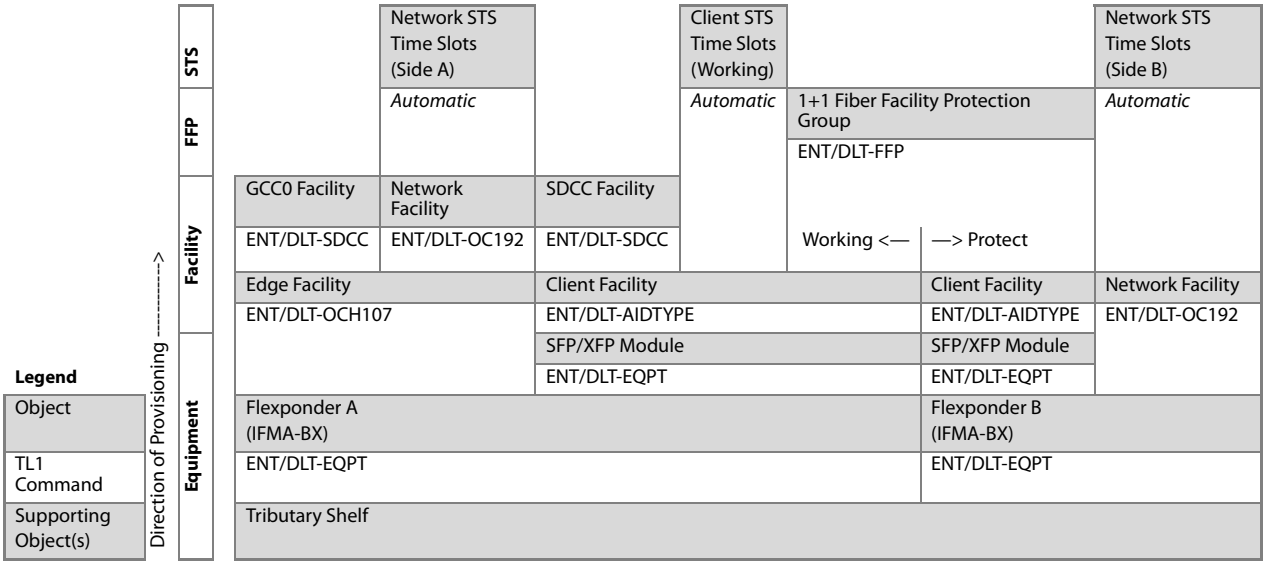


Figure 10: Service Provisioning Hierarchy–STS Time Slots for Flexponder Pair with Client 1+1 Protection with Flexponder B Provisioned for Native OC-192

The following figure presents the hierarchy for provisioning of STS cross-connects and the UPSR protection group.

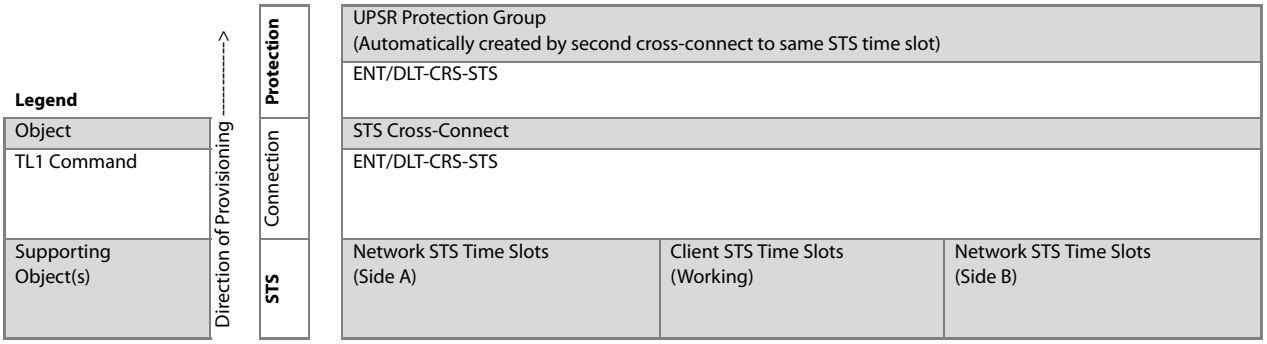


Figure 11: Service Provisioning Hierarchy–STS Cross-Connects and UPSR

1.1.2 Turn-Up Provisioning Hierarchy, Core Configuration

The various entities (equipment, facilities, cross-connects, and so on) within the FLASHWAVE 7500 Core Configuration must be provisioned in a certain order. This section contains provisioning hierarchy tables that indicates the order in which the entities can be added to or deleted from the system, along with the applicable TL1 root commands.

Shelf Entities, WSS Core Configuration

The following figure presents the provisioning hierarchy for shelves of the FLASHWAVE 7500 WSS Core Configuration system. Auxiliary Optical shelves OS2...OS4, OS25, and OS26 apply to HUB configurations only. Auxiliary Optical shelves OS25 and OS26 apply to asymmetric HUB configurations only. The WSS Core Configuration supports a maximum of 20 tributary shelves per node.

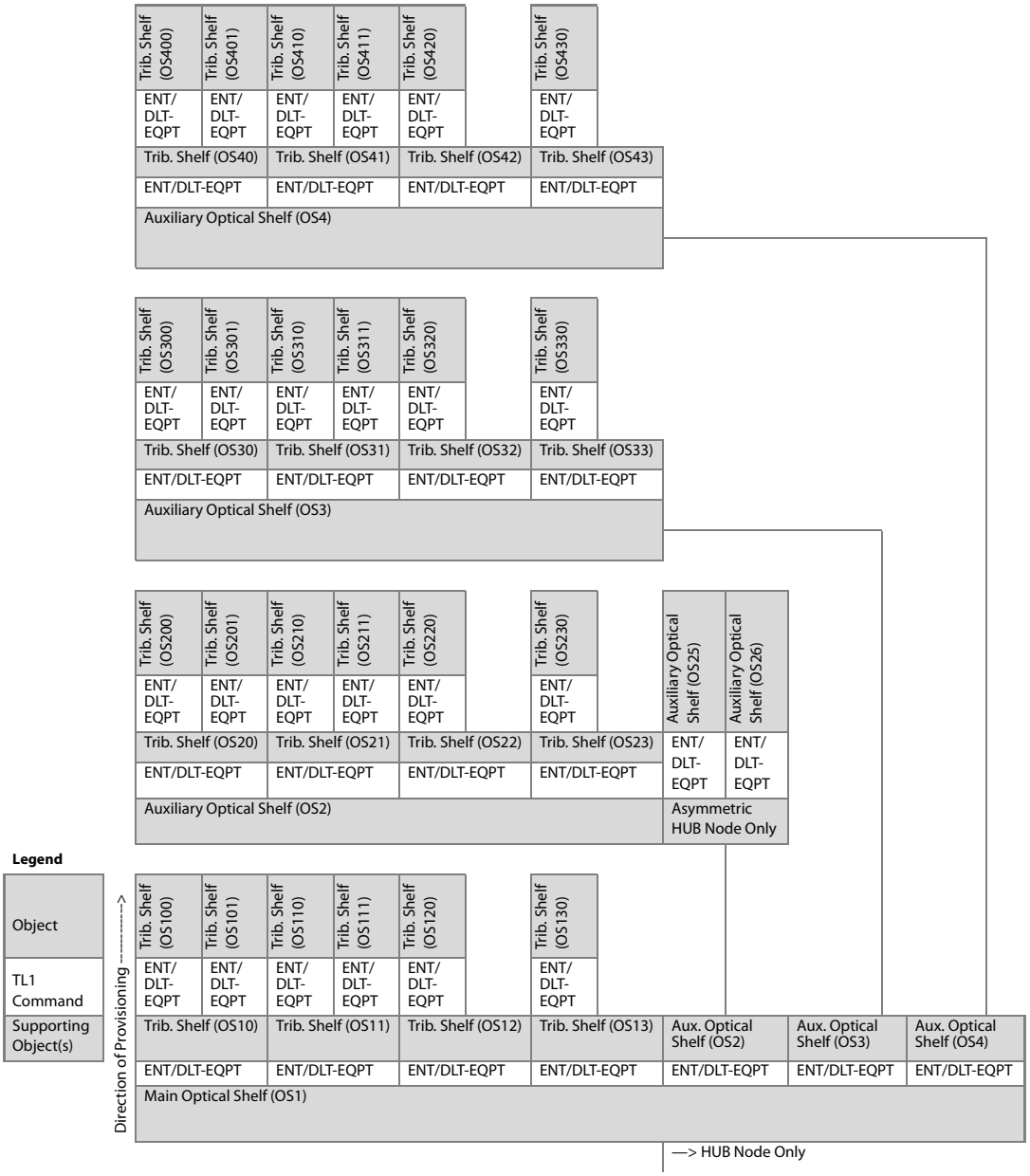


Figure 12: Turn-Up Provisioning Hierarchy–Shelves (WSS Core Configuration)

Optical Shelf Equipment, WSS Core Configuration

The following figure presents the hierarchy for provisioning equipment within optical shelves of the WSS Core Configuration system. It applies to the Main Optical shelf (OS1) and to the Auxiliary Optical shelves (OS2...OS4, OS25, OS26) if the node is a HUB node.

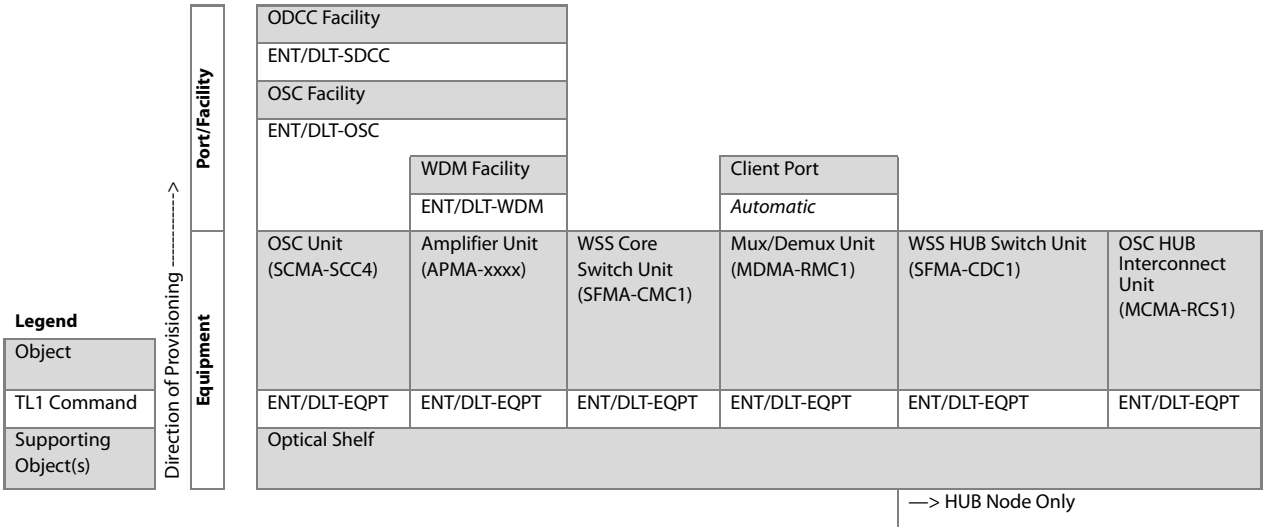


Figure 13: Turn-Up Provisioning Hierarchy–Optical Shelf (WSS Core Configuration)

Shelf Entities, 2D-ROADM Core Configuration

The following figure presents the provisioning hierarchy for shelves of the FLASHWAVE 7500 2D-ROADM Core Configuration system.

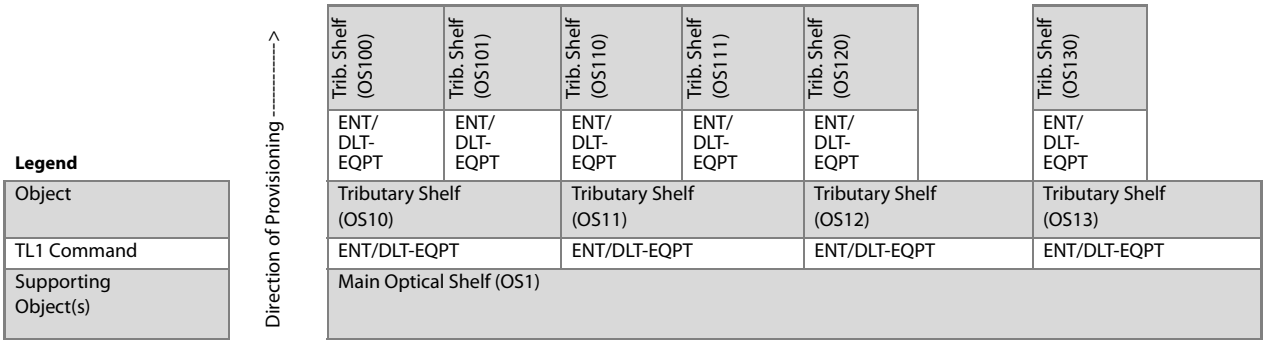


Figure 14: Turn-Up Provisioning Hierarchy–Shelves (2D-ROADM Configuration)

Optical Shelf Equipment, 2D-ROADM Core Configuration

The following figure presents the hierarchy for provisioning equipment within the Optical shelf of the 2D-ROADM Core Configuration system.

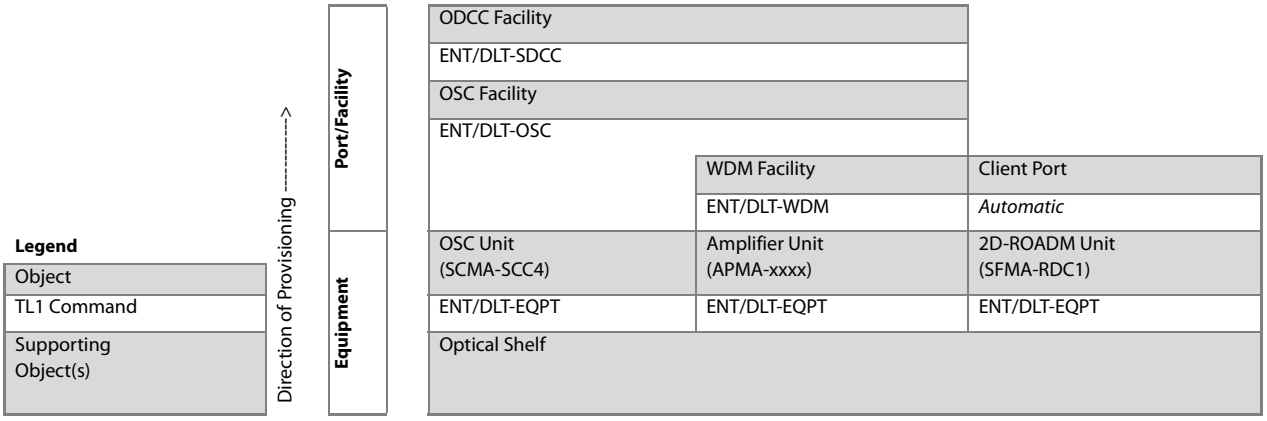


Figure 15: Turn-Up Provisioning Hierarchy–Optical Shelf (2D-ROADM Core Configuration)

1.1.3
Turn-Up Provisioning Hierarchy, Small and ETSI Configurations

The various entities (equipment, facilities, cross-connects, and so on) within the FLASHWAVE 7500 system must be provisioned in a certain order. The provisioning hierarchy diagrams presented in this section provide a graphical depiction of the order in which the entities can be added to or deleted from the system, along with the applicable TL1 root command.

Shelf Entities, Small and ETSI Configurations

The following figure presents the provisioning hierarchy for shelves of the FLASHWAVE 7500 Small and ETSI Configuration systems. Auxiliary Optical shelves OS2...OS4 apply to HUB configurations only.

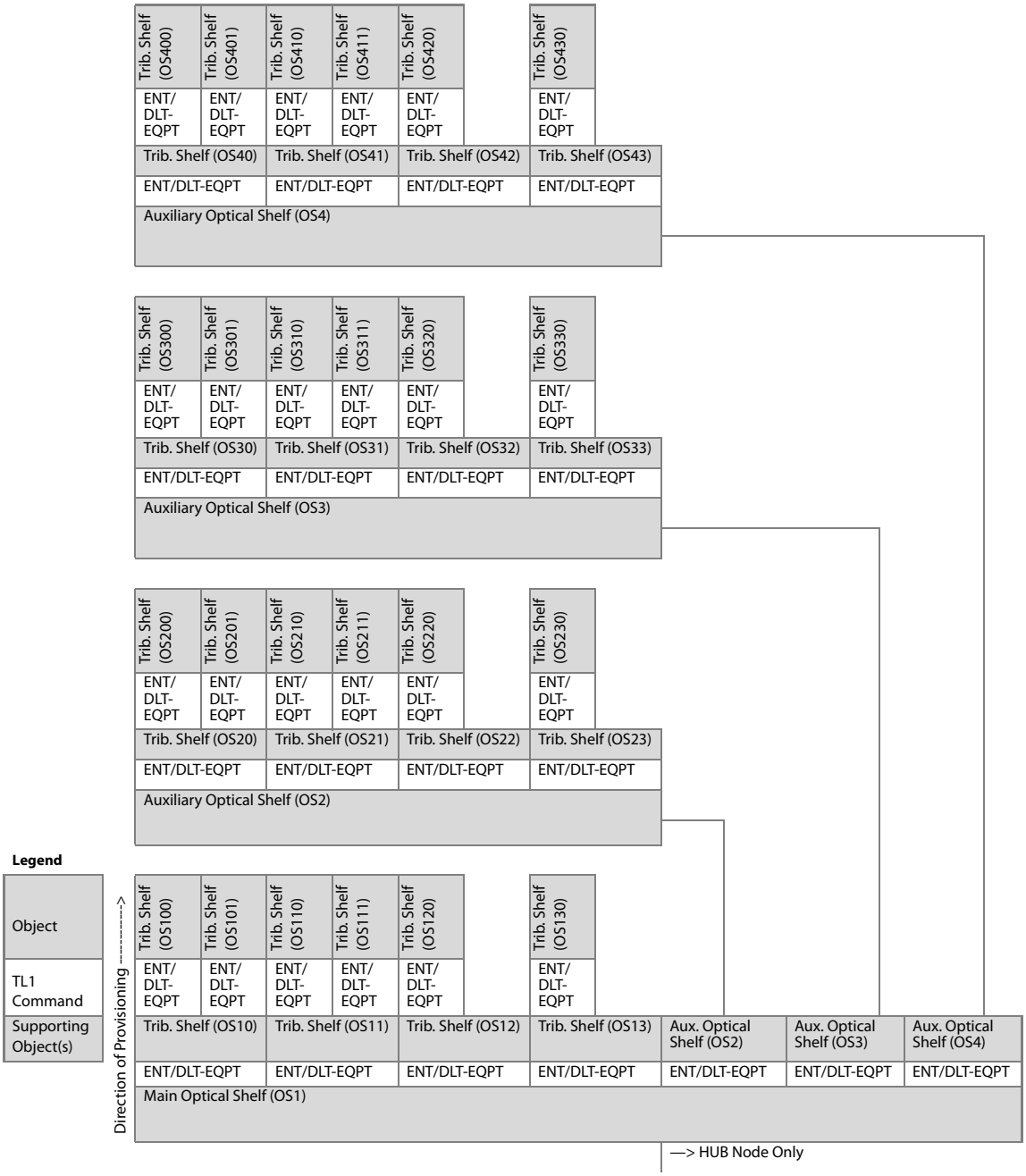


Figure 16: Turn-Up Provisioning Hierarchy–Shelves (Small/ETSI Configuration)

Turn-Up Provisioning, Small/ETSI WSS Configuration

The following figures present the hierarchy of provisioning for turning up the ETSI Configuration system. The first figure does not include the Raman Amplifier. The second figure includes the Raman Amplifier.

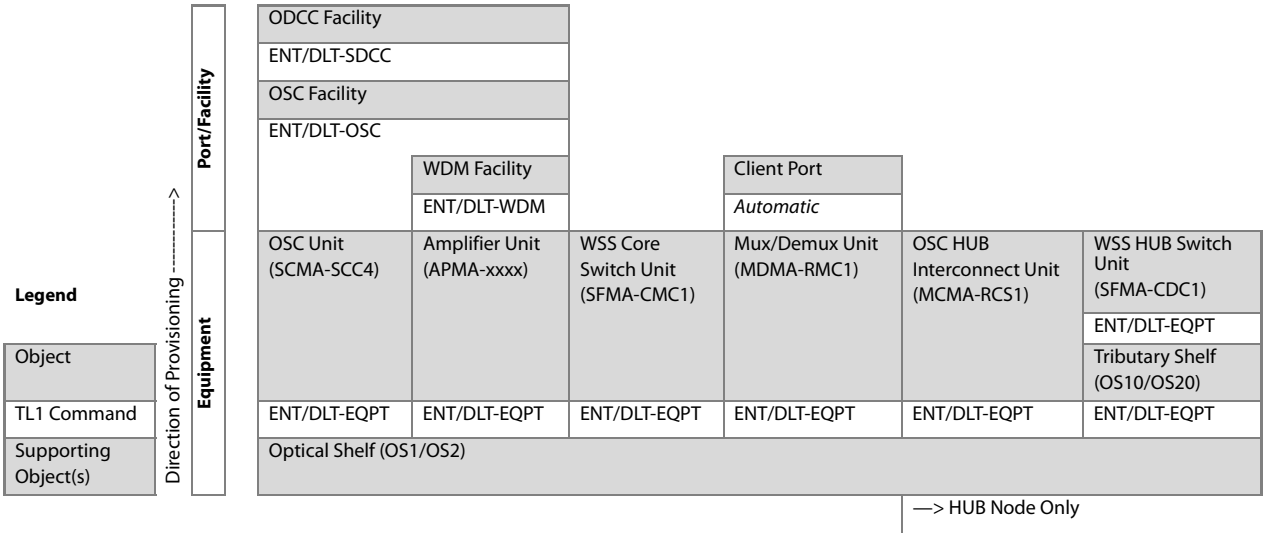


Figure 17: Turn-Up Provisioning Hierarchy–Small/ETSI WSS Configuration (without Raman Amplifier)

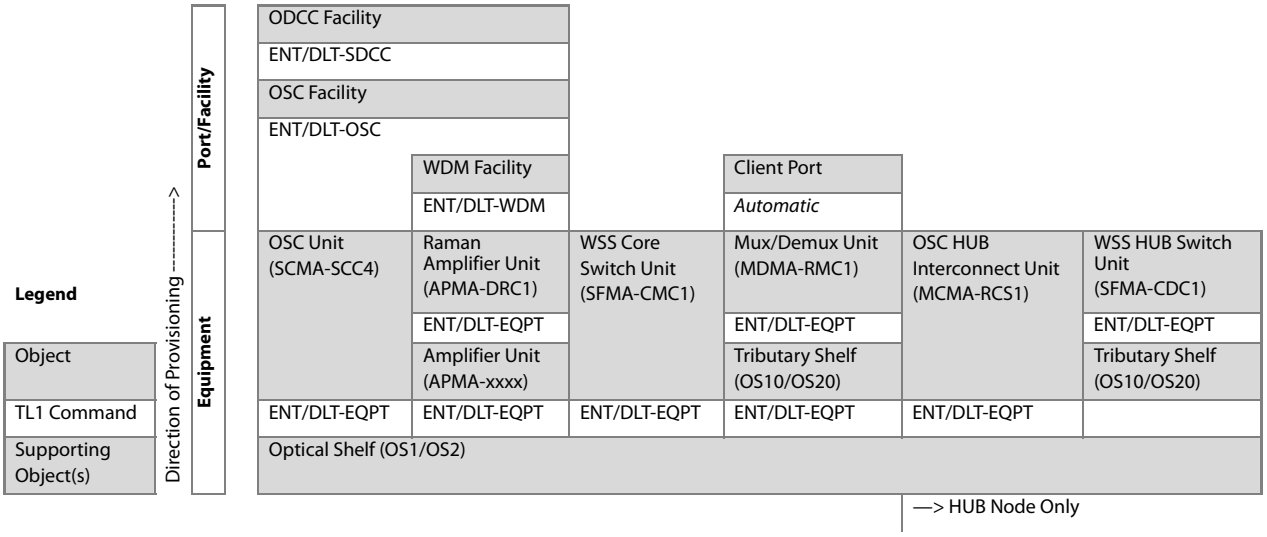


Figure 18: Turn-Up Provisioning Hierarchy–Small ETSI WSS Configuration (with Raman Amplifier)

Turn-Up Provisioning, 2D-ROADM Small/ETSI Configuration

The following figure presents the hierarchy for provisioning equipment within the Optical shelf of the 2D-ROADM Small/ETSI Configuration system.

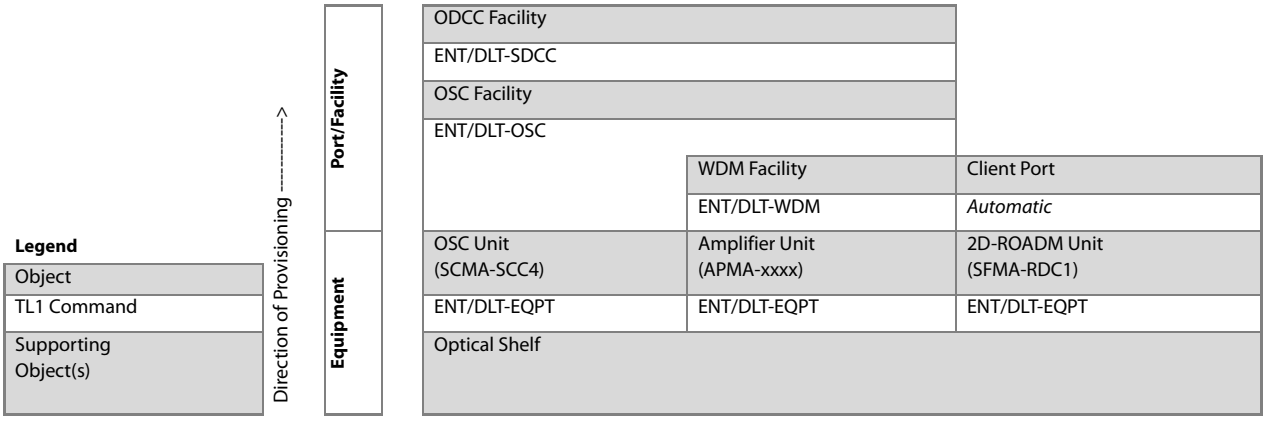


Figure 19: Turn-Up Provisioning Hierarchy–Optical Shelf (2D-ROADM Small/ETSI Configuration)

Turn-Up Provisioning, 32-Ch FOADM Small Configuration

The following figure presents the hierarchy for provisioning equipment within the Optical shelf of the 32-Ch FOADM Small Configuration system.

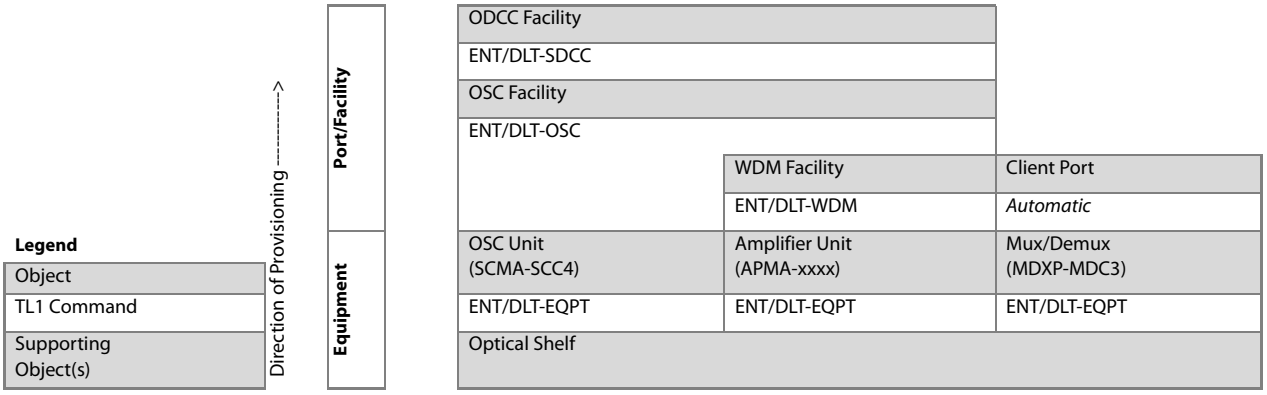
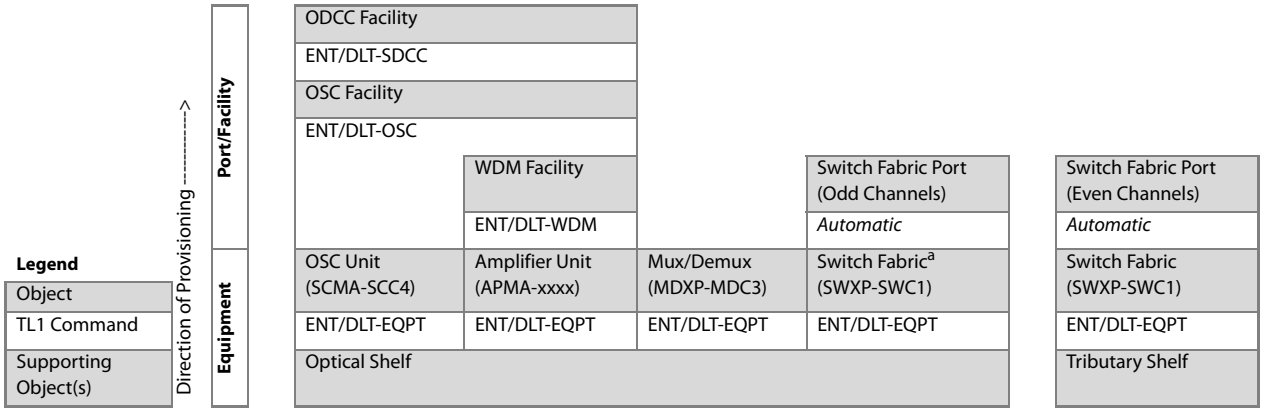


Figure 20: Turn-Up Provisioning Hierarchy–Optical Shelf (32-Ch FOADM Small Configuration)

Turn-Up Provisioning, 32-Ch ROADM Small Configuration

The following figure presents the hierarchy for provisioning equipment within the Optical shelf of the 32-Ch ROADM Small Configuration system. In addition, the following table describes provisioning of switch fabric plug-in units to support the even-numbered channels within one of the tributary shelves.



[a] The SWXP-SWC1 plug-in unit is not compatible with APMA-ULU1 Issue 6 and later or APMA-M2U1 Issue 4 and later.

Figure 21: Turn-Up Provisioning Hierarchy–Optical Shelf (32-Ch ROADM Small Configuration)

1.1.4 Turn-Up Provisioning Hierarchy, Extension Configuration

This section contains the provisioning hierarchy table for turning up the FLASHWAVE 7500 Extension Configuration system without service.

The various entities (equipment, facilities, cross-connects, and so on) within the FLASHWAVE 7500 Extension Configuration must be provisioned in a certain order. This section contains provisioning hierarchy tables that indicates the order in which the entities can be added to or deleted from the system, along with the applicable TL1 root commands.

The following figure presents the hierarchy for provisioning equipment within the Extension Configuration system.

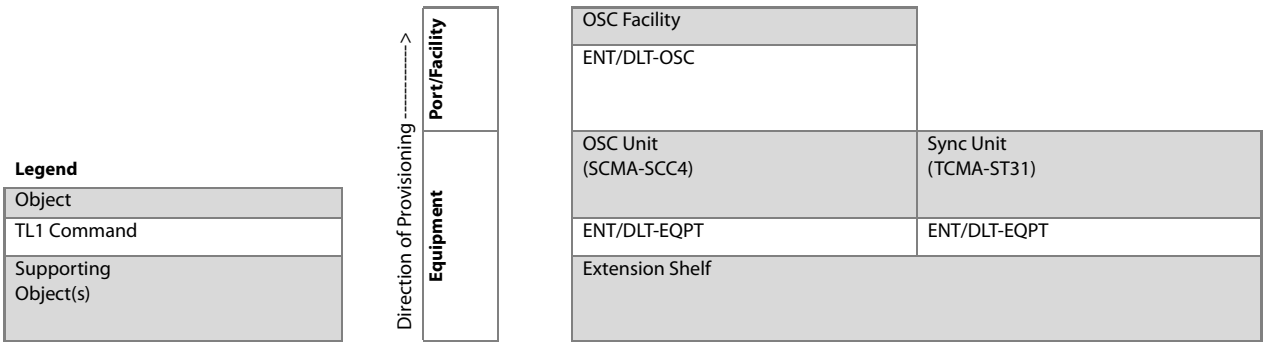


Figure 22: Turn-Up Provisioning Hierarchy–Shelf (Extension Configuration)

2
Upgrading System Software from Release 4.1

In this chapter:

This chapter provides instructions to upgrade the configuration from Release 4.1.

After completing the upgrade, if required, use the procedures in Upgrading System Software from Release 4.2 or Later to upgrade the configuration to Release 6.x, 7.x, 8.x, or 9.1.

The upgrade procedure does not affect traffic.

2.1 Device and User Prerequisites to Upgrade from Release 4.1 to Release 4.2

Before proceeding with the upgrade procedure, perform or verify the following:

- Ensure that the craft interface device or PC is connected, activated, and set up in the required interface modes as described in Craft and OSS.
- Verify that the user has user privilege code (UPC) Level 4 access and that the automatic time-out option (TMOUTA) is set to N (TL1) or False (NETSMART® 500 network element graphical user interface) as described in System Administration.

2.2
Software Requirements

The following table lists the software required to upgrade.

Table 4: Software Requirements to Upgrade Configuration

Release	Unit	Part Number (CD-ROM)	Description
Release 4.2	CD-ROM	FC9682CR04-I06	FLASHWAVE 7500 Release 4.2.2 software

The following table lists the system software file names and generic issue (GISSUE) values for the release upgrade.

Table 5: Software File Names and GISSUE Values

Release	Unit	Value/File Name	Description
Release 4.2	GISSUE	04-02-2	Release 4.2 GISSUE value
	Software generics	F7504022.PGM	Release 4.2 OSL program file
		A7504022.PGM	Release 4.2 firmware (FW) program file
	Additional software	F7504022.SIG	Release 4.2 signature file
		F7504022.CON	Release 4.2 configuration file
		SWDL.TXT	Release 4.2 software download text file

2.3 Upgrading System Software Using TL1

In this section:

Caution: *After the system software has upgraded and the latest firmware file (generic) containing the firmware loads for each plug-in unit has been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the procedure in Upgrading Firmware on Equipment, at an appropriate time by following local practices. For more details, refer to Maintenance.*

Caution: *In Release 5.1 of the FLASHWAVE 7500 system, support is discontinued for the 2.5G Flexponder plug-in unit (IFMA-AUxx) and all 4-channel OLCs except IFMA-SBxx plug-in units (Refer to the following table). Also, support is discontinued for redundant processors introduced in Release 4.2. Ensure that the system to be upgraded does not include the 2.5G Flexponder plug-in unit or any 4-channel OLCs, except IFMA-SB plug-in units, prior to upgrading system software to Release 5.1 and later.*

Table 6: 4-Channel OLCs Not Supported in Release 5.1 and later

Plug-In Unit
IFMA-8Txx, excluding IFMA-8TC1 and IFMA-8TC2
IFMA-GUxx, excluding IFMA-GUC1
IFMA-HGxx, excluding IFMA-HGC1
IFMA-HLxx, excluding IFMA-HLC1
IFMA-LExx, excluding IFMA-LEC1
IFMA-LLxx, excluding IFMA-LLC1
IFMA-SAxx

2.3.1 Prepare to Upgrade Using TL1

Use this procedure to copy software files from the CD-ROM to the File Transfer Protocol (FTP) server and to collect information about the FTP server in preparation for performing the procedure in Upgrading System Software Using TL1.

Step 1
Read the software release notes document that is packaged on the CD-ROM along with the software files.

Step 2
Ensure that an FTP server is setup and available on the craft interface PC, or another computer, that is available to the FLASHWAVE® 7500 NE through the local management port (LMP) or local communication network (LCN) port.

Note: *If the FTP server connection is through the LMP port, the Transmission Control Protocol/Internet Protocol (TCP/IP) settings of the FTP server must be set to match those listed in* Table: Craft Interface Set Up Procedures *in* Setting Up Craft Interface (TL1 Session through TERM2).

Note: *For instructions on setting up the LCN port, refer to* Craft Interface Connector Specifications.

Step 3
Record the IP address of the FTP server.

Note: *If the FTP server resides on the craft interface PC, the IP address of the FTP server is the same as the IP address of the craft interface PC.*

Note: *Enter this IP address as the value of SRC in* Upgrade System Software from a Server Using TL1.

```
139.145.23.43
```

Step 4
Record the user name and password to be used for accessing the FTP server.

Note: *The user name and password will be entered as values for keywords FTUID and FTPID in* Upgrade System Software from a Server Using TL1.

```
UID=swdluser,PID=moonrock
```

Step 5
On the FTP server, create a new directory (or locate an existing directory) to contain the software files.

Step 6
Record the path to the directory created (or located) in the previous step.

Note: *The path will be entered as the value of keyword FTPATH in* Upgrade System Software from a Server Using TL1.

```
C:\GENERICS
```

Step 7
Copy all of the files listed in Table 5 in Software Requirements from the CD-ROM to the directory you created (or identified) in Step 5.

Step 8
Continue to Upgrade System Software from a Server Using TL1.

2.3.2
Upgrade System Software from a Server Using TL1

This procedure provides the steps to upgrade system software for a FLASHWAVE 7500 NE using TL1 commands and software files located on an FTP server.

Upgrading a nonfirmware supporting software release to a firmware supporting software requires a two-stage process. Since a nonfirmware supporting system will not accept a firmware file download, the system must first be upgraded to a firmware supporting system without downloading the firmware file and configuration file. Steps 1 through 9 provide steps for the first stage (downloading and activating the software download without the firmware file and the configuration file). After the software activation completes, proceed with Steps 10 through 32 (second stage) to repeat the download of software files; however, this time include the firmware file and configuration file.

A high level outline of the first stage steps follows:

- Download the software program file and copy to standby memory.
- Activate the software (Release 4.2).

A high level outline of the second stage steps follows:

- Download the configuration file and copy to standby memory. Download the firmware file and copy to standby memory. Repeat download of the software program file and copy to standby memory. Activate the software.

Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command.

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

Before starting this procedure, complete all steps in Prepare to Upgrade Using TL1. The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Attention: *Failure to perform prerequisite procedures in the proper sequence may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages. For assistance, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822).*

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters.*

Log On

Upgrade system software as follows:

Note: *Default values are shown in bold.*

Step 1
Ensure that the NEM Shelf Processor and OSC plug-in units are inserted in the NE and that the NE is ready to be upgraded.

Step 2
Ensure that the system does not include any 4-channel OLCs, except IFMA-SB plug-in units. Refer to Table 6.

Step 3
Close all unrelated applications currently running on your craft interface or PC, and disable the PC screen saver and power save options, if enabled.

Step 4
Log on the NE.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to N (TL1).*

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values. The TID, UID, and PID values are not case-sensitive.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For more detailed information, refer to* Craft Interface Operations .

TL1

Start a terminal or terminal emulator program (for example, HyperTerminal®).

For **TERM1** (Serial):
Press CTRL+X.

The Welcome screen opens.
Press 3 for TL1.

For **TERM2** (TCP/IP):

Establish a Telnet session using IP address 192.168.1.1 and default port 23.

TL1

```
ACT-USER:TID:UID:CTAG::PID;
```

TID:

- FUJITSU (Target identifier of the node; 7 to 20 alphanumeric characters)

UID:

- ROOT (User identifier; 4 to 10 alphanumeric characters)

PID:

- ROOT (Private identifier associated with UID; 6 to 10 alphanumeric characters, with at least one alphabetic character and one nonalphabetic character, such as a punctuation mark or number)

Example:

```
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;
```

Download Software File

Step 5
Copy the software load file from the FTP server to the RAM disk of the NE.

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer to the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction) (Refer to Table 5 in Software Requirements.)

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to Table 7.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU:139.145.23.43,F7504022.PGM,RDISK,F7504022.PGM:CTAG:::
OVERWRITE=Y,FTUID=\"swduser\",FTPID=\"moonrock\", FTPATH=\"C:\GENERICS\\";
```

Table 7: CPY-FILE Keyword and Domain Input Parameters

Keyword	Domain (Default in Bold)	Description
OVERWRITE[9]	Overwrite files	

Table 7: CPY-FILE Keyword and Domain Input Parameters (Cont.)

Keyword	Domain (Default in Bold)	Description
	Y	Write over files with the same name at DST
	N	Do not write over files with the same name at DST
COMMENT	\"xxxxx\" **null**	Sets the user-defined comment, where the comment is up to 60 ASCII characters delineated by escape quotes ***Note:*** *The CPY-FILE command is denied if the COMMENT keyword exceeds 60 characters.*
SIGNATURE[10]	8 hex digits **00000000**	Signature code for each file. When more than one file is transferred, signatures are separated with an & character. ***Note:*** *If SIGNATURE is 0 (zero), the file checksum will not be performed.*
FTUID	\"xxxxx\" **null**	UID used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPID	\"xxxxx\" **null**	Password used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPATH	\"xxxxx\" **null**	Path to the control file on the server; up to 40 ASCII characters delineated by escape quotes

Step 6
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Step 7
Copy the software load from the RAM disk into standby nonvolatile memory (NVM).

[9] OVERWRITE=Y must be specified when transferring a file from the FLASHWAVE 7500 NE to another location when using FTP or FTAM.
[10] The SIGNATURE keyword is ignored when transferring a file from the NE to any other location.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- PGM (program file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,F7504022.PGM,STBY,:CTAG::PGM:
COMMENT=\"eth 01/17/2007\";
```

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow. The NOT READY LED goes out when the copy operation completes.*

Step 8
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Activate the Software

Step 9
Activate the software load in standby memory.

TL1

```
INIT-SYS:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- Refer to the following table for keyword and domain input parameters.

Example:

```
INIT-SYS:FUJITSU::CTAG:::GISSUE=04-02-1,ACTDAT=00-00-00,
ACTTM=00-00-00,VALTM=00-45-00;
```

Table 8: INIT-SYS Keyword and Domain Input Parameters for SWDL

Keyword	Domain (Default in Bold)	Description
GISSUE	xx-yy-z	Generic issue number: • xx = 00…99 • yy = 00…99 • z = 0…9, A…Z
ACTDAT[11]	yy-mm-dd	Activation date (year-month-day): • yy = 00…99 • mm = 00…12 • dd = 00…31
ACTTM[11][12]	hh-mm-ss	Activation time (hour-minute-second): • hh = 00…23 • mm = 00…59 • ss = 00…59 Activation time must be set using a 24-hour time format and be less than 185 days. Use 00-00-00 for immediate activation.
VALTM[11][13]	hh-mm-ss **00-45-00**	Validation time (hour-minute-second): • hh = 00…99 • mm = 00…59 • ss = 00…59 Minimum time is 45 minutes.

The user is automatically logged off once activation starts.

Step 10
Wait approximately 15 minutes to allow the NE to reset and convert the database into Release 4.2 format. When the FAIL/SVCE LED on the NEM Shelf Processor unit lights green, log on the NE. Refer to Step 4, if necessary.

Note: *During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 11
Retrieve and verify software version information.

[11] For a generic issue switch to take place, GISSUE, ACTDAT, and ACTTM must be specified. The VALTM parameter is optional.
[12] Only one scheduled activation of date and time is allowed. The INIT-SYS command is denied if a previous INIT-SYS command was entered with either a software generic or a database activation request.
[13] The timer is started after the new release of software is activated and expires after a duration of hhmmss. If the timer is not canceled with the CANC-VALTM command, its expiration causes the system to revert back to the previous release of the software.

TL1

```
RTRV-VERSION:TID:AID:CTAG;
```

AID:

- ACT, STBY, **ALL**

Example:

```
RTRV-VERSION:FUJITSU::CTAG;
```

Step 12
Accept the new software load before the validation timer expires.

TL1

```
CANC-VALTM:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- ACCEPT=**Y**, N

Example:

```
CANC-VALTM:FUJITSU::CTAG;
```

Note: *The operation may take up to 20 minutes to complete. The NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units go out at the completion of this step.*

Download Configuration File

Step 13
Copy the configuration file from the FTP server to the RAM disk of the NE.

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer to the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction) (Refer to Table 5 in Software Requirements.)

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to Table 7.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU:139.145.23.43,F7504022.CON,RDISK,F7504022.CON:CTAG:::
OVERWRITE=Y,FTUID=\"swduser\",FTPID=\"moonrock\", FTPATH=\"C:\GENERICS\\";
```

Step 14
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Step 15
Copy the configuration file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- CON (configuration file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,F7504022.CON,STBY,:CTAG::CON:
COMMENT=\"eth 01/17/2007\";
```

Step 16
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Step 17
Delete the configuration file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- As specified in previous step

Example:

```
DLT-FILE:FUJITSU:F7504022.CON:CTAG;
```

Repeat Download of Software File

Step 18

Copy the software load file from the FTP server to the RAM disk of the NE.

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer to the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction) (Refer to Table 5 in Software Requirements.)

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to Table 7.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU:139.145.23.43,F7504022.PGM,RDISK,F7504022.PGM:CTAG:::
OVERWRITE=Y,FTUID=\"swdluser\",FTPID=\"moonrock\", FTPATH=\"C:\GENERICS\\";
```

Note: *The operation may take up to 10 minutes to complete. Wait for the "100% FILE COMPLETE" message before continuing.*

Step 19

Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Step 20
Copy the software load from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- PGM (program file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,F7504022.PGM,STBY,:CTAG::PGM:
COMMENT=\"eth 01/17/2007\";
```

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow. The NOT READY LED goes out when the copy operation completes.*

Step 21
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Step 22
Delete the software load from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- As specified in previous step

Example:

```
DLT-FILE:FUJITSU:F7504022.PGM:CTAG;
```

Download Firmware File

Step 23
Copy the firmware file from the FTP server to the RAM disk of the NE.

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer to the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction) (Refer to Table 5 in Software Requirements.)

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to Table 7.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU:139.145.23.43,A7504022.PGM,RDISK,A7504022.PGM:CTAG:::
OVERWRITE=Y,FTUID=\"swduser\",FTPID=\"moonrock\", FTPATH=\"C:\GENERICS\\";
```

Note: *The operation may take up to 10 minutes to complete. Wait for the "100% FILE COMPLETE" message before continuing.*

Step 24
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- As specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Step 25
Copy the firmware file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- PGM (program file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,A7504022.PGM,STBY,:CTAG::PGM:
COMMENT=\"eth 01/17/2007\";
```

Note: *The operation may take up to 10 minutes to complete. Wait for the "100% TRANSFER COMPLETE" message before continuing.*

Step 26
Retrieve and verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- Same as SRCFILE specified in Step 23
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Activate the Software

Step 27
Activate the software and accept the firmware file in standby memory.

Note: *For a generic issue switch to take place, the four keywords GISSUE, ACTDAT, and ACTTM must be specified. The VALTM keyword is optional.*

Note: *Refer to Software Requirements, through Software File Names and GISSUE Values for the appropriate GISSUE value.*

TL1

```
INIT-SYS:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- Refer to Table 8 for keyword and domain input parameters.

Example:

```
INIT-SYS:FUJITSU::CTAG:::GISSUE=04-02-1,ACTDAT=00-00-00,
ACTTM=00-00-00,VALTM=00-45-00;
```

Step 28
The user is automatically logged off once activation starts.

Step 29
Wait approximately 10 minutes to allow the NE to reset and adjust to the new software and firmware file. When the FAIL/SVCE LED on the NEM Shelf Processor unit lights green, log on the NE. Refer to Step 4, if necessary.

Note: *During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 30
Retrieve and verify software version information.

TL1

```
RTRV-VERSION:TID:AID:CTAG;
```

AID:

- ACT, STBY, **ALL**

Example:

```
RTRV-VERSION:FUJITSU::CTAG;
```

Step 31
Accept the new software and firmware file before the validation timer expires.

Note: *The NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units go out approximately 5 minutes after the new software and firmware loads are accepted.*

TL1

```
CANC-VALTM:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- ACCEPT=**Y**, N

Example:

```
CANC-VALTM:FUJITSU::CTAG;
```

After the system software is activated and the latest firmware file (generic) is downloaded to the system, the system may generate some firmware version mismatch alarms (FVM) against individual plug-in units with incompatible firmware versions. However, Release 4.2 and later software is compatible with firmware used by the Release 4.1 system, so FVM alarms should not occur for the Release 4.1 to Release 4.2 upgrade. Refer to FVM (Alarmed Standing Condition), for information on clearing FVM alarms.

Caution: *Installing new firmware on a plug-in unit programs the programmable hardware on the plug-in unit and can impact traffic associated with the plug-in unit. Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command and should be scheduled at an appropriate time to avoid service interruption. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit. Refer to Maintenance, for more information.*

Step 32
Log off the NE.

TL1

```
CANC-USER:TID:UID:CTAG;
```

Example:
```
CANC-USER:FUJITSU:ROOT:CTAG;
```

This procedure is complete.

✔ This procedure is complete.

2.4 Upgrading System Software Using the NETSMART 500 Software Download Wizard

In this section:

Overview NETSMART 500 Software Download Wizard

The NETSMART 500 Software Download wizard assists you in upgrading system software for a FLASHWAVE 7500 NE. For assistance, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822).

Caution: *After the system software has upgraded and the latest firmware file (generic) containing the firmware loads for each plug-in unit has been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the TL1 command INIT-EQPT at an appropriate time by following local practices. For more details, refer to* Maintenance.

Caution: *In Release 5.1 of the FLASHWAVE 7500 system, support is discontinued for the 2.5G Flexponder plug-in unit (IFMA-AUxx) and all 4-channel OLCs except IFMA-SBxx plug-in units (Refer to the following table). Also, support is discontinued for redundant processors introduced in Release 4.2. Ensure that the system to be upgraded does not include the 2.5G Flexponder plug-in unit or any 4-channel OLCs, except IFMA-SB plug-in units, prior to upgrading system software to Release 5.1 and later.*

Table 9: 4-Channel OLCs Not Supported in Release 5.1 and later

Plug-In Unit
IFMA-8Txx, excluding IFMA-8TC1 and IFMA-8TC2
IFMA-GUxx, excluding IFMA-GUC1
IFMA-HGxx, excluding IFMA-HGC1
IFMA-HLxx, excluding IFMA-HLC1
IFMA-LExx, excluding IFMA-LEC1
IFMA-LLxx, excluding IFMA-LLC1
IFMA-SAxx

Note: *Upgrading a nonfirmware supporting software release to a firmware supporting software requires a two-stage process. Since a nonfirmware supporting system will not accept a firmware file download, the system must first be upgraded to a firmware supporting system without downloading the firmware file and configuration file. Then the system can be upgraded to a Release 4.2 system with the firmware file.*

Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 Software Download wizard.*

The Software Download wizard assists you in:

- Downloading the software and the firmware to the NE
- Activating or scheduling the activation of the new software
- Confirming or rejecting the new software after activation

The wizard determines the applicable tasks based on the software download state and makes available only the applicable tasks.

Note: *These tasks are not available if the NE is pending activation of a new software or database file.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a software download (SWDL) is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Prepare to Upgrade Using the Software Download Wizard

Use the procedure in Prepare to Upgrade Using TL1 to copy software files from the CD-ROM to the File Transfer Protocol (FTP) server and to collect information about the FTP server in preparation for performing the procedure in Upgrading System Software Using the NETSMART 500 Software Download Wizard.

2.4.1 Upgrade System Software from Server Using Software Download Wizard

Attention: *The following procedure is applicable for upgrading the software from Release 4.1 to Release 4.2 for a FLASHWAVE 7500 system.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters.*

To download and activate system software using the NETSMART 500 Software Download wizard, perform the following:

Log On

Step 1
Ensure that the NEM Shelf Processor and OSC plug-in units are inserted in the NE and that the NE is powered up.

Step 2
Ensure that the system does not include any 4-channel OLCs, except IFMA-SB plug-in units. Refer to Table 9.

Step 3
Log on the NE.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to False.*

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For more detailed information, refer to* Craft Interface Operations .

NETSMART 500

To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select *NE > Logon*.

Note: *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.*

The NE Logon dialog box opens.
Make the following selections:

For **TERM2** (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

NETSMART 500

Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 graphical user interface.*

Step 4
Retrieve alarms and conditions on the NE.

NETSMART 500

NE ▸ *Alarms*

View ▸ *Filter*

Verify that all Fault Types and Severity Levels are selected as reporting.
Click Close.
Close Active Alarms window.

Step 5
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Download Software

Step 6
From the menu bar, select *Wizards* > *Software Download*.

Note: *When progressing through the screens in the Software Download wizard, the current screen may momentarily be gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

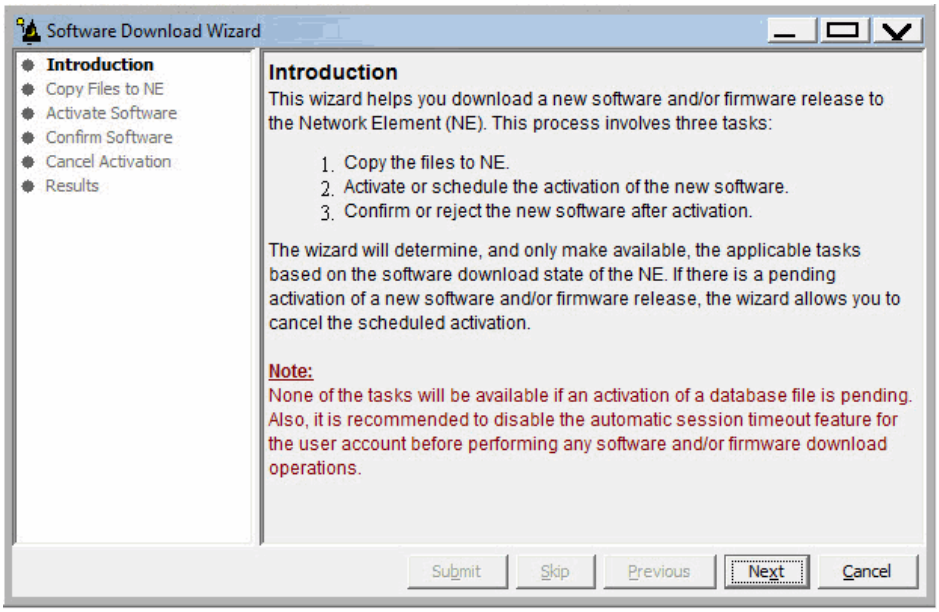


Figure 23: Example Software Download Wizard Introduction Screen

Step 7
Click *Next*.

The *Copy Files to NE* screen opens.

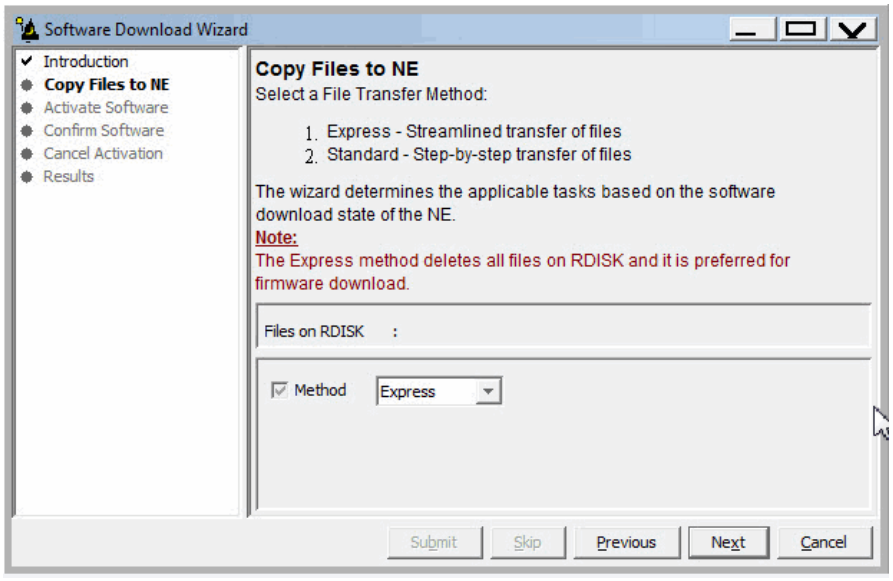


Figure 24: Example Software Download Wizard Copy Files to NE Screen

Step 8
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *This procedure documents the Express method only. Fujitsu recommends this method for software download because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 9
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

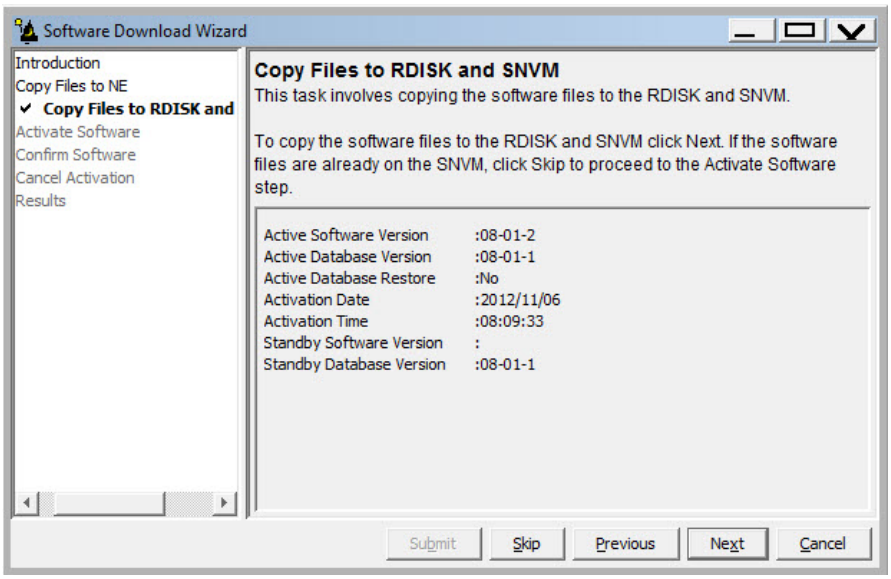


Figure 25: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 10
Verify the *Active Software Version* is *04-01-3* for the upgrade and then click *Next*.

Note: *The current software must be Release 4.1 (software version 04-01-3) in order to upgrade to Release 4.2.*

The *Select Host* screen appears.

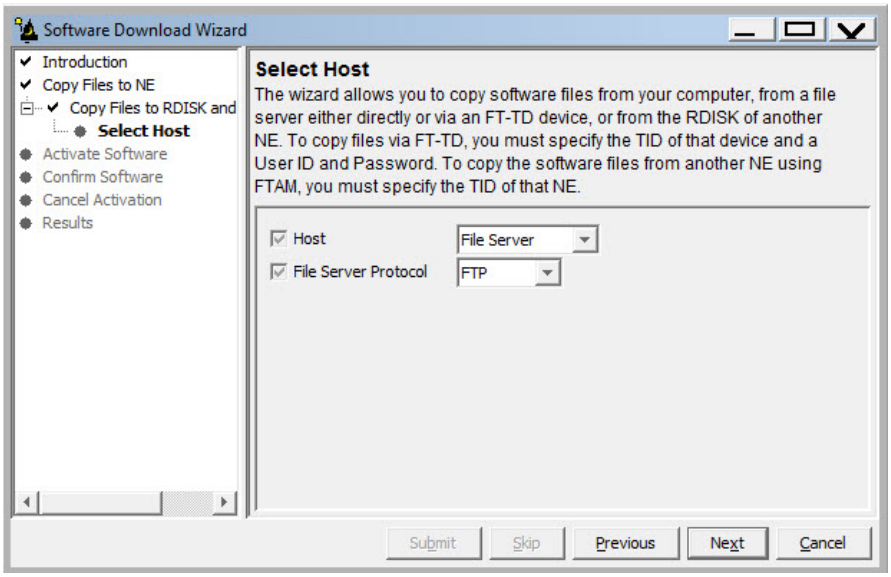


Figure 26: Example Software Download Wizard Select Host Screen

Step 11
Verify File Server is selected in the *Host* drop-down list.

Refer to Upgrade System Software from Another NE Using Software Download Wizard to download software from another NE.

Step 12
Click *Next*.

The *Select FTP Server* screen opens.

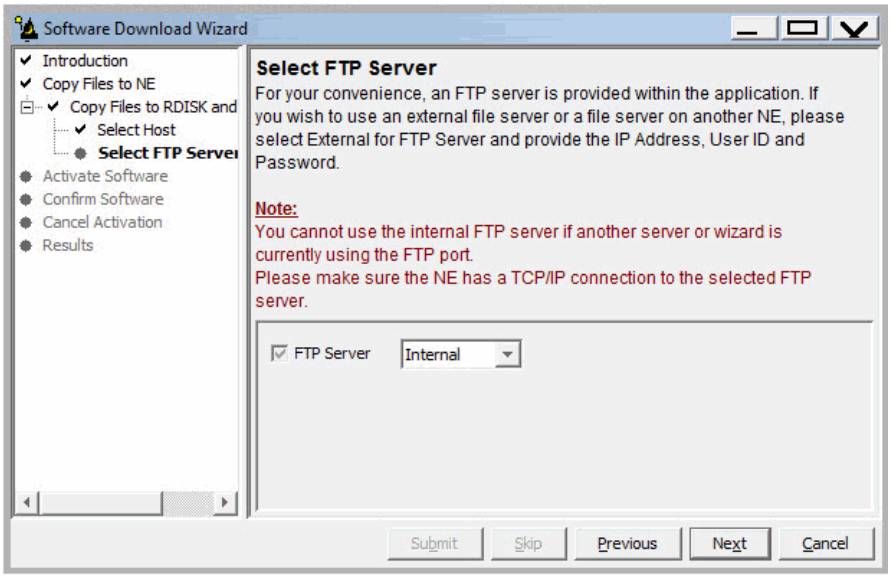


Figure 27: Example Software Download Wizard Select FTP Server Screen

Step 13
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 14
From the *FTP Server* drop-down list, select *Internal* and go to Step 16.

Step 15
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

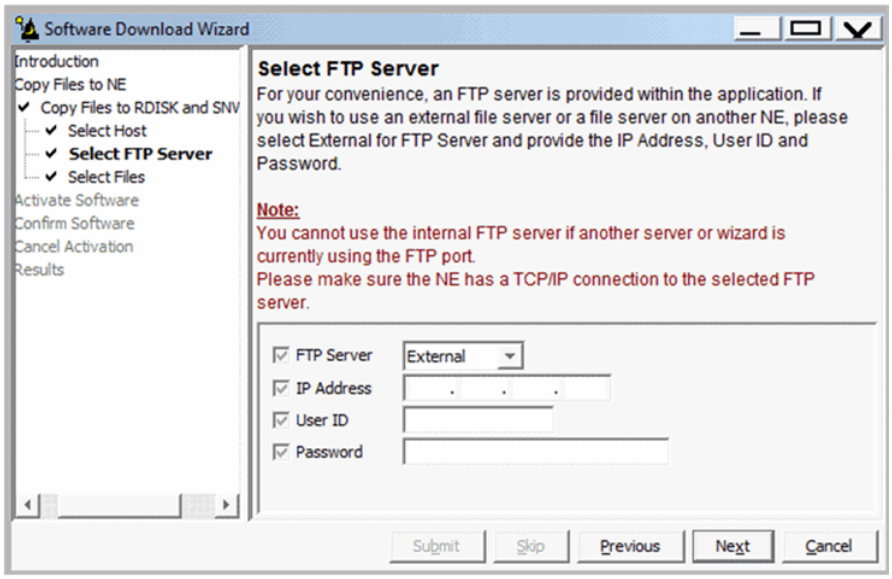


Figure 28: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 16
Click *Next*.

The *Select Files* screen opens.

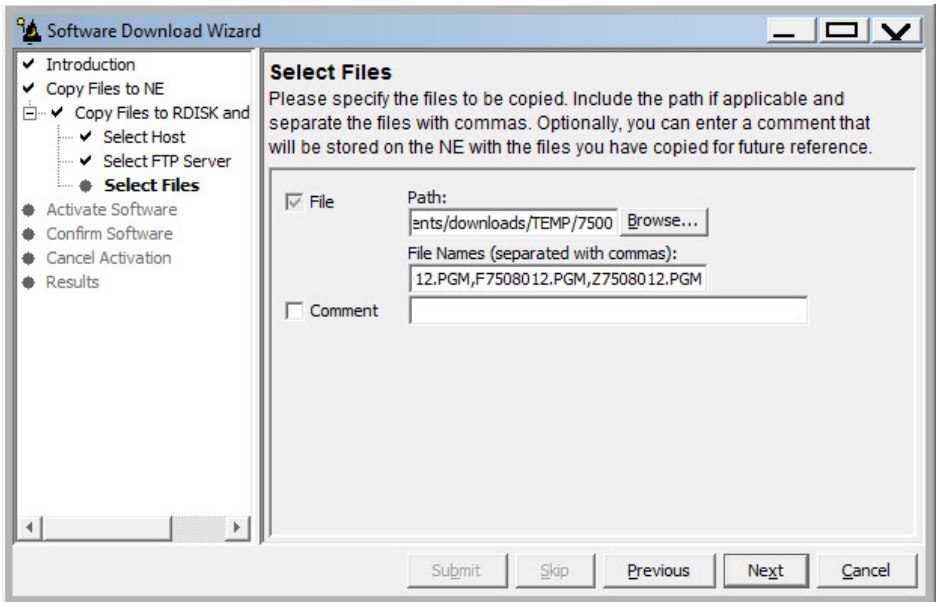


Figure 29: Example Software Download Wizard Select Files Screen

Step 17
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 18
In the *File* text box, enter the appropriate file name of the software file: F7504022.PGM

Step 19
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 20
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 15 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

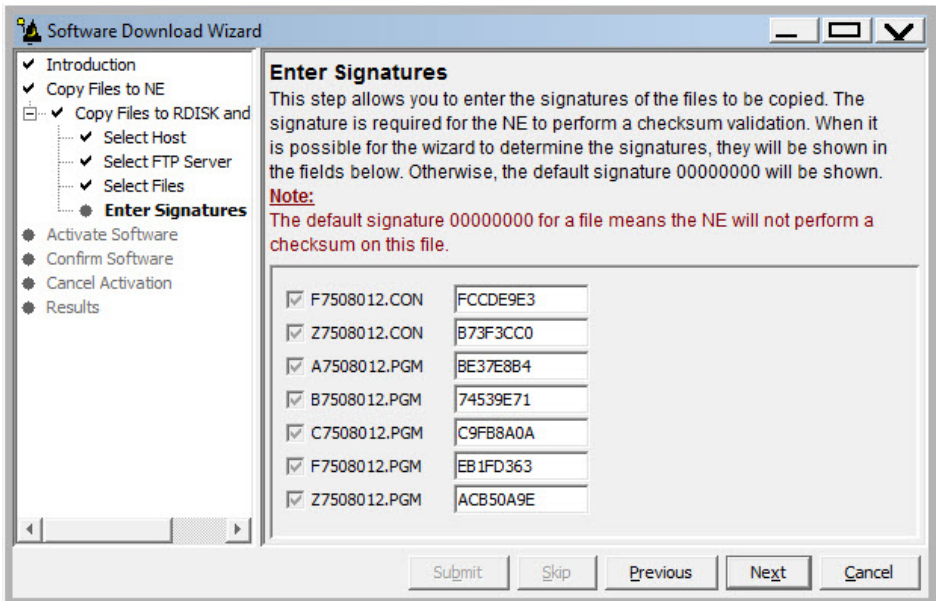


Figure 30: Example Software Download Wizard Enter Signatures Screen

Step 21
Click *Next*.

The *Copy to RDISK and SNVM* screen opens.

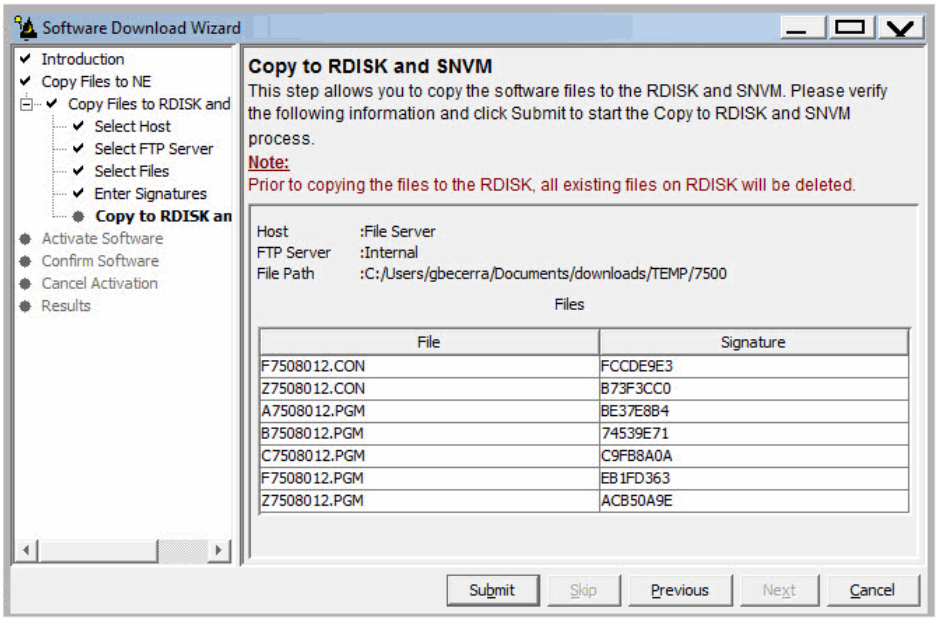


Figure 31: Example Software Download Wizard Copy to RDISK and SNVM Screen

Step 22
Click *Submit*.

A *Performing Copy File* dialog box opens, showing the progress in copying each file.

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

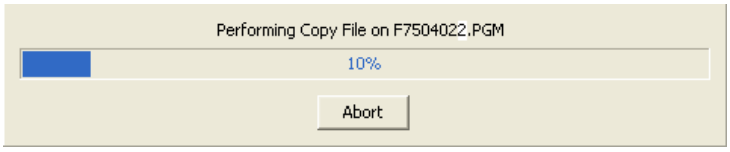


Figure 32: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

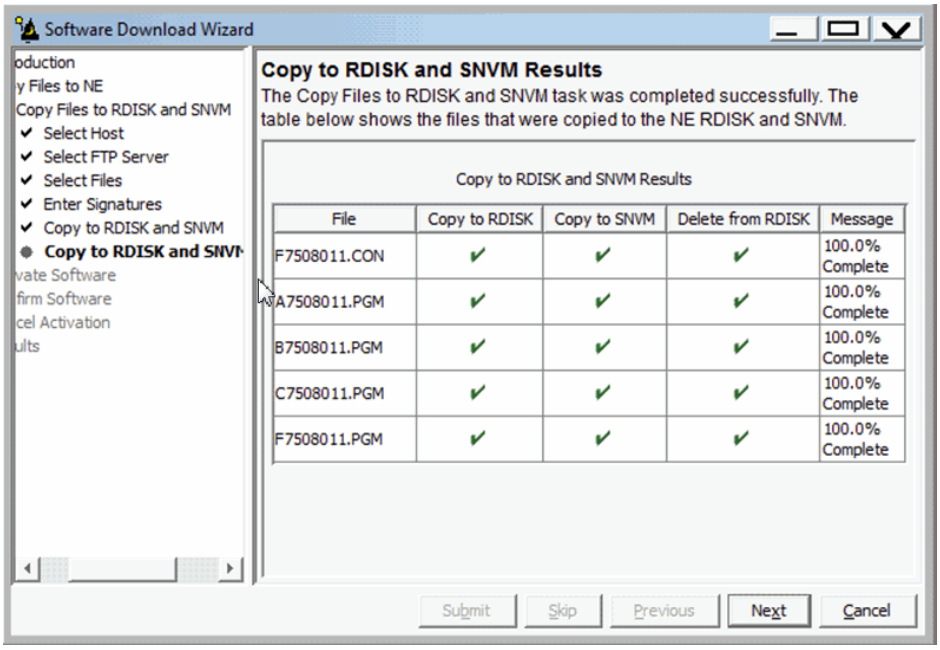


Figure 33: Example Software Download Wizard Copy to RDISK Results Screen

Activate Software

Step 23
Click *Next*.

The *Activate Software* screen opens.

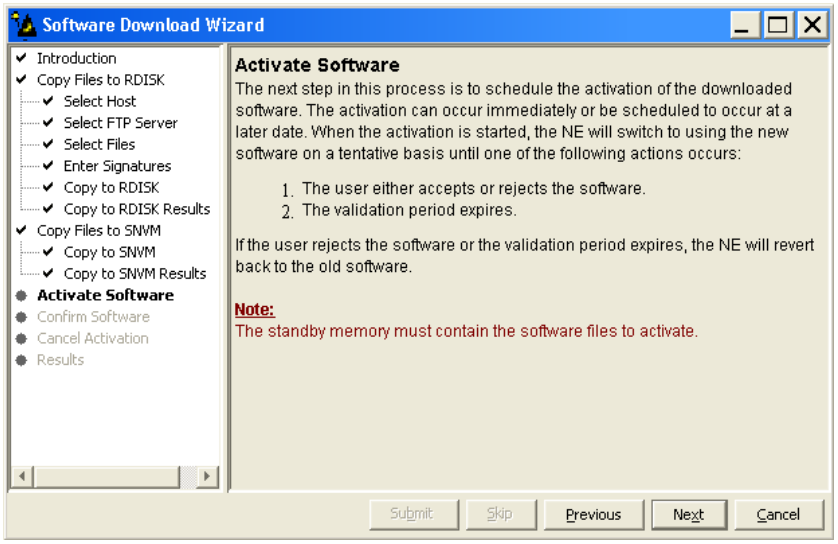


Figure 34: Example Software Download Wizard Activate Software Screen

Step 24
Click *Next*.

The *Software Activation Parameters* screen opens.

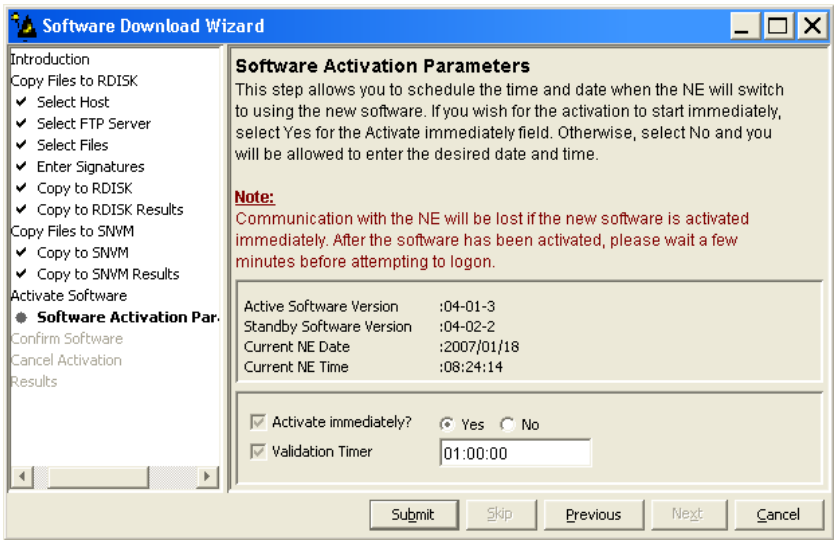


Figure 35: Example Software Download Wizard Software Activation Parameters Screen

Step 25
Verify *Yes* is selected for the *Activate immediately* option.

Note: *The Release 4.2 system software must be activated before the firmware can be upgraded.*

Step 26
In the *Validation Timer* text box, enter the desired time before the system reverts back to the previous software (the default is 01:00:00 [1 hour]).

Step 27
Click *Submit*.

The *Software Activation Result* screen opens.

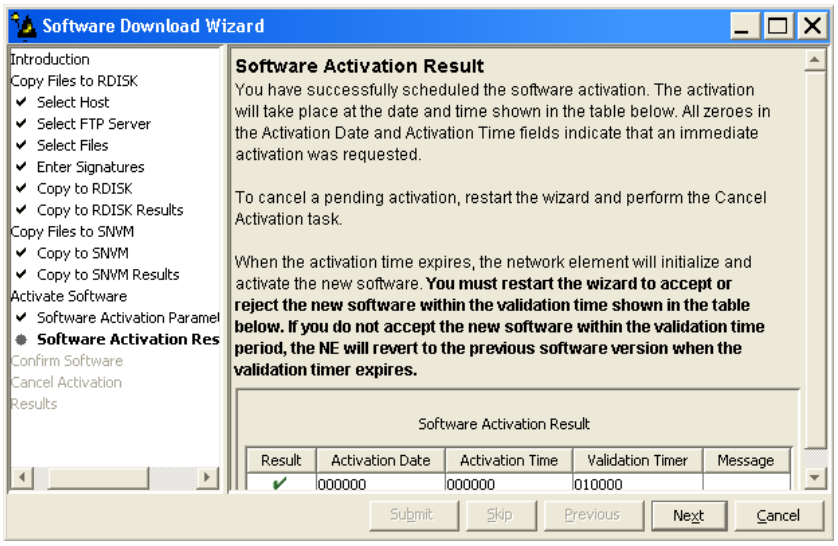


Figure 36: Example Software Download Wizard Software Activation Result Screen

Step 28
Click *Next*.

A *Warning* dialog box opens.

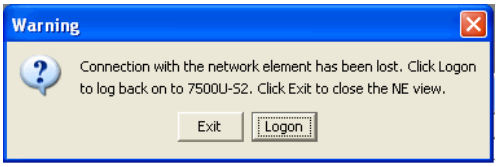


Figure 37: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 29
Click *Logon*.

The *Software Activation Result* screen closes, and the Software Download wizard closes.

Note: *A no firmware (NOFW) alarm is raised on the NE because the firmware supporting software is expecting to see firmware. This condition will clear once the firmware is loaded.*

Confirm Software Download

Note: *You must accept the new software load before the validation timer set in* Step 26 *expires. Otherwise, the system software will revert back to the previous load.*

Step 30
Log back on the NE. Refer to Step 3, if necessary.

Step 31
From the menu bar, select *Wizards* > *Software Download*.

The Software Download wizard starts, and the *Introduction* screen opens.

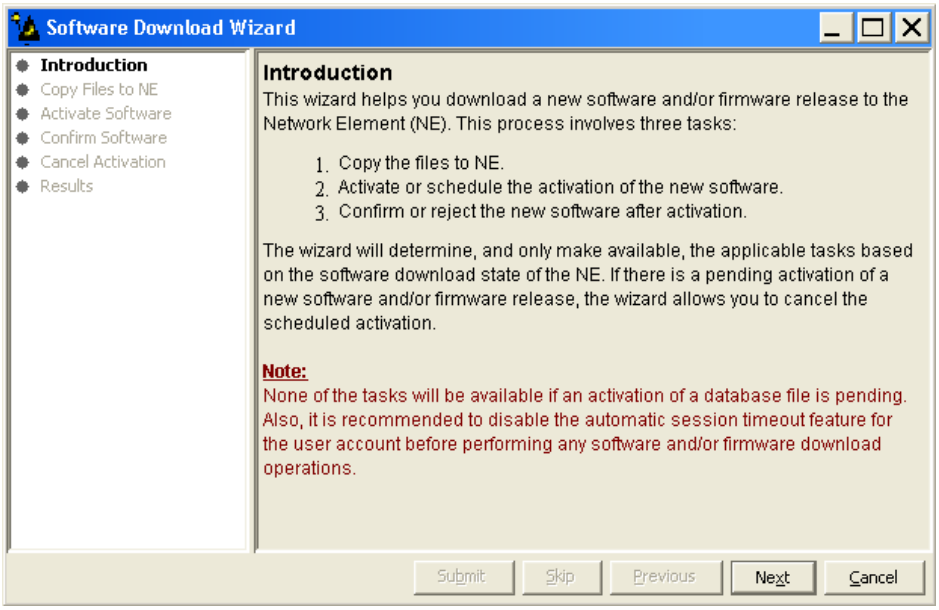


Figure 38: Example Software Download Wizard Introduction Screen

Step 32
Click *Next*.

The *Confirm Software* screen opens.

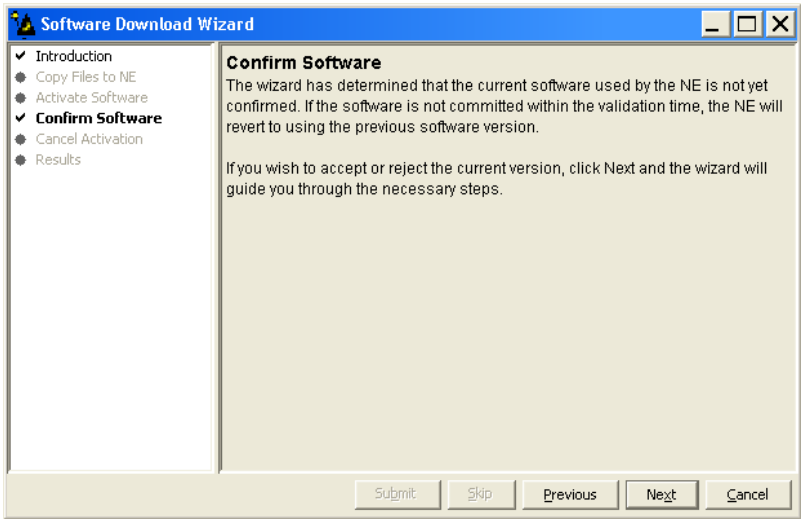


Figure 39: Example Software Download Wizard Confirm Software Screen

Step 33
Click *Next*.

The *Accept/Reject Software* screen opens.

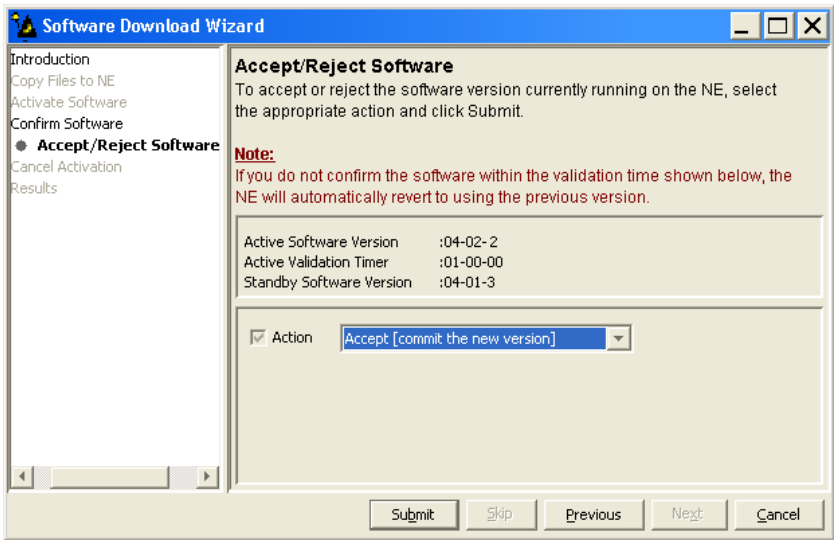


Figure 40: Example Software Download Wizard Accept/Reject Software Screen

Step 34
Verify that the *Accept [commit the new version]* option is selected in the *Action* drop-down list.

Step 35
Click *Submit*.

A progress bar displays while the validation timer is cancelled and the software is accepted.

Once the software is accepted, the *Software Confirmation Result* screen opens.

Note: *The screen may take up to 20 minutes to open.*

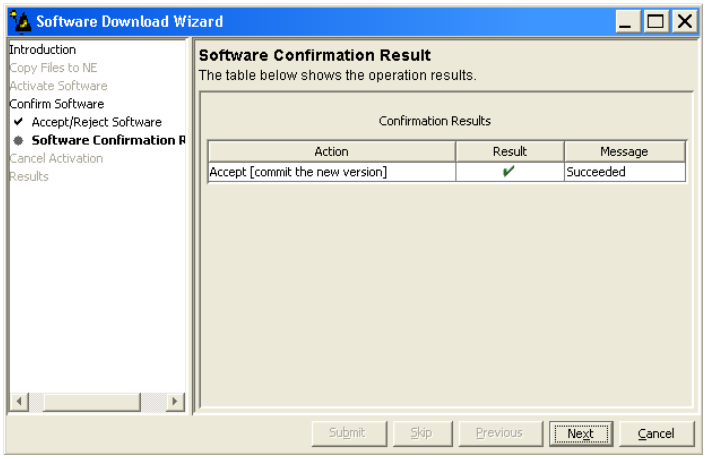


Figure 41: Example Software Download Wizard Software Confirmation Result Screen

Step 36
Click *Next*.

The final *Results* screen opens.

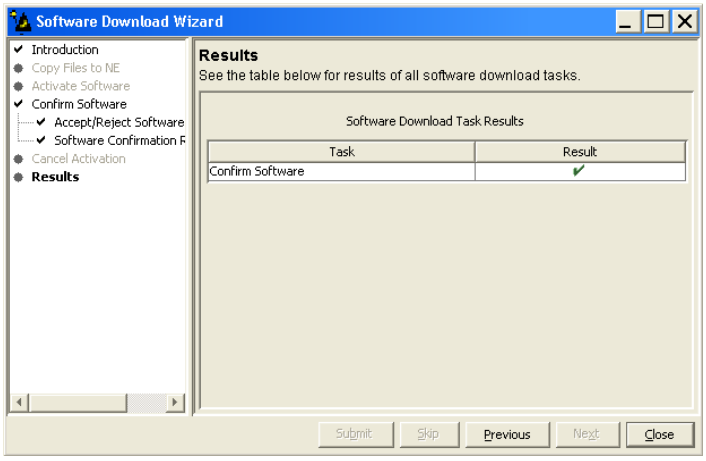


Figure 42: Example Software Download Wizard Results Screen

Step 37
Click *Close*.

The *Results* screen closes and the Software Download wizard closes.

Step 38
Retrieve alarms and conditions on the NE.

NETSMART 500

NE ▸ *Alarms*

View ▸ *Filter*

Verify that all Fault Types and Severity Levels are selected as reporting.
Click Close.
Close Active Alarms window.

Step 39
Are any active alarms or conditions being reported on the NE, other than the NOFW alarm?

If YES:
Clear all active alarms and conditions (excluding the NOFW alarm). After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *The NOFW alarm will clear once firmware is loaded in stage two of this procedure.*

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Download Firmware and Software

Step 40
From the menu bar, select *Wizards* > *Software Download*.

Note: *When progressing through the screens in the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and *Introduction* screen opens.

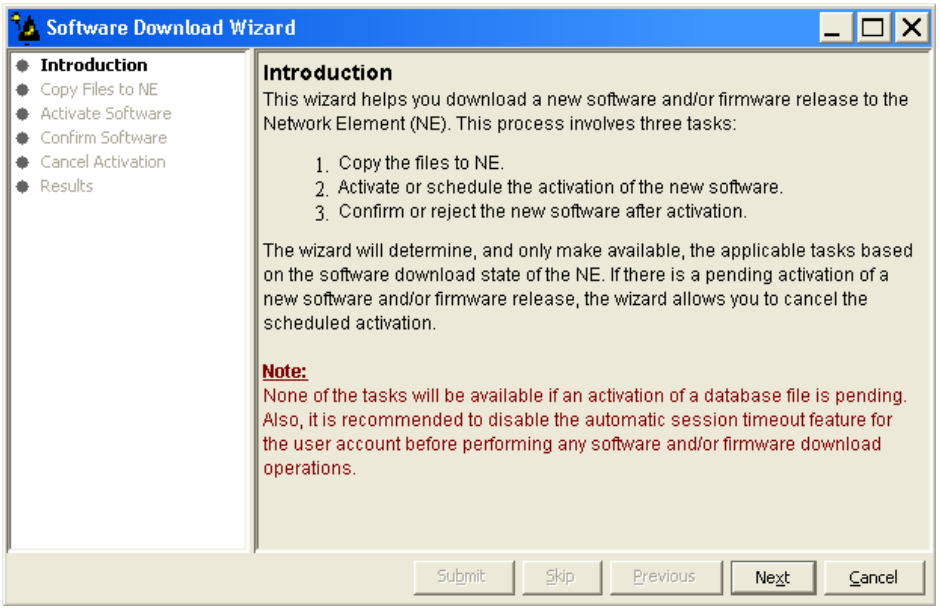


Figure 43: Example Software Download Wizard Introduction Screen

Step 41
Click *Next*.

The *Copy Files to NE* screen opens.

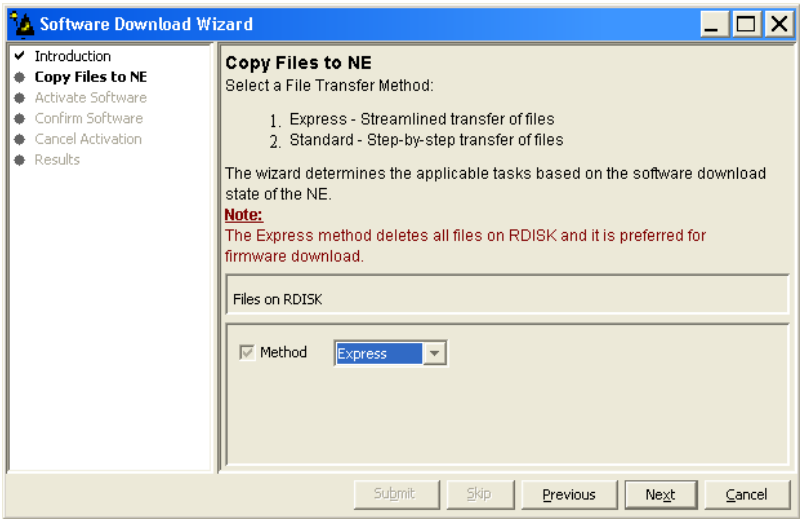


Figure 44: Example Software Download Wizard Copy Files to NE Screen

Step 42
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *This procedure documents the Express method only. Fujitsu recommends this method for software download because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 43
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

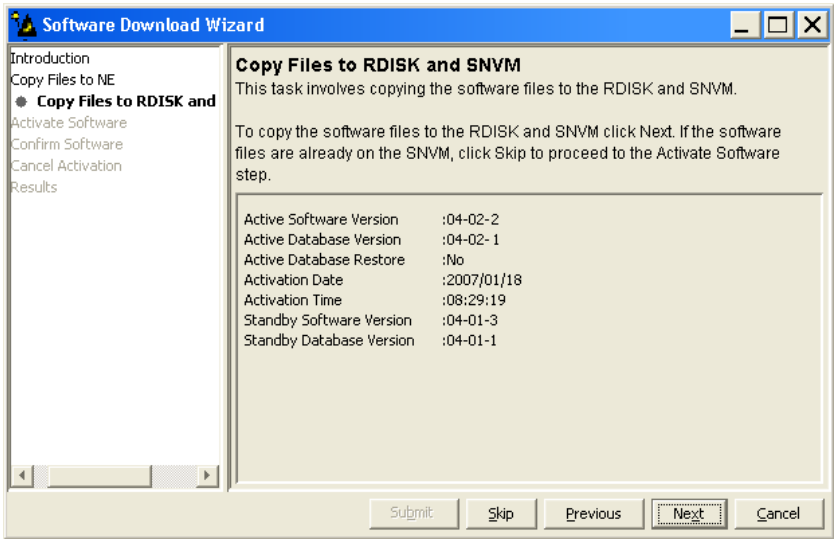


Figure 45: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 44
Click *Next*.

The *Select Host* screen opens.

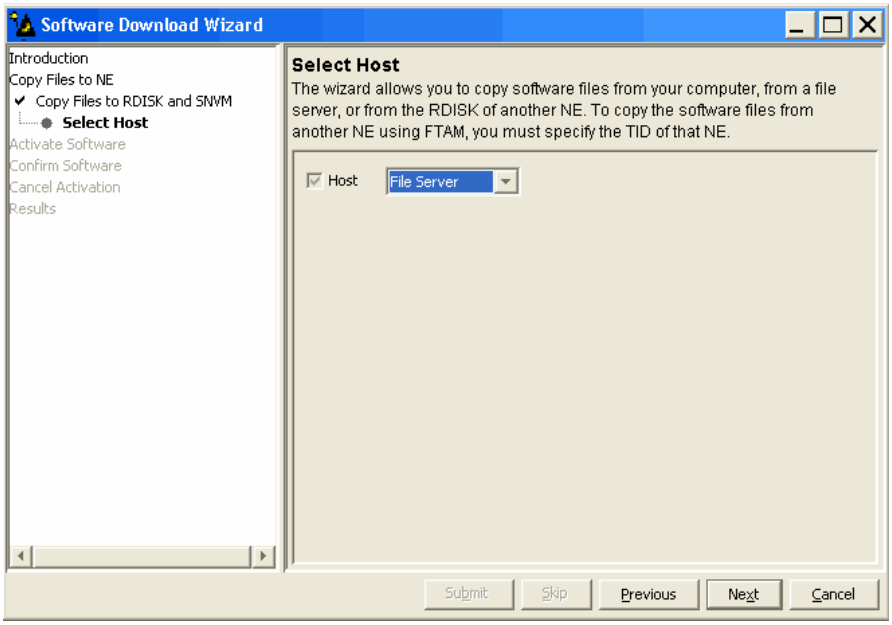


Figure 46: Example Software Download Wizard Select Host Screen

Step 45
Verify File Server is selected in the *Host* drop-down list.

Refer to Upgrade System Software from Another NE Using Software Download Wizard to download software from another NE.

Step 46
Click *Next*.

The *Select FTP Server* screen opens.

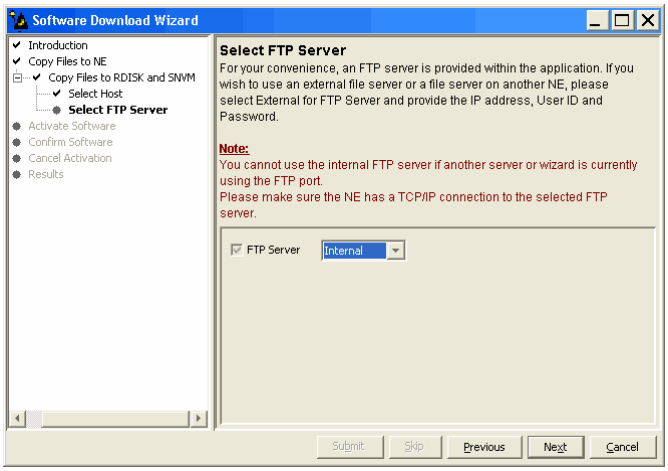


Figure 47: Example Software Download Wizard Select FTP Server Screen

Step 47
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 48
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 49
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

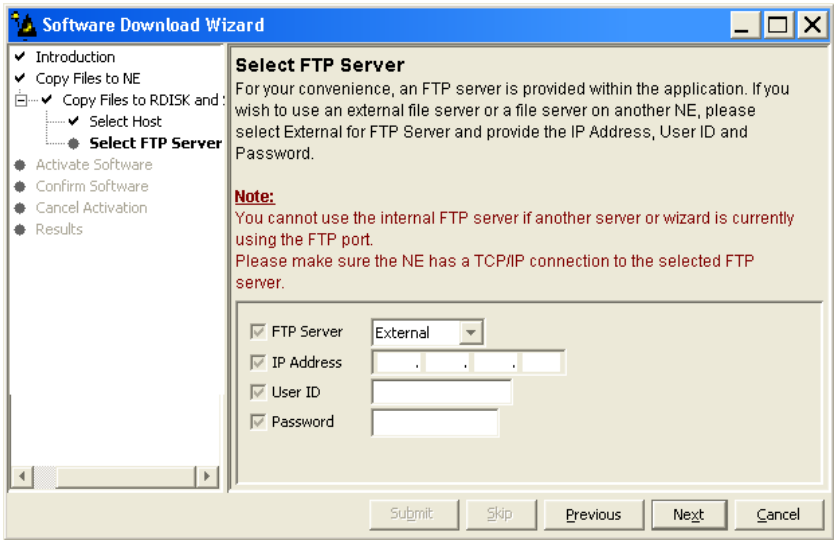


Figure 48: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 50
Click *Next*.

The *Select Files* screen opens.

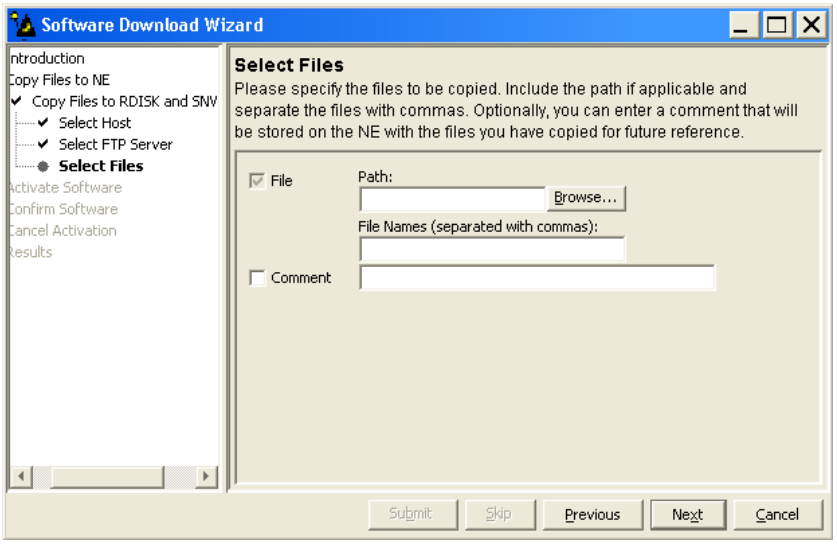


Figure 49: Example Software Download Wizard Select Files Screen

Step 51
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 52
In the *File: File Names (separated with commas)* text box, enter the appropriate file names:

- *F7504022.CON*
- *F7504022.PGM*
- *A7504022.PGM*

Step 53
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 54
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 48 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can manually enter the signatures or leave the zeros to bypass the checksum.*

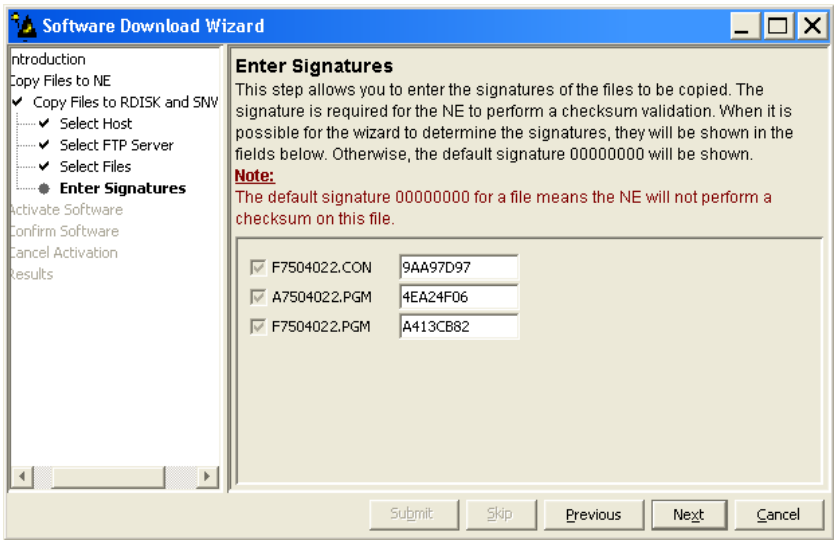


Figure 50: Example Software Download Wizard Enter Signatures Screen

Step 55
Click *Next*.

The *Copy to RDISK and SNVM* screen opens.

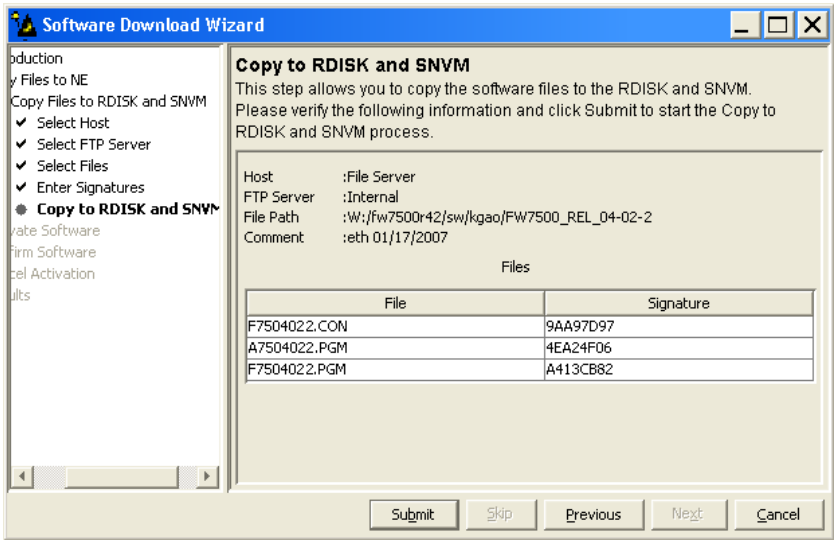


Figure 51: Example Software Download Wizard Copy to RDISK and SNVM Screen

Step 56
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying for each file.

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

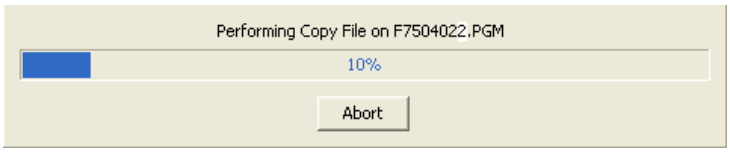


Figure 52: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen opens.

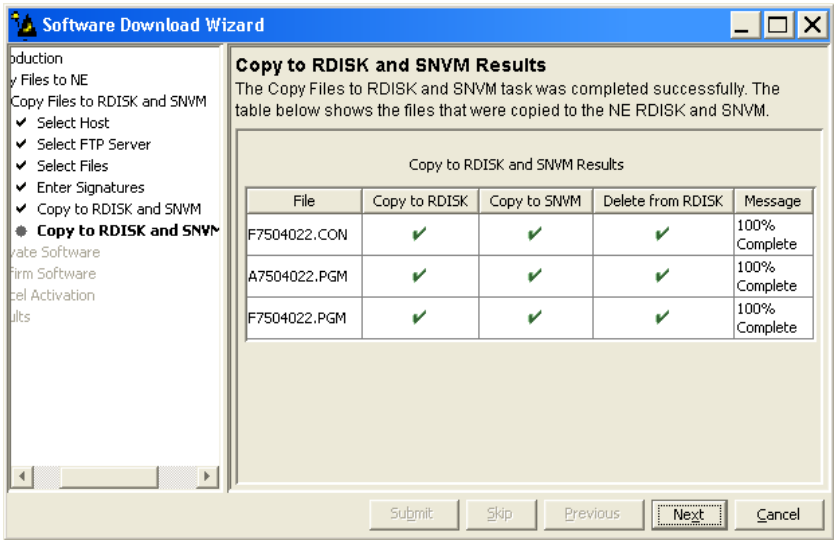


Figure 53: Example Software Download Wizard Copy to RDISK and SNVM Results Screen

Activate Software

Step 57
Click *Next*.

The *Activate Software* screen opens.

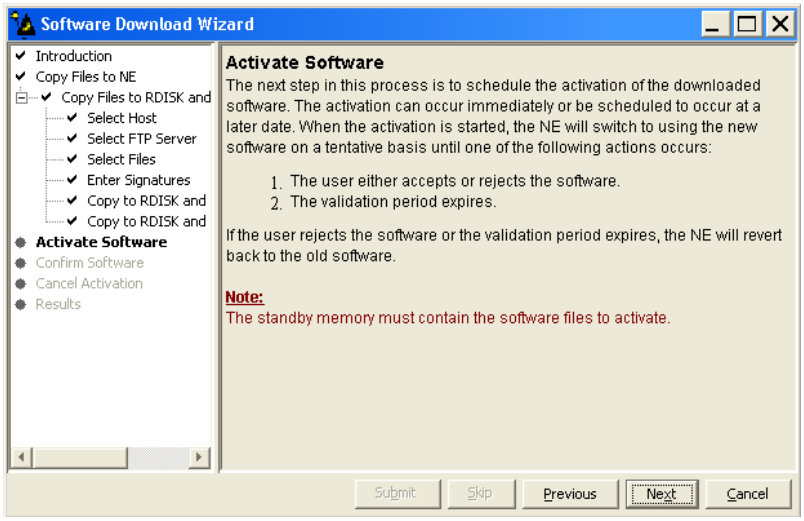


Figure 54: Example Software Download Wizard Activate Software Screen

Step 58
Click *Next*.

The *Software Activation Parameters* screen opens.

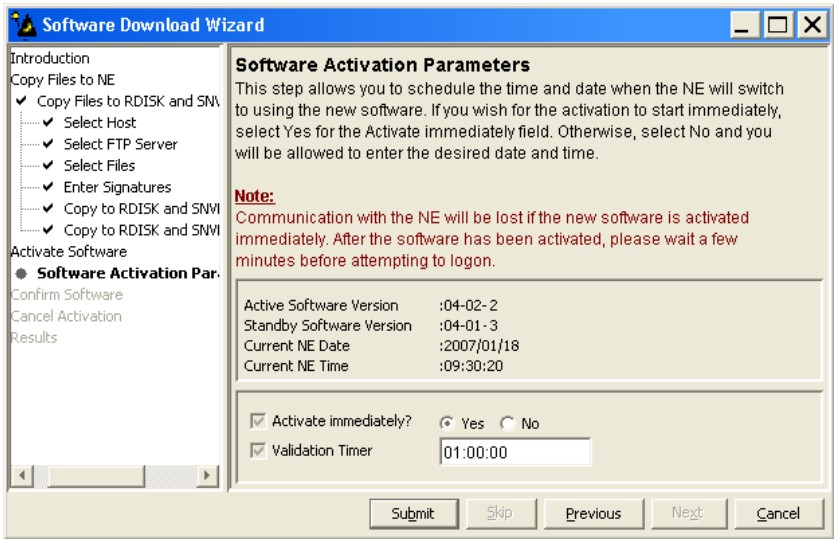


Figure 55: Example Software Download Wizard Software Activation Parameters Screen

Step 59
Do you want to activate the firmware and software immediately?

If YES:
Continue with the next step.

If NO:
Go to Step 66.

Step 60
Verify *Yes* is selected for the *Activate immediately* option.

Step 61
In the *Validation Timer* text box, enter the desired time before the system reverts back to the previous software (the default is 01:00:00 [1 hour]).

Step 62
Click *Submit*.

The *Software Activation Result* screen opens.

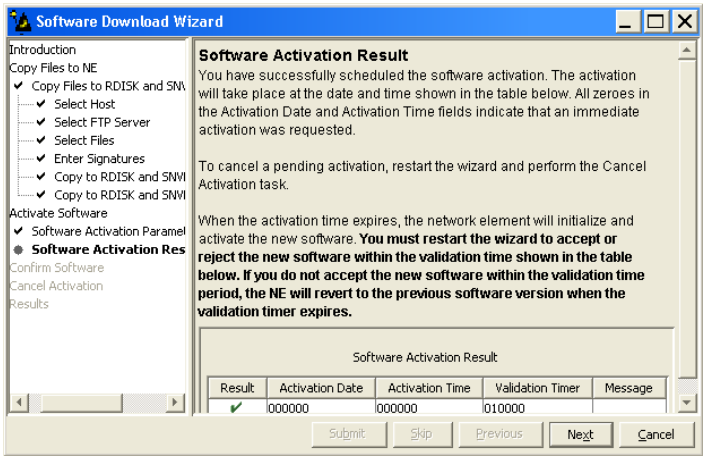


Figure 56: Example Software Download Wizard Software Activation Result Screen

Step 63
Click *Next*.

A *Warning* dialog box opens.

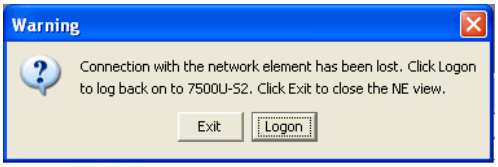


Figure 57: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 64
Click *Logon*.

The *Software Activation Result* screen closes, and the Software Download wizard closes.

Step 65
Go to Step 71.

Step 66
Select *No* for the *Activate immediately* option.

The *Software Activation Parameters* screen displays additional fields.

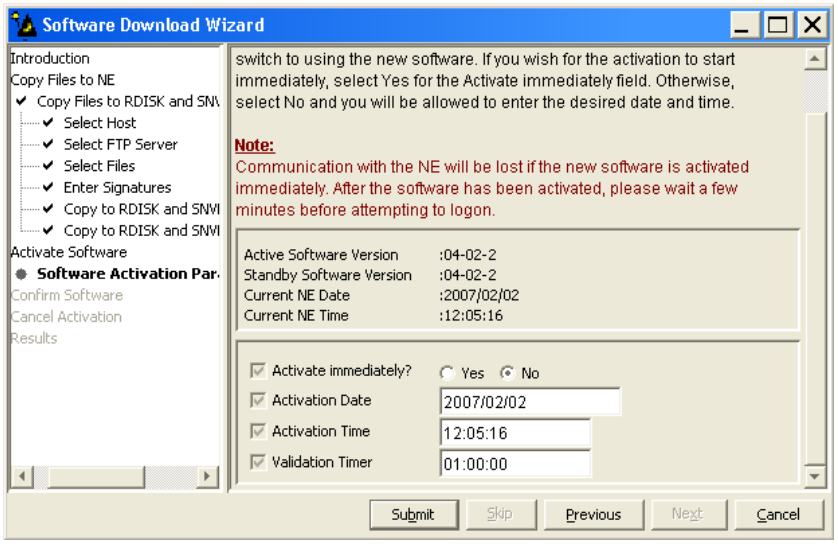


Figure 58: Example Software Activation Parameters–Scheduled Activation

a) Enter the *Activation Date* for the firmware and software activation.

b) Enter the *Activation Time* for the firmware and software activation.

c) Enter the *Validation Time* for the firmware and software activation.

Step 67
Click *Submit*.

The *Software Activation Result* screen opens.

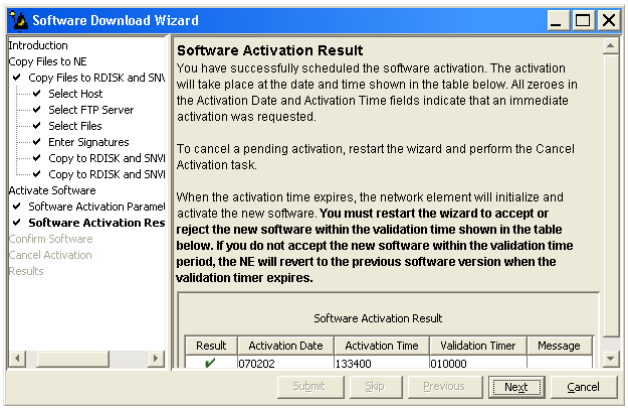


Figure 59: Example Software Download Wizard Software Activation Result Screen

Step 68
Click *Next*.

The *Results* screen opens.

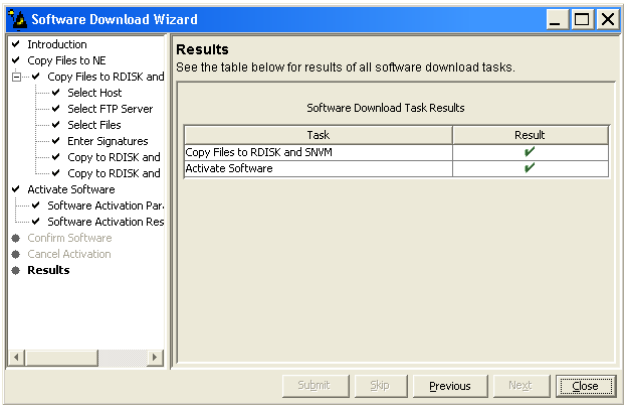


Figure 60: Example Software Download Wizard Results Screen

Step 69
Click *Close*.

The Software Download wizard closes. You may continue working in the NETSMART 500 environment and stay logged on to the NE. When the activation date and time is reached, you are logged off the NE and a *Warning* dialog box appears.

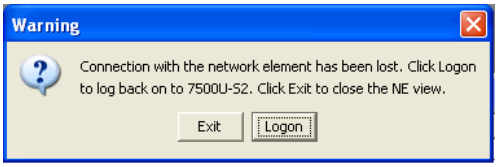


Figure 61: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 70
Click *Logon*.

The NETSMART 500 window closes.

Confirm Software Download

Note: *You must accept the new software load before the validation timer set in Step 61 expires. Otherwise, the system software will revert back to the previous load.*

Step 71
Log back on the NE. Refer to Step 3, if necessary.

Step 72
From the menu bar, select *Wizards* > *Software Download*.

The Software Download wizard starts, and the *Introduction* screen opens.

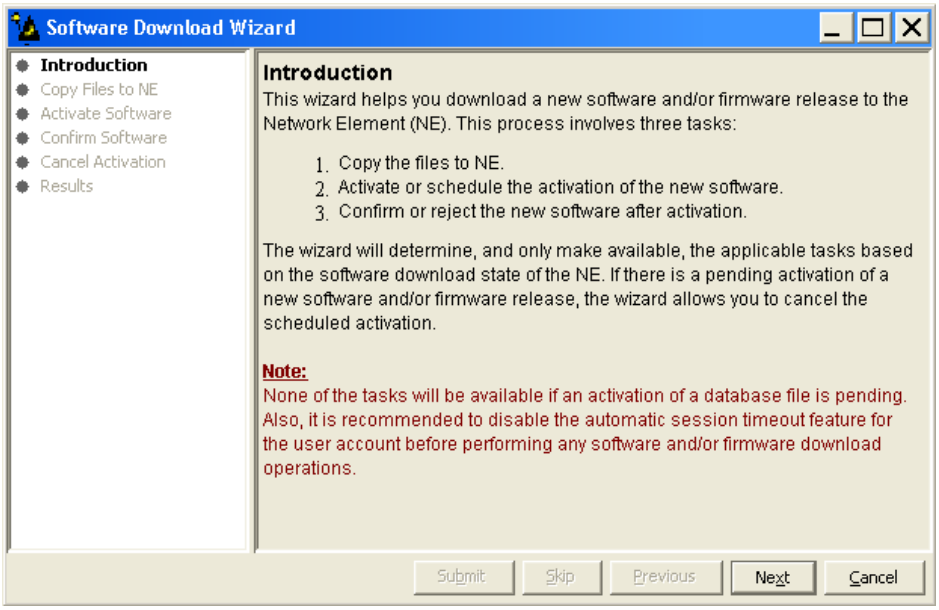


Figure 62: Example Software Download Wizard Introduction Screen

Step 73
Click *Next*.

The *Confirm Software* screen opens.

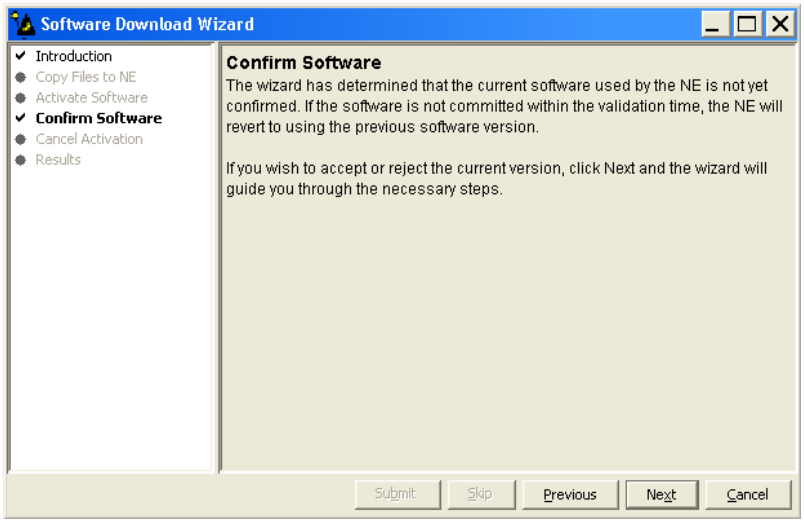


Figure 63: Example Software Download Wizard Confirm Software Screen

Step 74
Click *Next*.

The *Accept/Reject Software* screen opens.

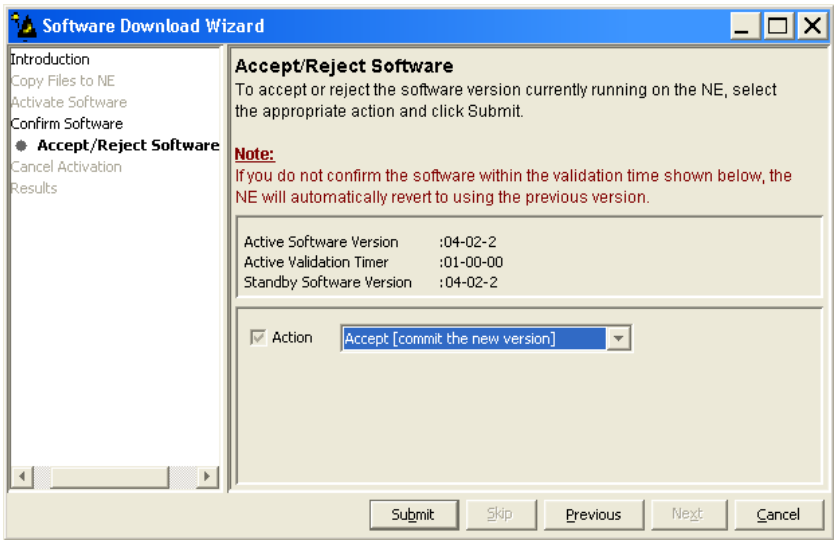


Figure 64: Example Software Download Wizard Accept/Reject Software Screen

Step 75
Verify that the *Accept [commit the new version]* option is selected in the *Action* drop-down list.

Step 76
Click *Submit*.

A progress bar displays while the validation timer is cancelled and the software is accepted.

Once the software is accepted, the *Software Confirmation Result* screen opens.

Note: *The screen may take several minutes to open.*

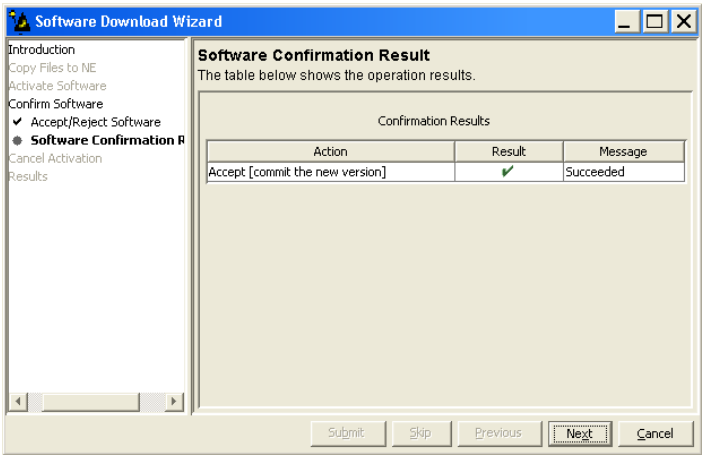


Figure 65: Example Software Download Wizard Software Confirmation Result Screen

Step 77
Click *Next*.

The final *Results* screen opens.

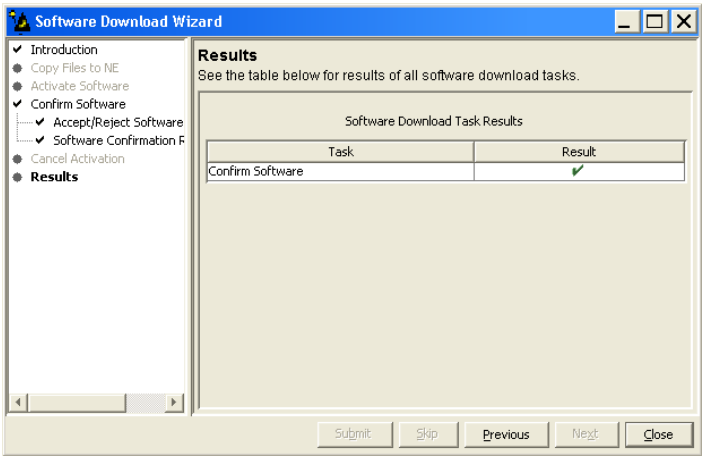


Figure 66: Example Software Download Wizard Results Screen

Step 78
Click *Close*.

The *Results* screen closes and the Software Download wizard closes.

After the system software is activated, and the latest firmware file (generic) is downloaded to the system, the NOFW condition clears. The system then may generate some firmware version mismatch alarms (FVM) against units with incompatible firmware versions.

Step 79
Retrieve alarms and conditions on the NE.

NETSMART 500

NE ▸ *Alarms*

View ▸ *Filter*

Verify that all Fault Types and Severity Levels are selected as reporting.
Click Close.
Close Active Alarms window.

Step 80
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment, for information on clearing FVM alarms). After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

Caution: *Installing new firmware on a plug-in unit programs the programmable hardware on the plug-in unit and can impact traffic associated with the plug-in unit. Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command and should be scheduled at an appropriate time to avoid service interruption. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

If NO:
Proceed to the next step.

Step 81
Log off the NE.

This procedure is complete.

✔ This procedure is complete.

2.4.2 Upgrade System Software from Another NE Using Software Download Wizard

Caution: *After the system software has upgraded and the latest firmware file (generic) containing the firmware loads for each plug-in unit has been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the procedure in* Upgrading Firmware on Equipment*, at an appropriate time by following local practices.*

Note: *Upgrading a nonfirmware supporting software release to a firmware supporting software release requires a two-stage process. Since a nonfirmware supporting system will not accept a firmware file download, the system must first be upgraded to a firmware supporting system without downloading the firmware file and configuration file. Then the system can be upgraded to a Release 4.2 system with the firmware file.*

Attention: *The figures in this procedure shows a software upgrade of a system from Release 4.1 to Release 4.2, where the gateway NE is loaded with Release 4.2 software. If you are upgrading a system from Release 4.1 to Release 4.2, and you are using a Release 4.1 NE as the Local NE, some of the steps and figures in the following procedure will be different. You can upgrade the Local NE before beginning this procedure by following the procedure in* Upgrade System Software from Server Using Software Download Wizard.

Attention: *The following procedure is applicable for upgrading the software from Release 4.1 to Release 4.2 for a FLASHWAVE 7500 system.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters.*

Perform the following procedure to download and activate system software to a remote NE from a local NE using the NETSMART 500 Software Download wizard:

Log On Local and Remote NEs

Step 1
Ensure that the NEM Shelf Processor and OSC plug-in units are inserted in the NEs and the NEs are powered up.

Step 2
Ensure that the systems do not include any 4-channel OLCs, except IFMA-SB plug-in units. Refer to Table 9.

Step 3
Log on both NEs.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to No.*

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values. The TID, UID, and PID values are not case-sensitive.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For more detailed information, refer to* Craft Interface Operations .

NETSMART 500

To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select *NE > Logon*.

Note: *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.*

The NE Logon dialog box opens.
Make the following selections:

For **TERM1** (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial

Comm. Port: COMx (for example, COM2)

Configure: use default[14]

For **TERM2** (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 graphical user interface.*

Step 4
Retrieve alarms and conditions on the Local and Remote NEs.

[14] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

NETSMART 500

NE ▸ *Alarms*

View ▸ *Filter*

Verify that all Fault Types and Severity Levels are selected as reporting.
Click Close.
Close Active Alarms window.

Step 5
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Step 6
Delete all files from the RAM disk (RDISK) of the Local NE and Remote NE.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select DLT-FILE command from the *Command Name* drop-down list.
Enter *ALL* in the *AID* field.
Click *Send*.

Do not close the TL1 Command Builder dialog box.

Step 7
Verify the RDISK on the Local NE and Remote NE is empty.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.

Enter the program file name or ALL in the AID field.
Click *Send*.

Close the TL1 Command Builder dialog box.

Start the Software Download Wizard at Local NE

Step 8
Switch to the local NE.

Step 9
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this screen, and each subsequent screen.*

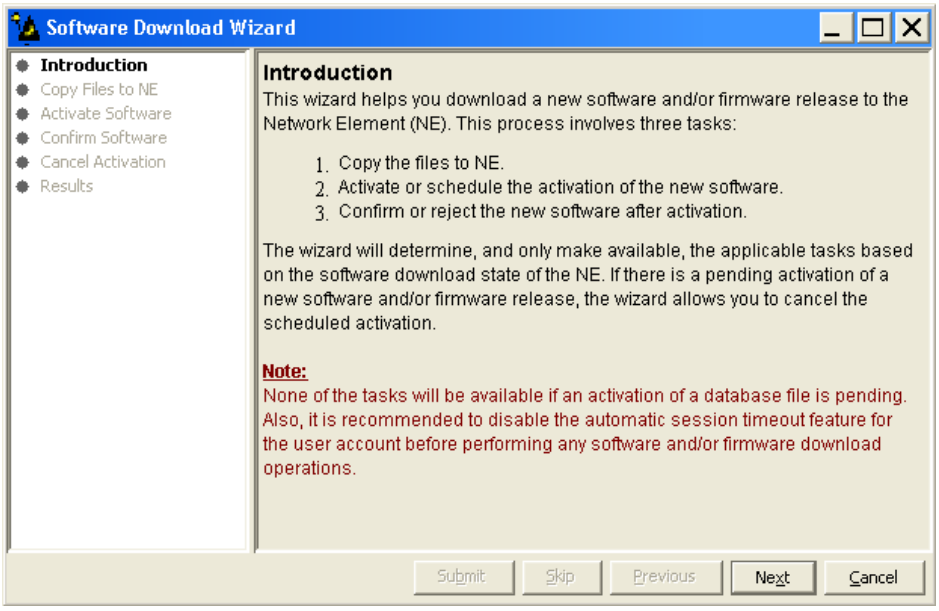


Figure 67: Example Software Download Wizard Introduction Screen

Step 10
Click *Next*.

The *Copy Files to NE* screen appears.

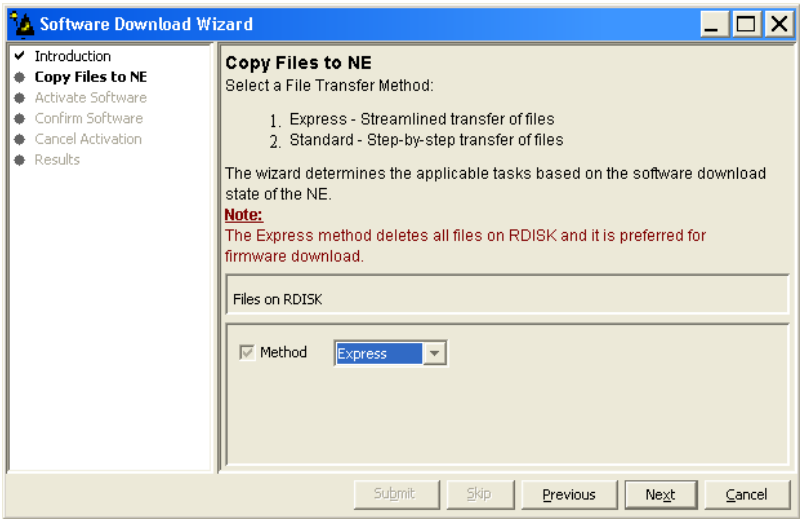


Figure 68: Example Software Download Wizard Copy Files to NE Screen

Step 11
Select *Standard* from the *Method* drop-down list.

Note: *Do not use the Express method at the Local NE. The Express method copies the software files to the RDISK, then to the SNVM, then deletes the software files from the RDISK. This procedure requires that the software files are only copied to the RDISK of the Local NE.*

Step 12
Click *Next*.

The *Copy Files to RDISK* screen opens.

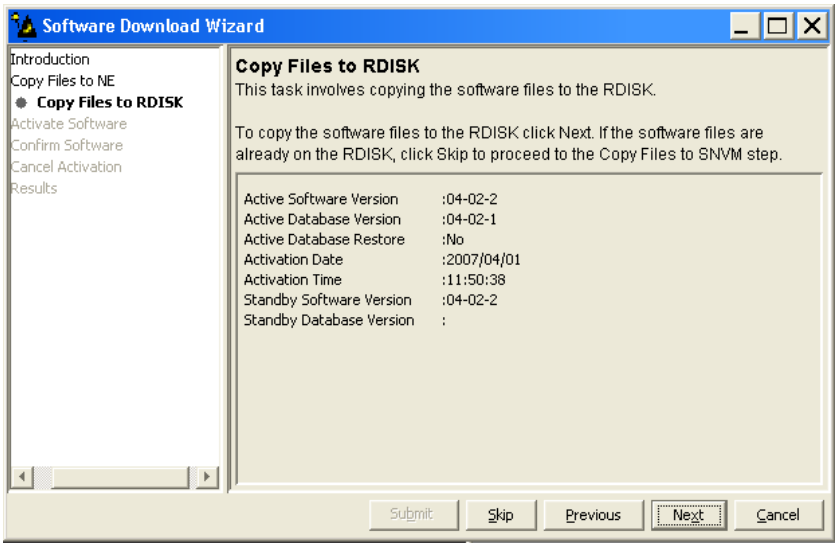


Figure 69: Example Copy Files to RDISK Screen

Step 13
Click *Next*.

The *Select Host* screen opens.

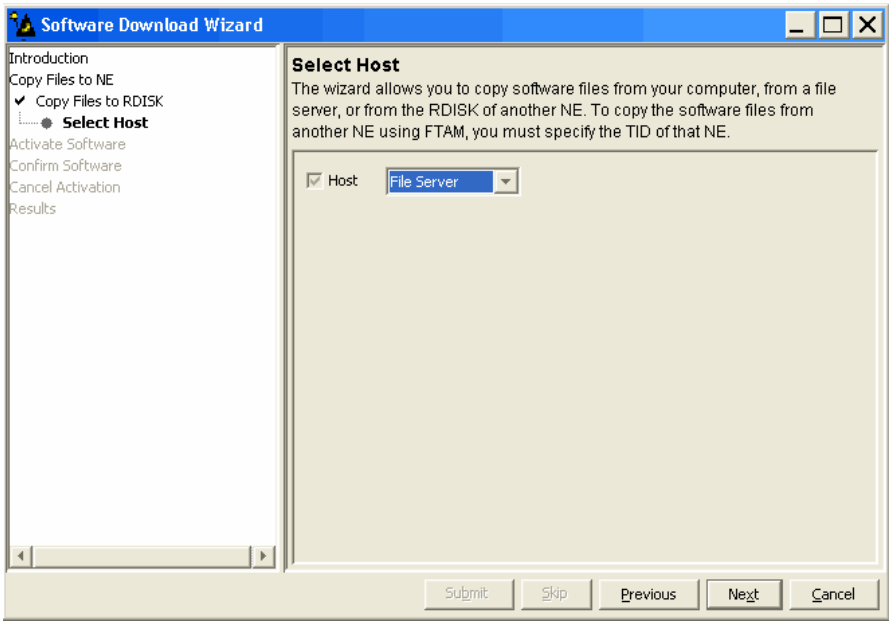


Figure 70: Example Software Download Wizard Select Host Screen

Download Software Program File from Server

Step 14
From the *Host* drop-down list, select *File Server*.

Step 15
Click *Next*.

The *Select FTP Server* screen opens.

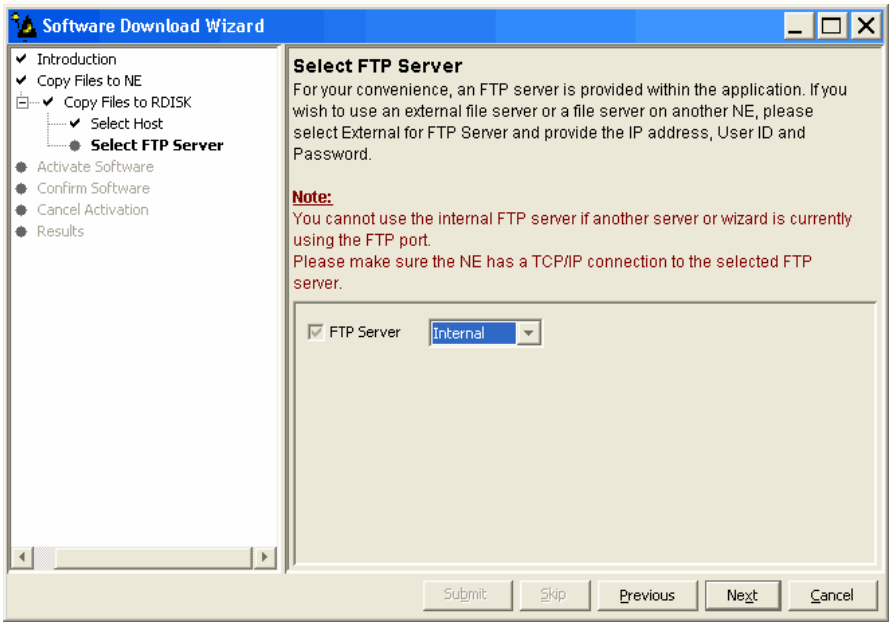


Figure 71: Example Software Download Wizard Select FTP Server Screen

Step 16
Are the software files located on an internal or external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 17
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 18
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

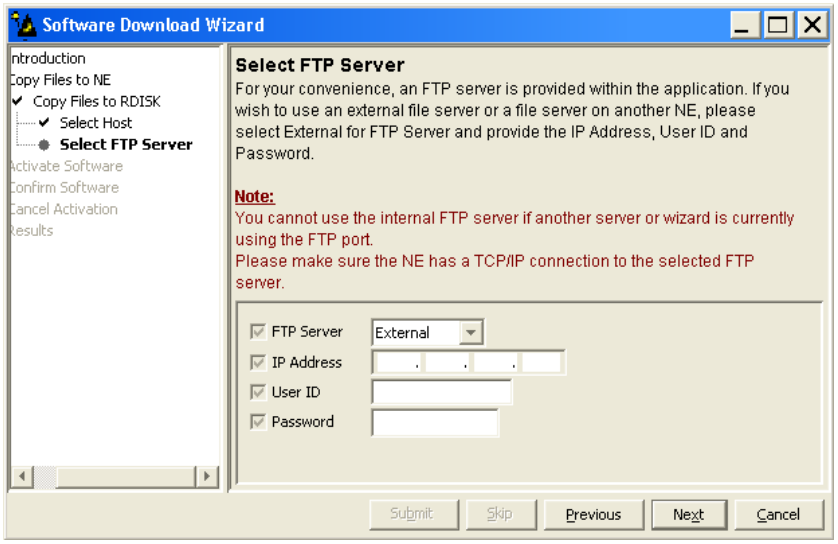


Figure 72: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 19
Click *Next*.

The *Select Files* screen opens.

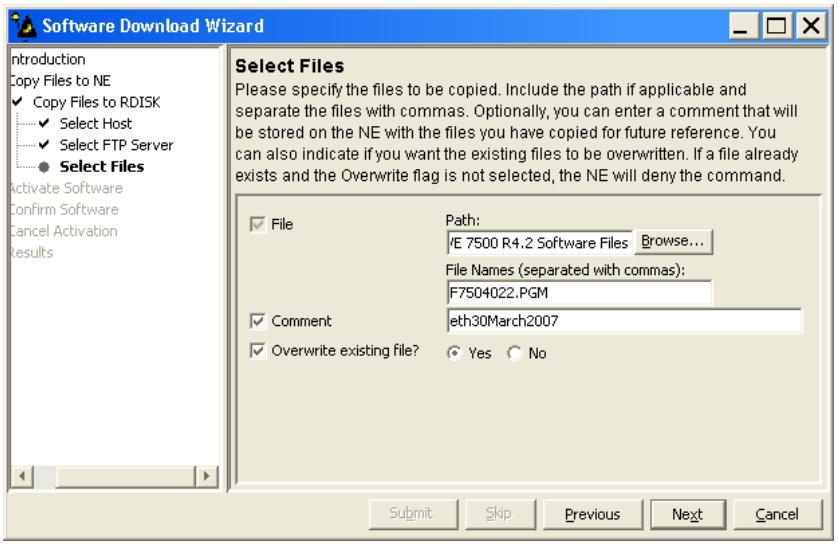


Figure 73: Example Software Download Wizard Select Files Screen

Step 20
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 21
In the *File* text box, enter the appropriate file name of the software file: F7504022.PGM.

Step 22
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 23
Select *Yes* for the *Overwrite existing file* option.

Step 24
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 18 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

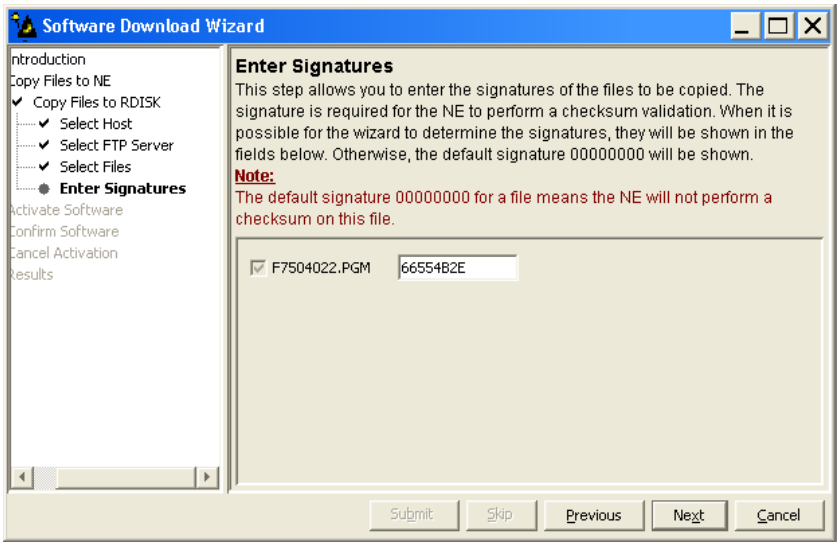


Figure 74: Example Software Download Wizard Enter Signatures Screen

Step 25
Click *Next*.

The *Copy to RDISK* screen opens.

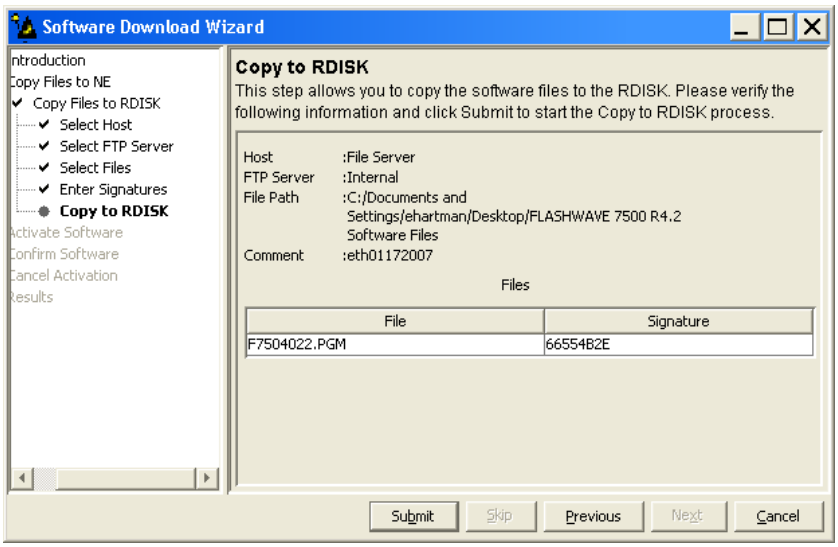


Figure 75: Example Software Download Wizard Copy to RDISK Screen

Step 26
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying for each file.

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

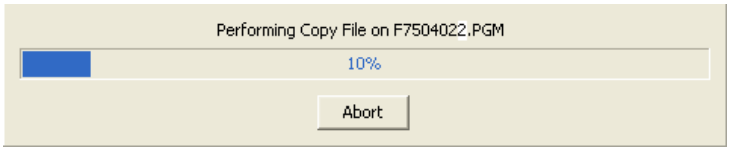


Figure 76: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

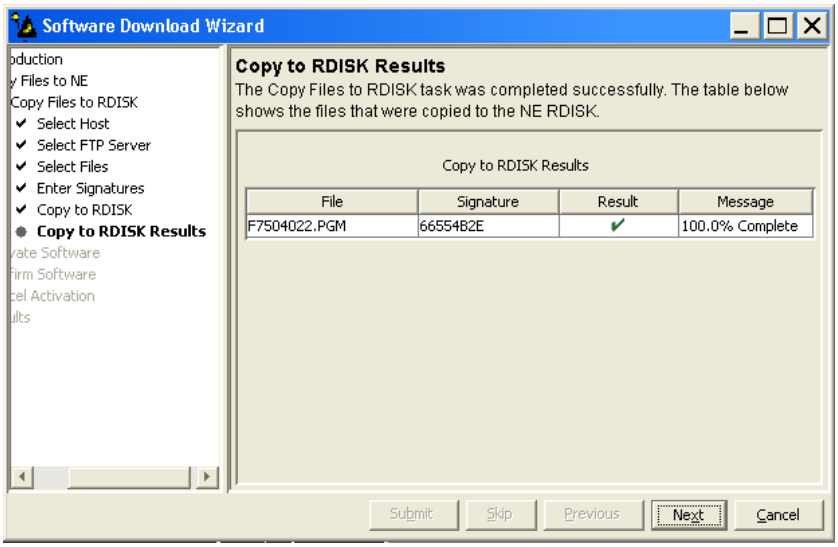


Figure 77: Example Software Download Wizard Copy to RDISK Results Screen

Step 27
Click *Cancel* and then *Yes* to close the wizard.

Step 28
Continue with the next step.

Start the Software Download Wizard at Remote NE

Step 29
Switch to the Remote NE.

Step 30
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may be momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this screen, and each subsequent screen.*

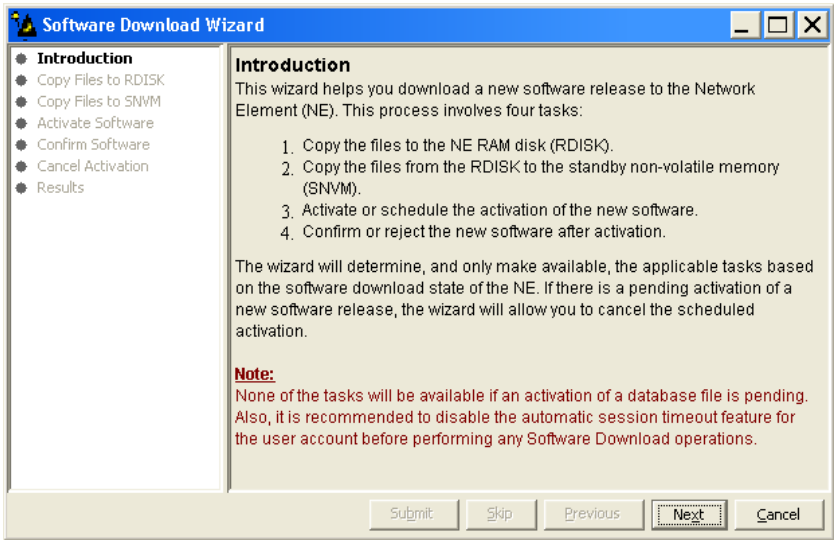


Figure 78: Example Software Download Wizard Introduction Screen

Step 31
Click *Next*.

The *Copy Files to RDISK* screen appears.

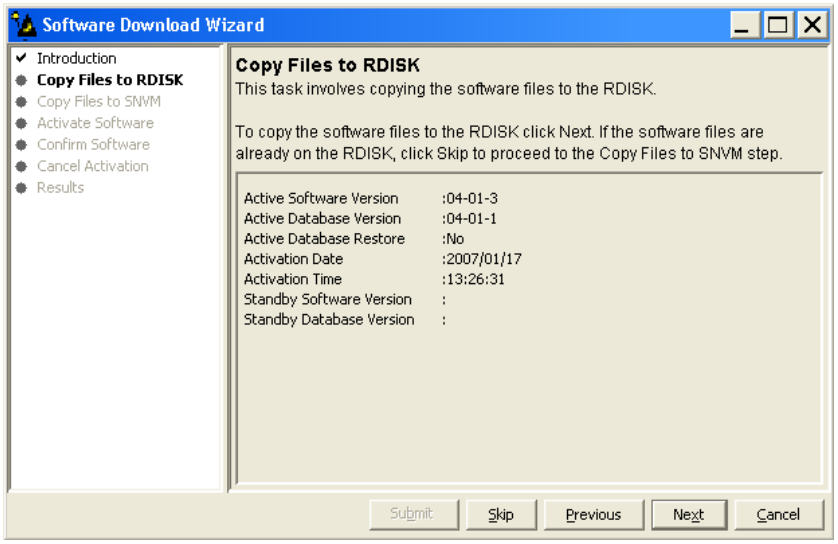


Figure 79: Example Software Download Wizard Copy Files to RDISK Screen

Step 32
Click *Next*.

The *Select Host* screen opens.

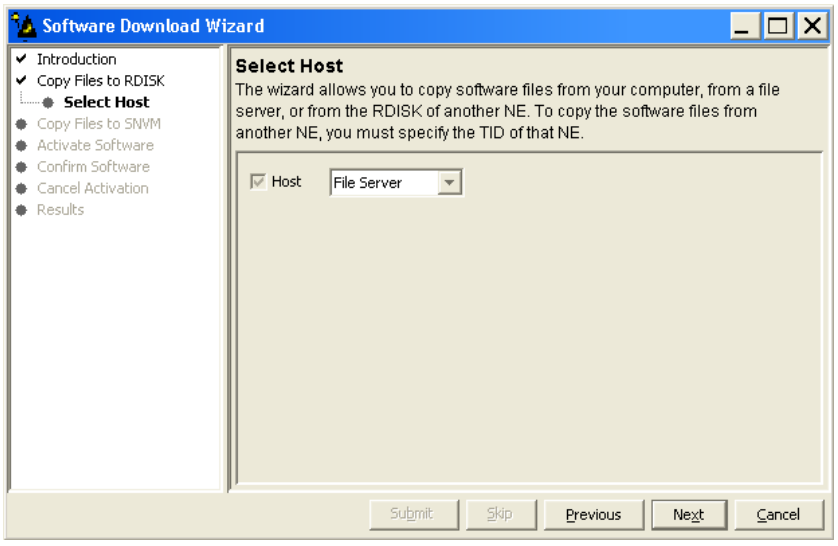


Figure 80: Example Software Download Wizard Select Host Screen

Download Software Program File from Another NE

Step 33
From the *Host* drop-down list, select *Another NE*.

The *Select Host* screen displays an additional field.

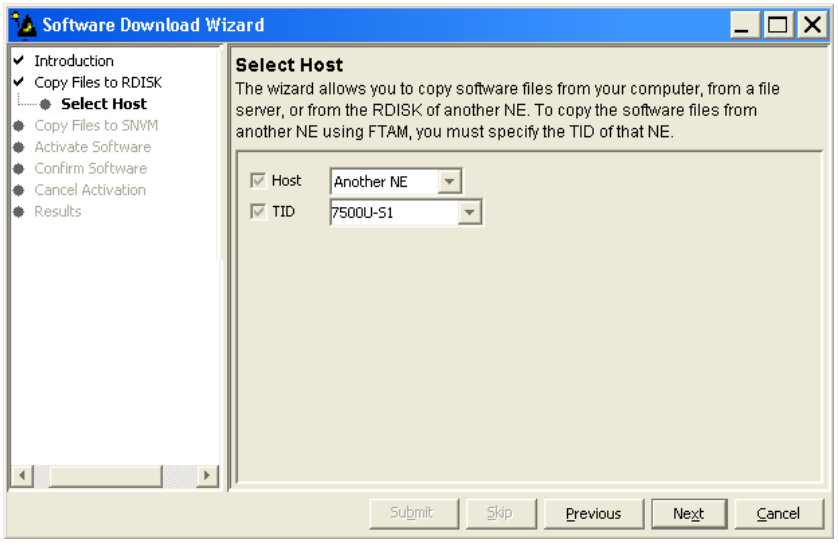


Figure 81: Example Software Download Wizard Select Host–Another NE Selected

Step 34
From the *TID* drop-down list, select the TID of the Local NE.

Step 35
Click *Next*.

The *Select Files* screen appears.

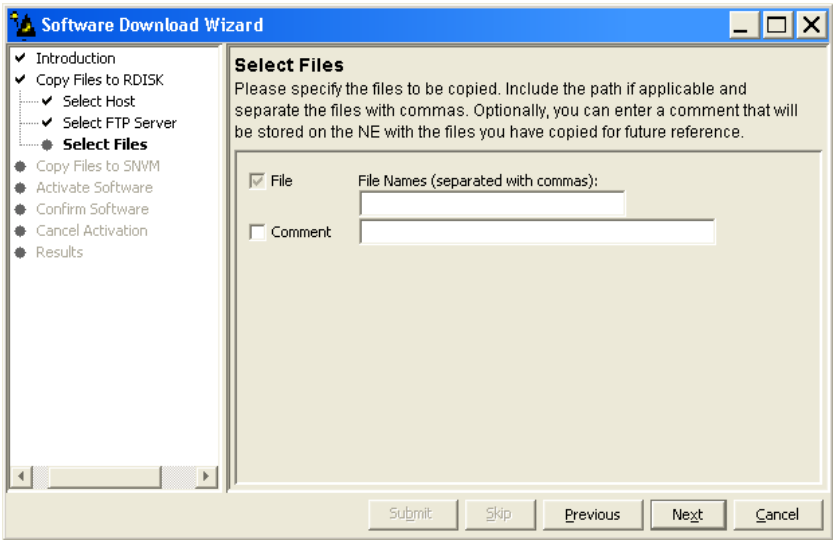


Figure 82: Example Software Download Wizard Select Files Screen

Step 36
In the *File: File Names (separated with commas)* text box, enter the appropriate file name of the software file: F7504022.PGM.

Step 37
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 38
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 33 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

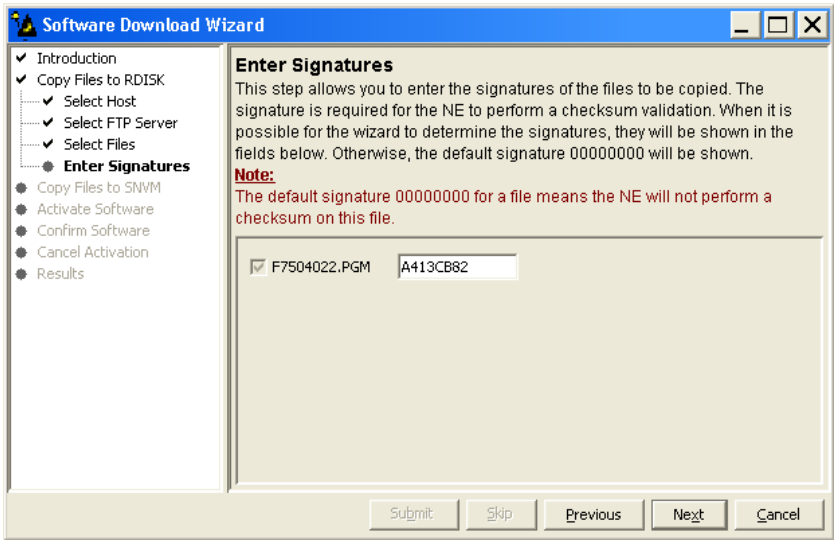


Figure 83: Example Software Download Wizard Enter Signatures Screen

Step 39
Click *Next*.

The *Copy to RDISK* screen opens.

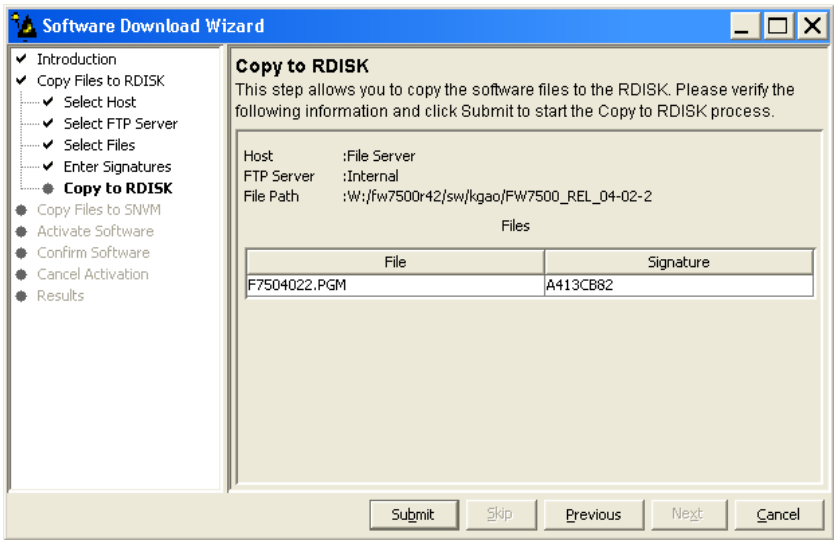


Figure 84: Example Software Download Wizard Copy to RDISK Screen

Step 40
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying for each file (see Figure 76).

Note: *The file may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

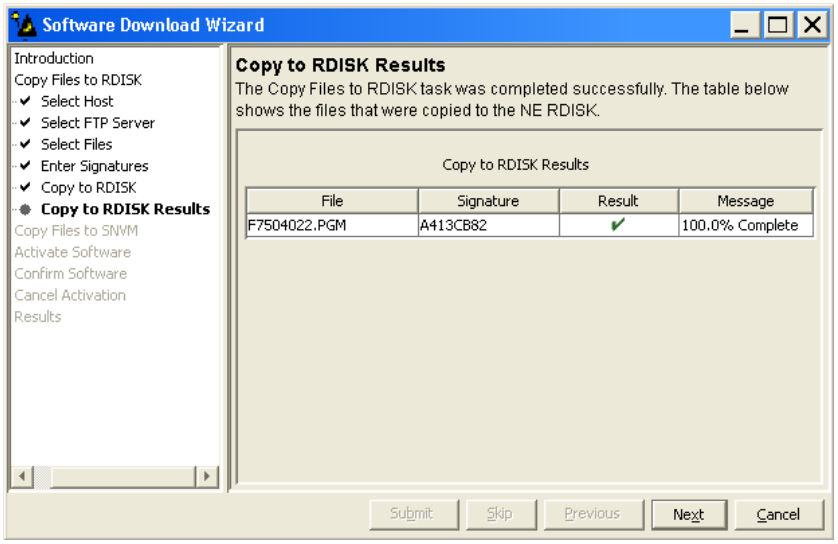


Figure 85: Example Software Download Wizard Copy to RDISK Results Screen

Step 41
Click *Next*.

The *Copy Files to SNVM* screen appears.

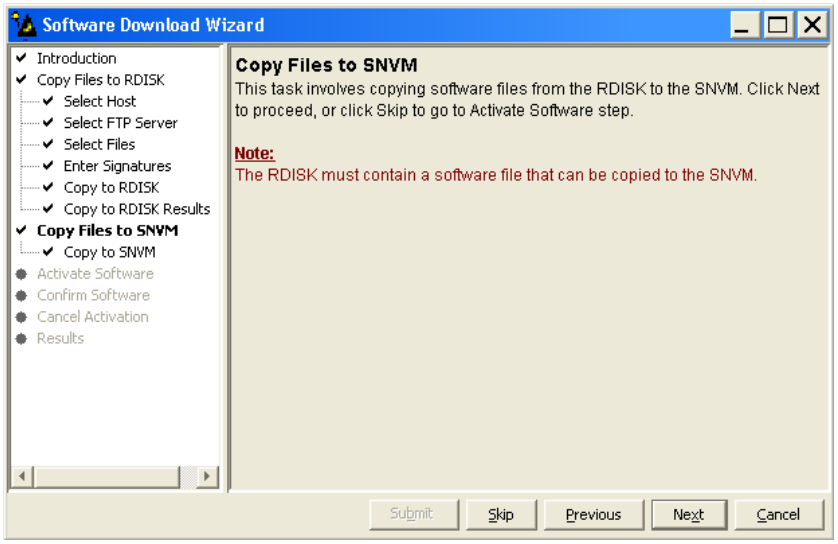


Figure 86: Example Software Download Wizard Copy Files to SNVM Screen

Step 42
Click *Next*.

The *Copy to SNVM* screen appears.

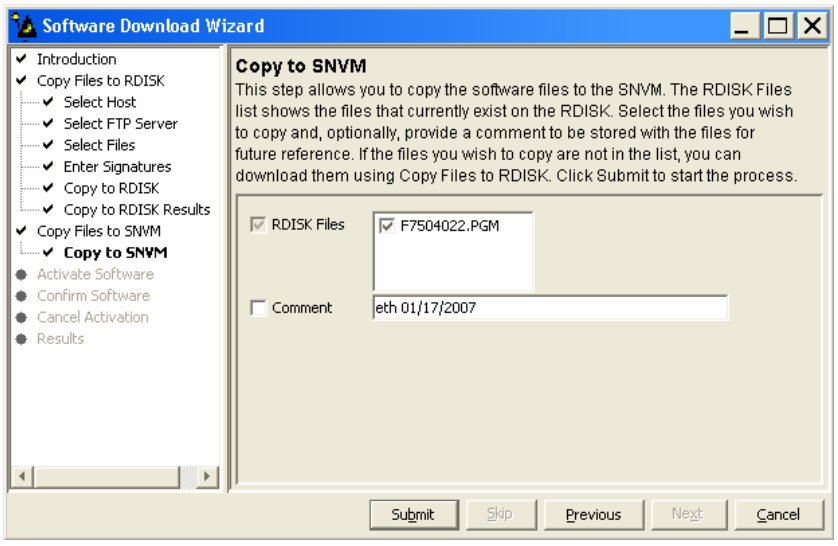


Figure 87: Example Software Download Wizard Copy to SNVM Screen

Step 43
Click *Submit*.

A *Performing Copy* progress window opens, displaying the progress of the copying.

Note: *The copying of the file may take up to 15 minutes.*

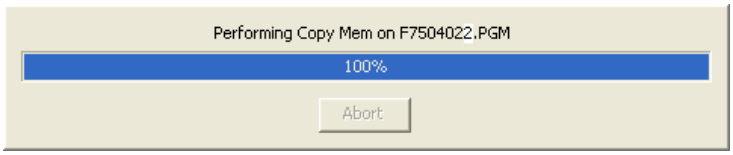


Figure 88: Example of a Typical Performing Copy Progress Window

A successful completion message box momentarily appears, and then the *Copy to SNVM Results* screen appears.

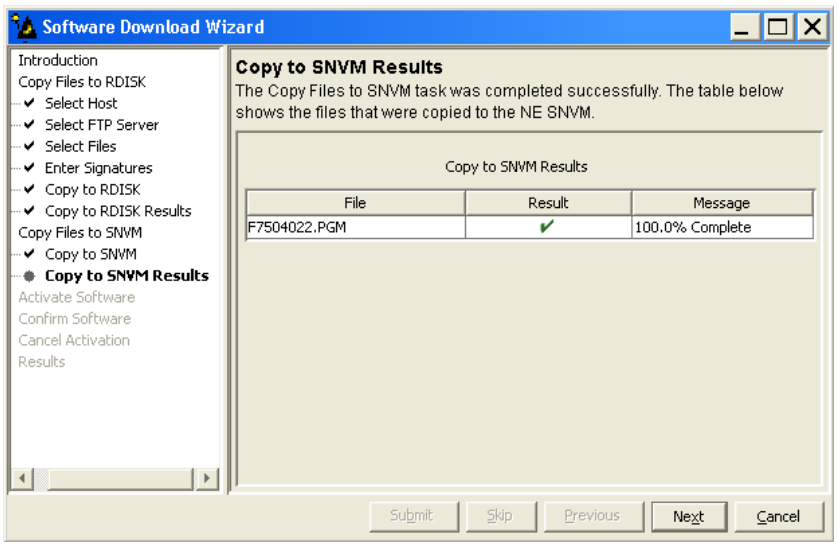


Figure 89: Example Software Download Wizard Copy to SNVM Results Screen

Activate Software on Remote NE

Step 44
Click *Next*.

The *Activate Software* screen opens.

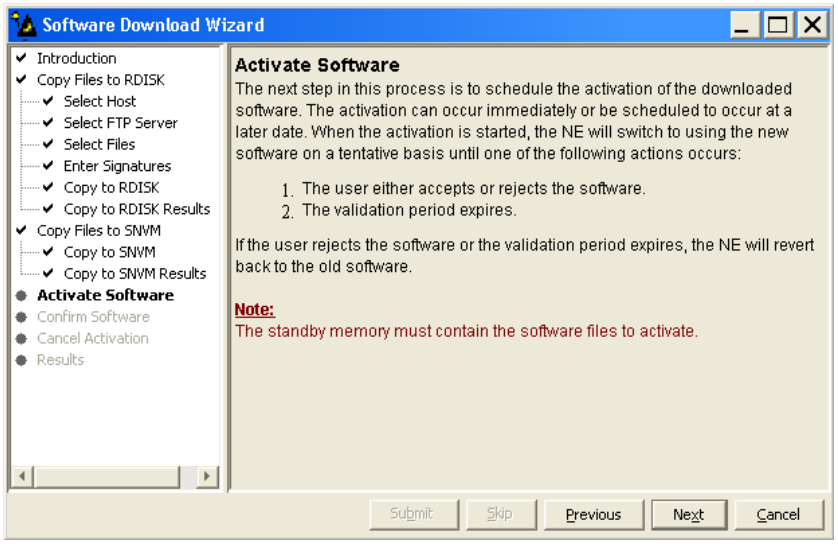


Figure 90: Example Software Download Wizard Activate Software Screen

Step 45
Click *Next*.

The *Software Activation Parameters* screen opens.

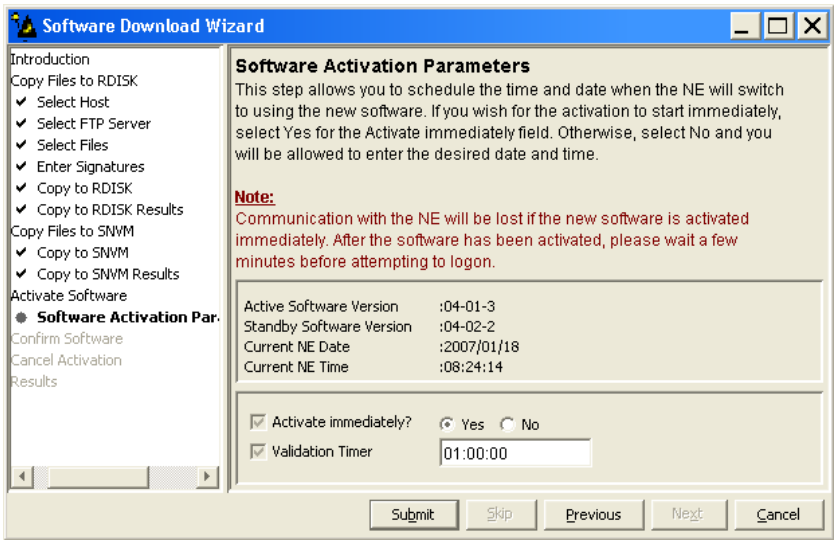


Figure 91: Example Software Download Wizard Software Activation Parameters Screen

Step 46
Verify *Yes* is selected for the *Activate immediately* option.

Note: *The Release 4.2 software must be activated before the firmware can be upgraded.*

Step 47
In the *Validation Timer* text box, enter the desired time before the system reverts back to the previous software (the default is 01:00:00 [1 hour]).

Step 48
Click *Submit*.

The *Software Activation Result* screen opens.

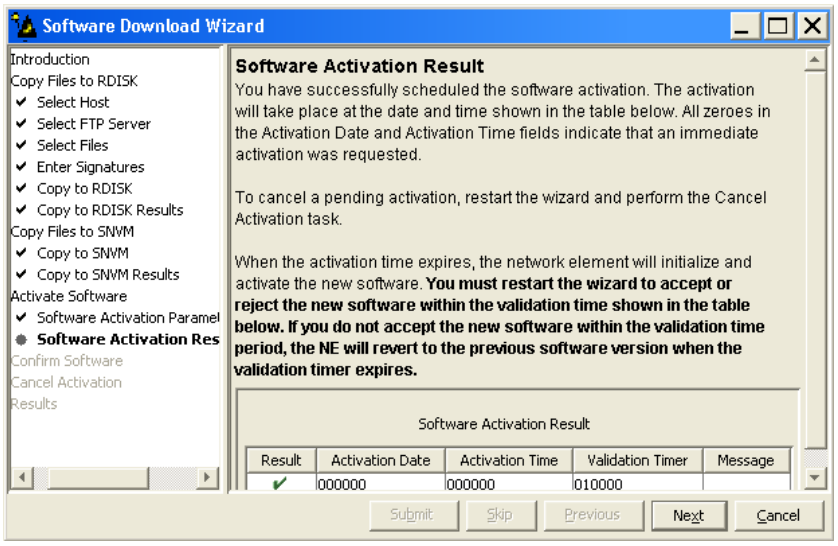


Figure 92: Example Software Download Wizard Software Activation Result Screen

Step 49
Click *Next*.

A *Warning* dialog box opens.

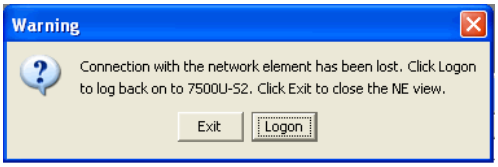


Figure 93: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, a data communication channel failure (DCCFAIL) alarm is raised on the Local NE. The DCCFAIL alarm will clear once the Remote NE resets. You can then log on the Remote NE.*

Step 50
Click *Logon*.

The *Software Activation Result* screen closes, and the Software Download wizard closes.

Confirm Software Download

Note: *You must accept the new software load before the validation timer set in* Step 47 *expires. Otherwise, the system software will revert back to the previous load.*

Step 51
Log back on the Remote NE. Refer to Step 3, if necessary.

Step 52
From the menu bar, select *Wizards* > *Software Download*.

The Software Download wizard starts, and the *Introduction* screen opens.

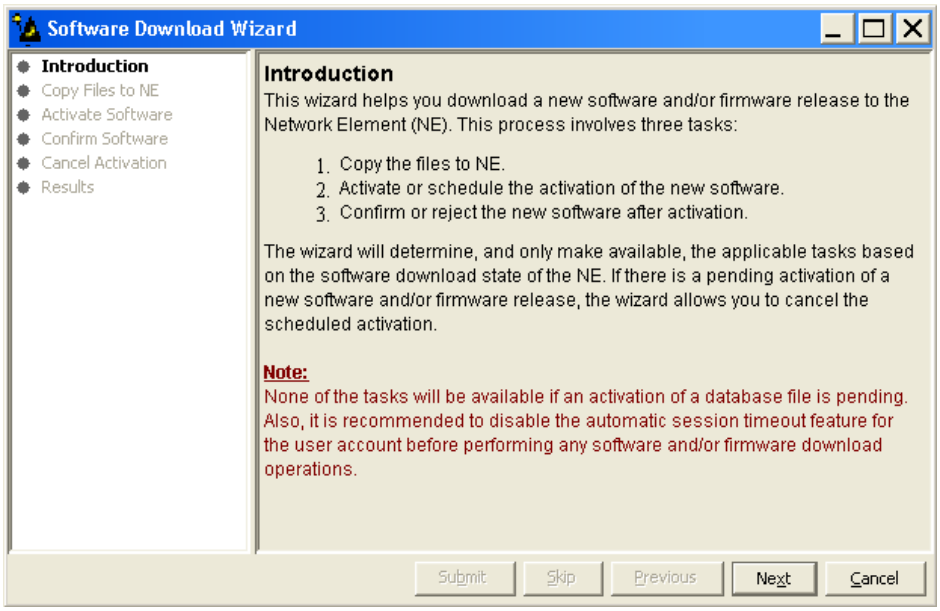


Figure 94: Example Software Download Wizard Introduction Screen

Step 53
Click *Next*.

The *Confirm Software* screen opens.

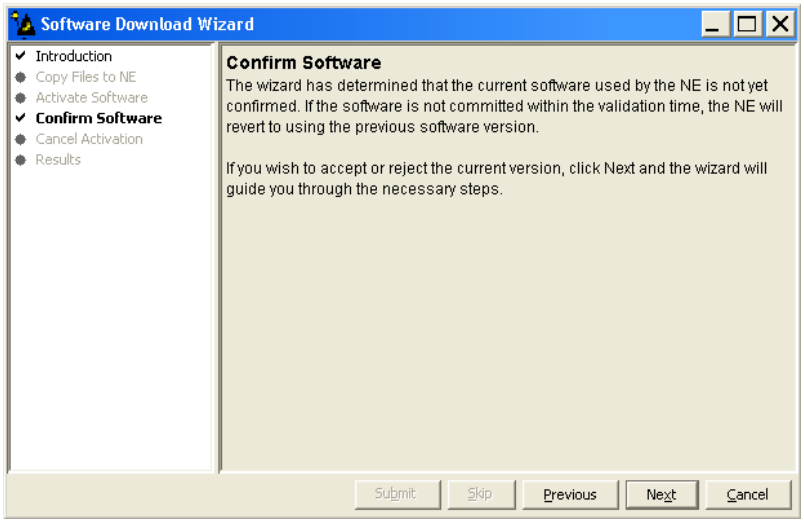


Figure 95: Example Software Download Wizard Confirm Software Screen

Step 54
Click *Next*.

The *Accept/Reject Software* screen opens.

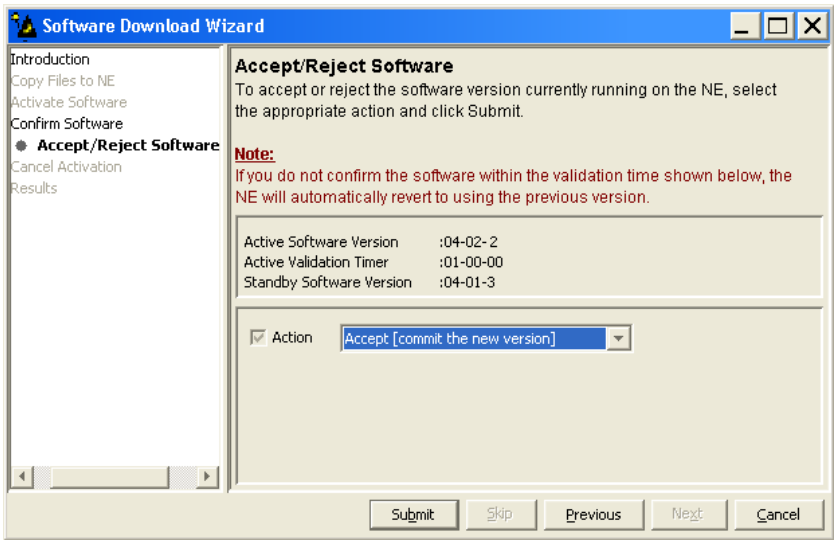


Figure 96: Example Software Download Wizard Accept/Reject Software Screen

Step 55
Verify that the *Accept [commit the new version]* option is selected in the *Action* drop-down list.

Step 56
Click *Submit*.

A progress bar displays while the validation timer is cancelled and the software is accepted.

Attention: *During the software acceptance process, an alarm is raised on the Remote NE. The no firmware (NOFW) alarm is raised because the system is now operating with firmware supporting software and is expecting firmware. Ignore this alarm; it will clear once the firmware is loaded on the system.*

Once the software is accepted, the *Software Confirmation Result* screen opens.

Note: *The screen may take up to 20 minutes to open.*

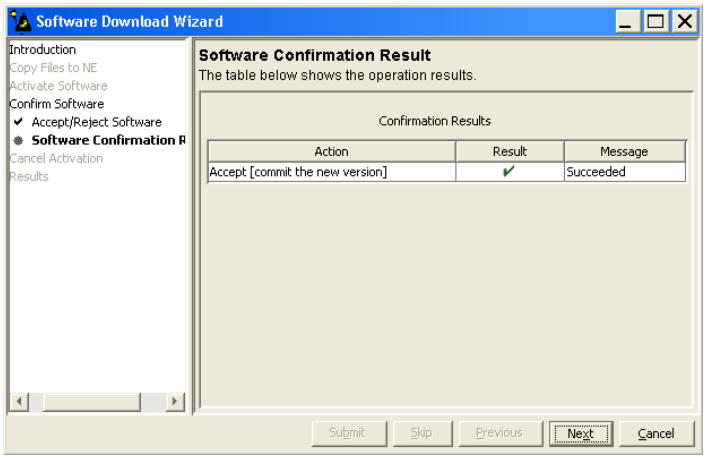


Figure 97: Example Software Download Wizard Software Confirmation Result Screen

Step 57
Click *Next*.

The final *Results* screen opens.

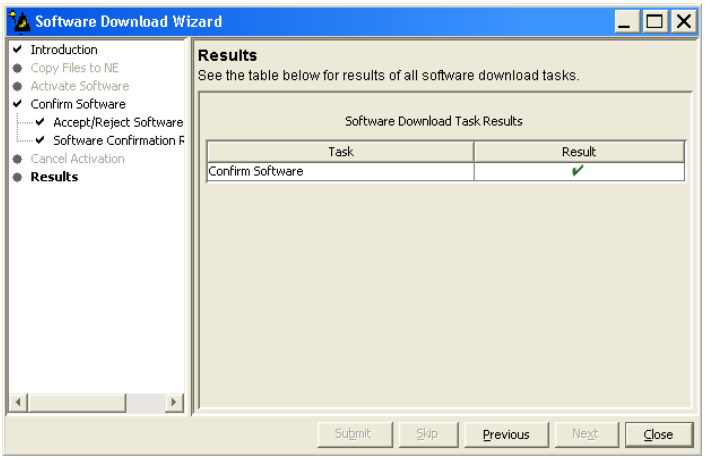


Figure 98: Example Software Download Wizard Results Screen

Step 58
Click *Close*.

The *Results* screen closes and the Software Download wizard closes.

Step 59
Retrieve alarms and conditions on the NE.

NETSMART 500

NE ▸ *Alarms*

View ▸ *Filter*

Verify that all Fault Types and Severity Levels are selected as reporting.
Click Close.
Close Active Alarms window.

Step 60
Are any active alarms or conditions being reported on the NE, other than the NOFW alarm?

If YES:
Clear all active alarms and conditions (excluding the NOFW alarm). After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *The NOFW alarm will clear once firmware is loaded in stage two of this procedure.*

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Delete Program File from RDISK of the Remote NE and Local NE

Step 61
At the Remote NE, delete the software files from the RDISK.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select DLT-FILE command from the *Command Name* drop-down list.
Enter *ALL* in the *AID* field.
Click *Send*.

Do not close the TL1 Command Builder dialog box.

Step 62
Verify the RDISK disk on the Remote NE is empty.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.

Enter the program file name or ALL in the AID field.
Click *Send*.

Close the TL1 Command Builder dialog box.

Step 63
Switch to the Local NE.

Step 64
At the Local NE, delete the software files from the RDISK.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select DLT-FILE command from the *Command Name* drop-down list.
Enter *ALL* in the *AID* field.
Click *Send*.

Do not close the TL1 Command Builder dialog box.

Step 65
Verify the RDISK disk on the Local NE is empty.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.

Enter the program file name or ALL in the AID field.
Click *Send*.

Close the TL1 Command Builder dialog box.

Step 66
Continue with the next step.

Start the Software Download Wizard at Local NE

Step 67
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens (the following figure).

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this screen, and each subsequent screen.*

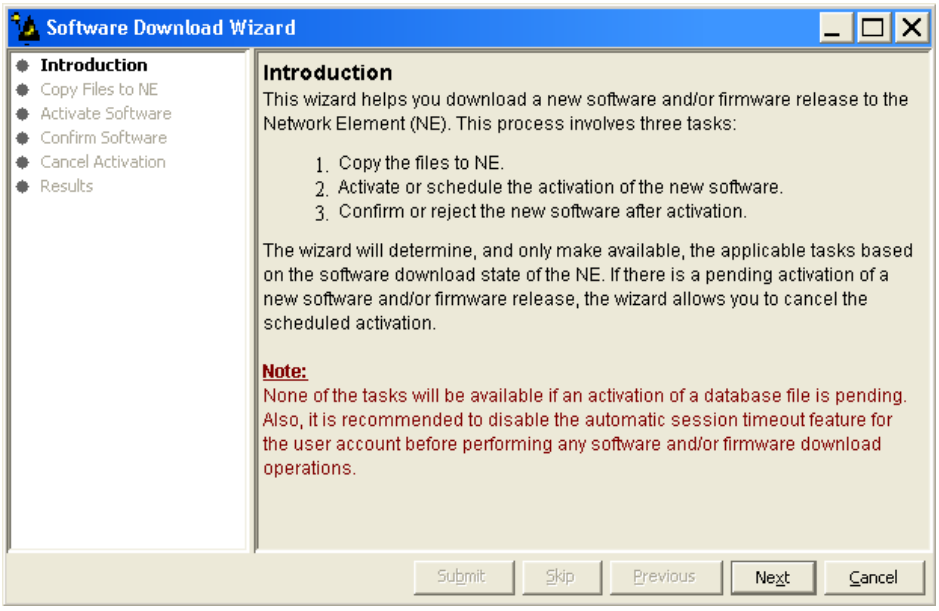


Figure 99: Example Software Download Wizard Introduction Screen

Step 68
Click *Next*.

The *Copy Files to NE* screen appears.

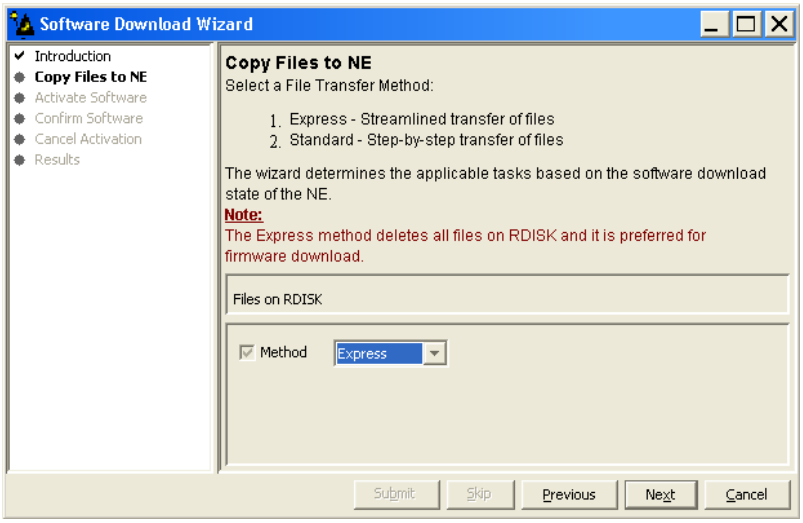


Figure 100: Example Software Download Wizard Copy Files to NE Screen

Step 69
Select *Standard* from the *Method* drop-down list.

Note: *Do not use the Express method at the Local NE. The Express method copies the software files to the RDISK, then to the SNVM, then deletes the software files from the RDISK. This procedure requires that the software files are copied only to the RDISK of the Local NE.*

Step 70
Click *Next*.

The *Copy Files to RDISK* screen opens.

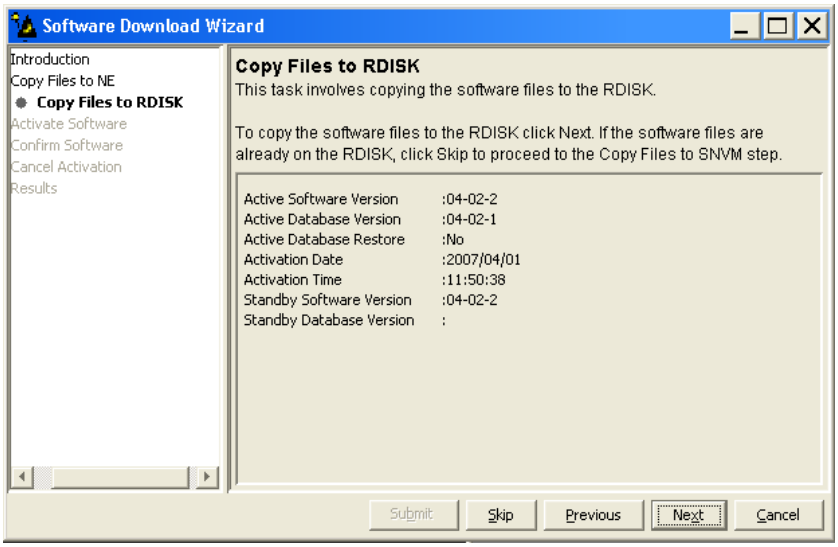


Figure 101: Example Software Download Wizard Copy Files to RDISK Screen

Step 71
Click *Next*.

The *Select Host* screen opens.

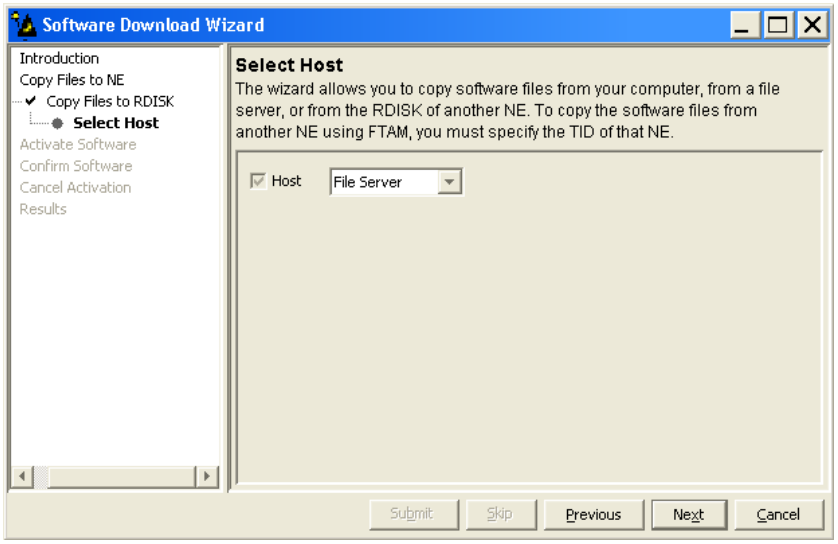


Figure 102: Example Software Download Wizard Select Host Screen

Download Firmware and Configuration Files from Server

Step 72
From the *Host* drop-down list, select *File Server*.

Step 73
Click *Next*.

The *Select FTP Server* screen opens.

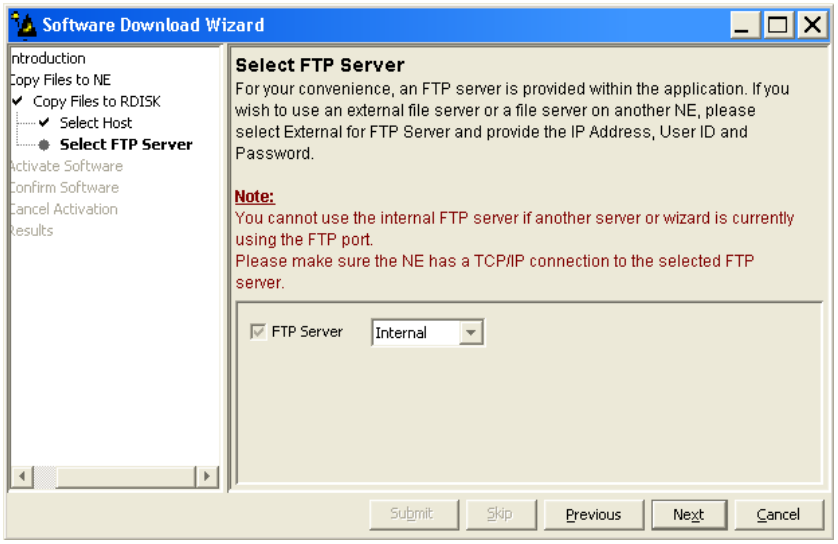


Figure 103: Example Software Download Wizard Select FTP Server Screen

Step 74
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 75
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 76
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

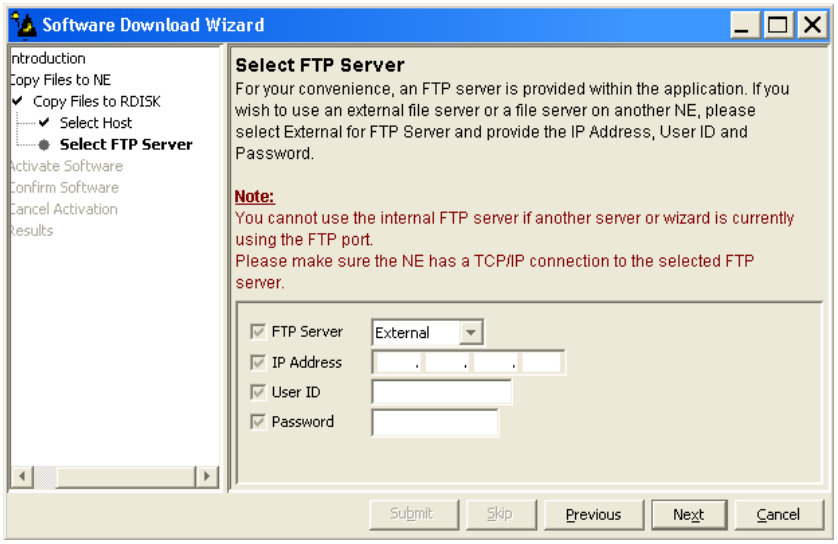


Figure 104: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 77
Click *Next*.

The *Select Files* screen opens.

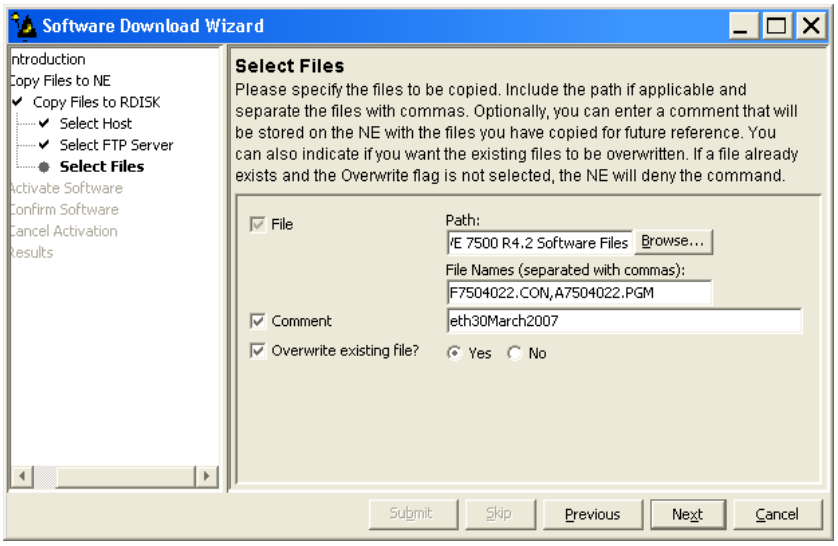


Figure 105: Example Software Download Wizard Select Files Screen

Step 78
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 79
In the *File: File Names (separated with commas)* text box, enter the appropriate file names:

- *F7504022.CON*
- *A7504022.PGM*

Step 80
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 81
Select *Yes* for the *Overwrite existing file* option.

Step 82
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 76 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

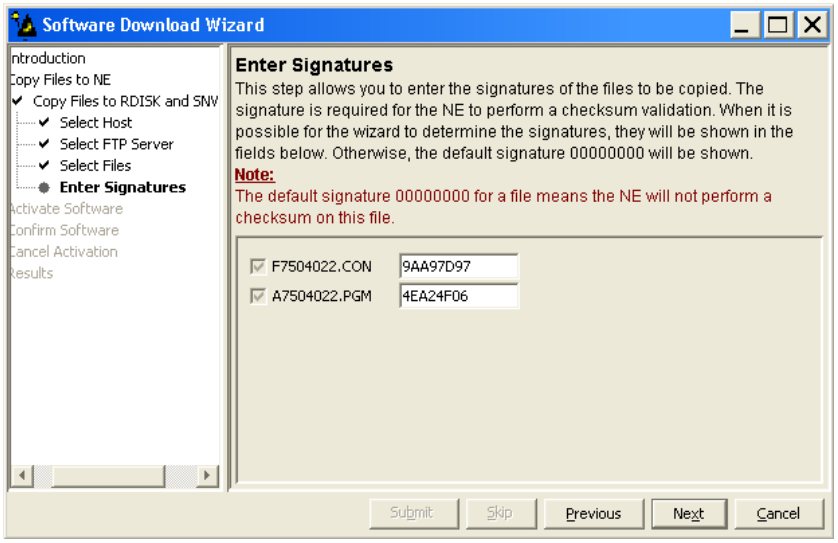


Figure 106: Example Software Download Wizard Enter Signatures Screen

Step 83
Click *Next*.

The *Copy to RDISK* screen opens.

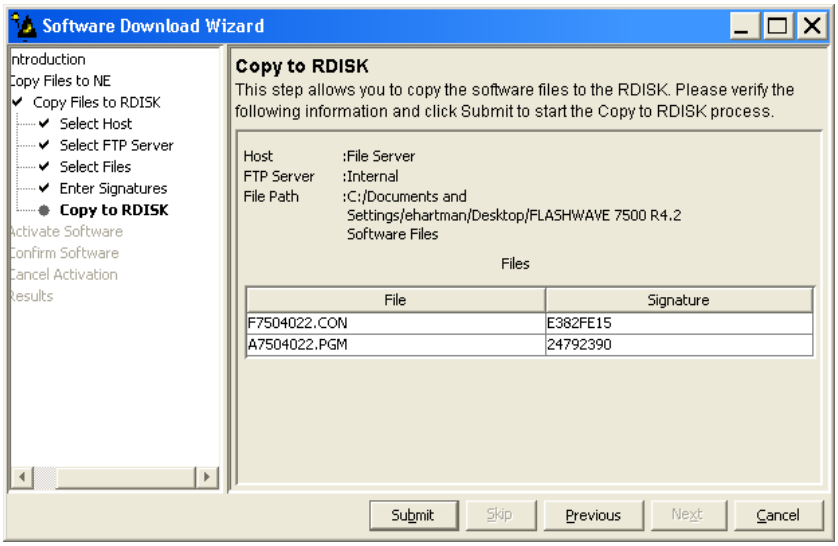


Figure 107: Example Software Download Wizard Copy to RDISK Screen

Step 84
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying of the software file from the server to the RDISK of the local NE (see Figure 88).

Note: *The file takes several minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

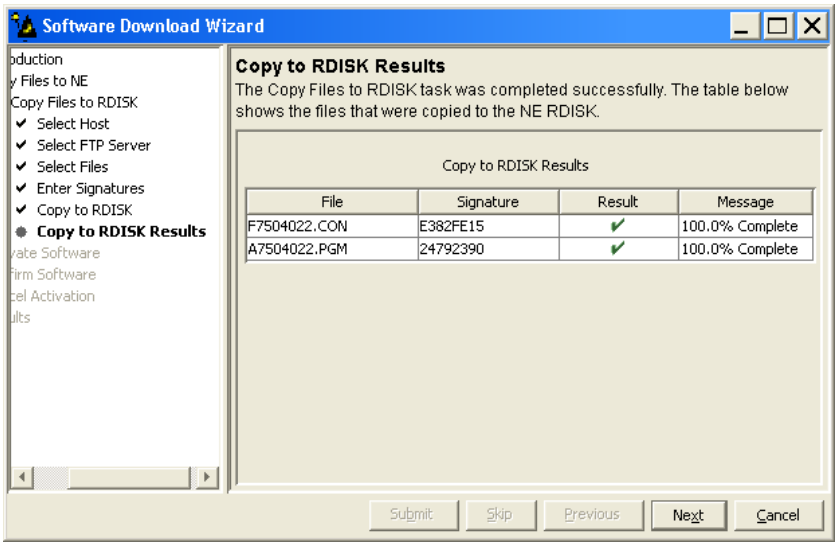


Figure 108: Example Software Download Wizard Copy to RDISK Results Screen

Step 85
Click *Cancel* and then *Yes* to close the wizard.

Step 86
Continue with the next step.

Start the Software Download Wizard at Remote NE

Step 87
Switch to the Remote NE.

Step 88
From the menu bar, select *Wizards* > *Software Download*.

Note: *When progressing through the screens in the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

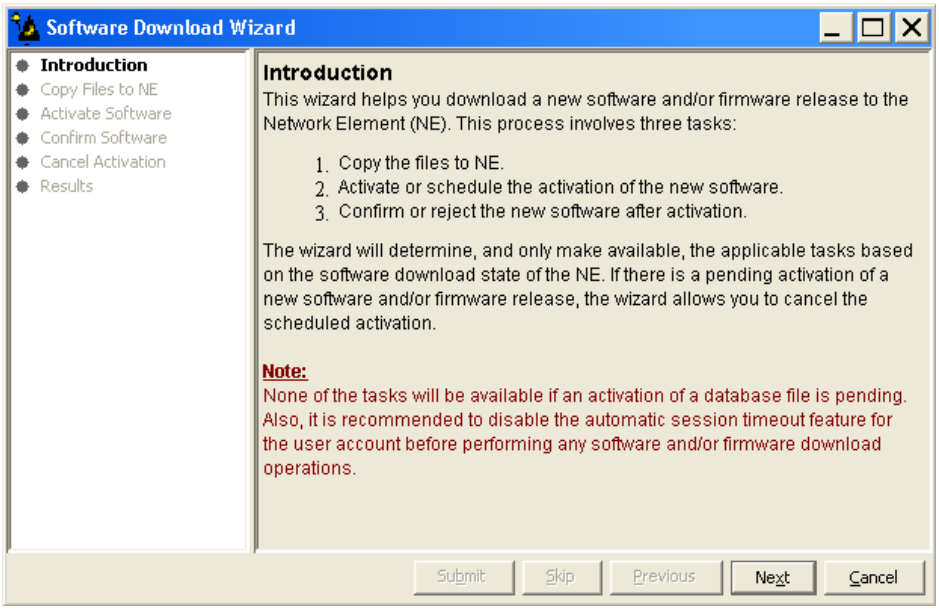


Figure 109: Example Software Download Wizard Introduction Screen

Step 89
Click *Next*.

The *Copy Files to NE* screen opens.

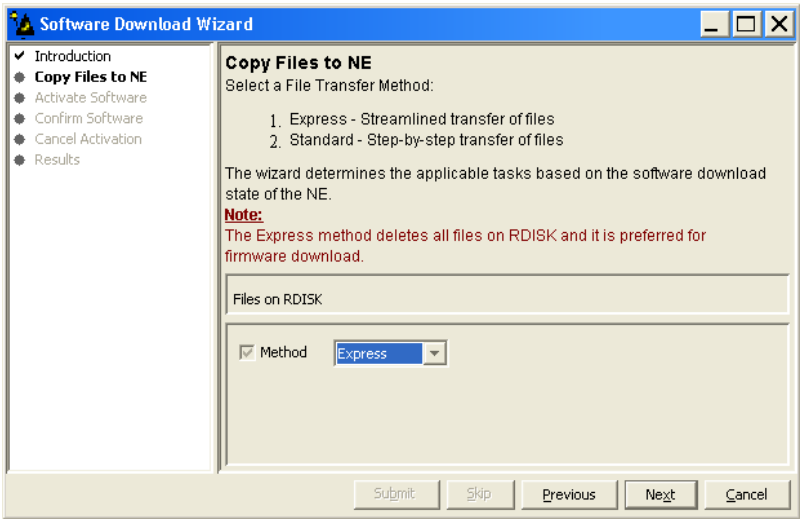


Figure 110: Example Software Download Wizard Copy Files to NE Screen

Step 90
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *The Express method is used to copy the software file from the random access memory disk (RDISK) of the Local NE to the standby nonvolatile memory (SNVM) of the Remote NE. Fujitsu recommends this method because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 91
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

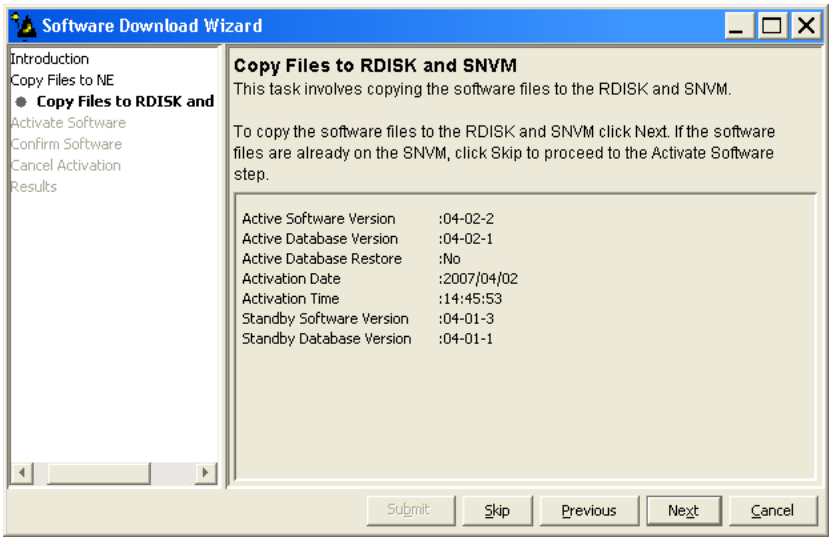


Figure 111: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 92
Verify the *Active Software Version* is *04-02-2*, then click *Next*.

The *Select Host* screen opens.

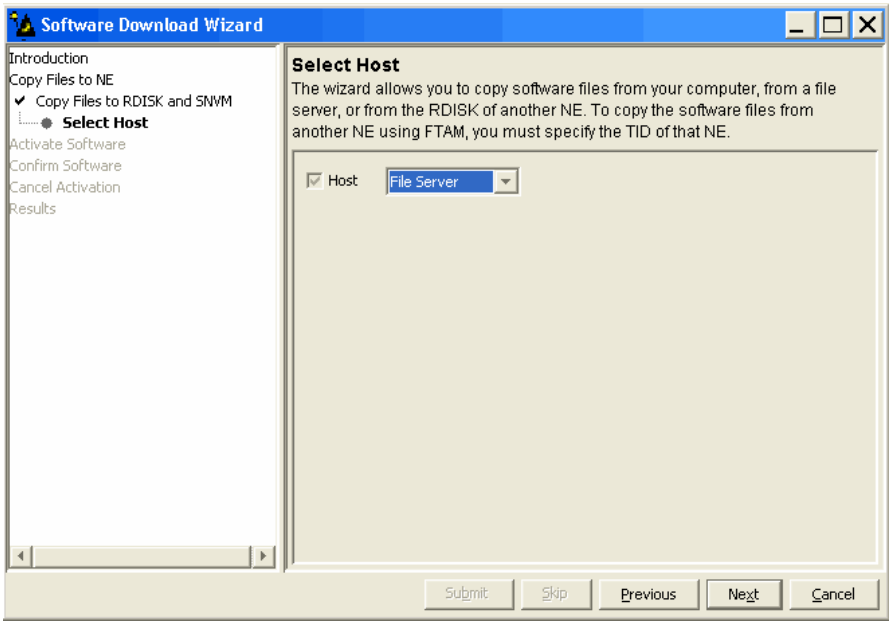


Figure 112: Example Software Download Wizard Select Host Screen

Download Firmware and Configuration Files from Another NE

Step 93
From the *Host* drop-down list, select *Another NE*.

The *Select Host* screen displays an additional field.

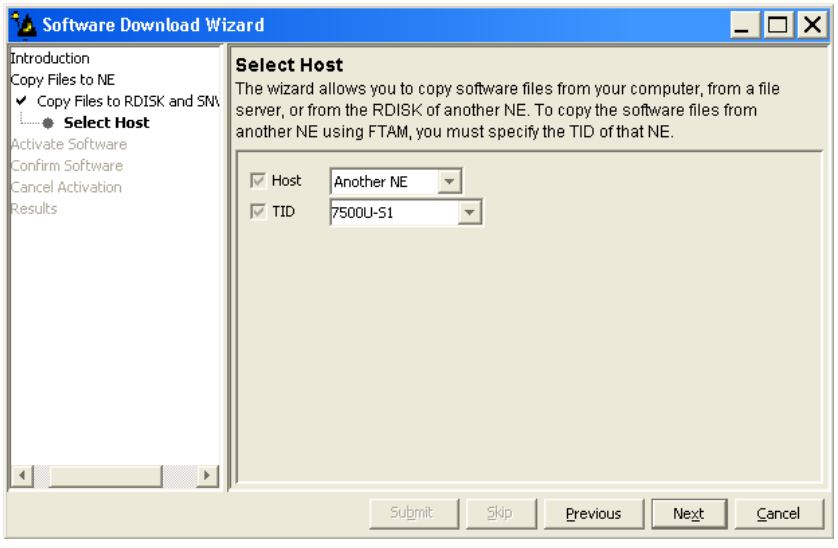


Figure 113: Example Software Download Wizard Select Host–Another NE Selected

Step 94
Select the TID of the Local NE from the *TID* drop-down list, or type the name directly into the *TID* field.

Step 95
Click *Next*.

The *Select Files* screen appears.

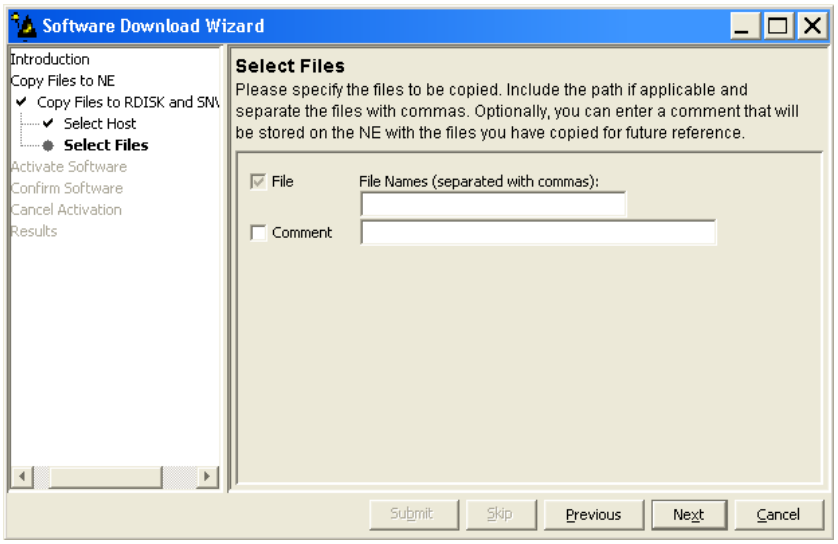


Figure 114: Example Software Download Wizard Select Files Screen

Step 96
In the *File: File Names (separated with commas)* text box, enter the appropriate file names:

- *F7504022.CON*
- *A7504022.PGM*

Step 97
In the *Comment* text box, enter comments.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 98
Click *Next*.

The *Enter Signatures* screen appears.

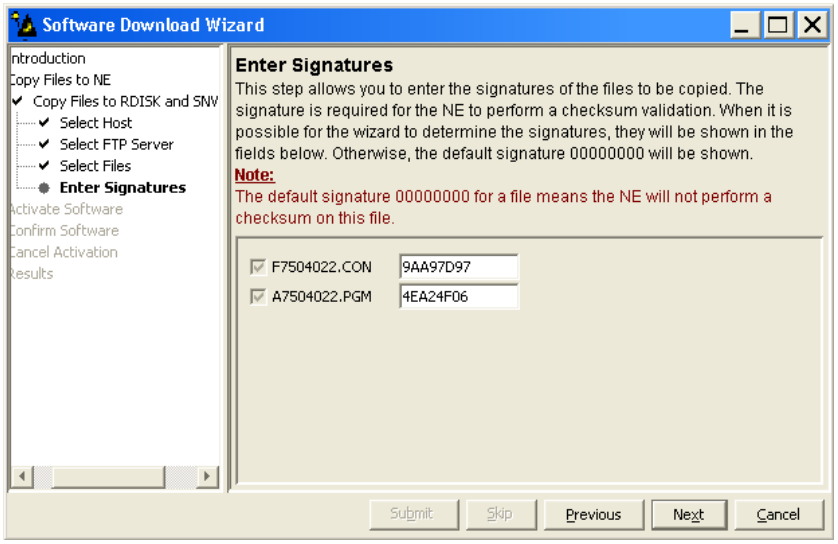


Figure 115: Example Software Download Wizard Enter Signatures Screen

Note: *When the files are being copied from another NE, the signature fields are populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

Step 99
Click *Next*.

The *Copy to RDISK and SNVM* screen appears.

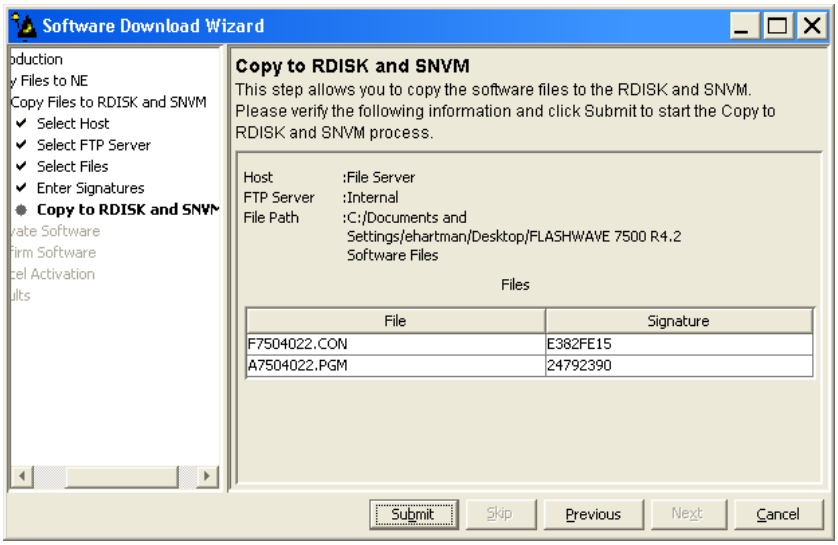


Figure 116: Example Software Download Wizard Copy to RDISK and SNVM Screen

Step 100
Click *Submit*.

A Performing Copy File window opens, displaying the progress of the copying of the software program file from the RDISK of the Local NE (see Figure 88).

Note: *The files can take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen appears.

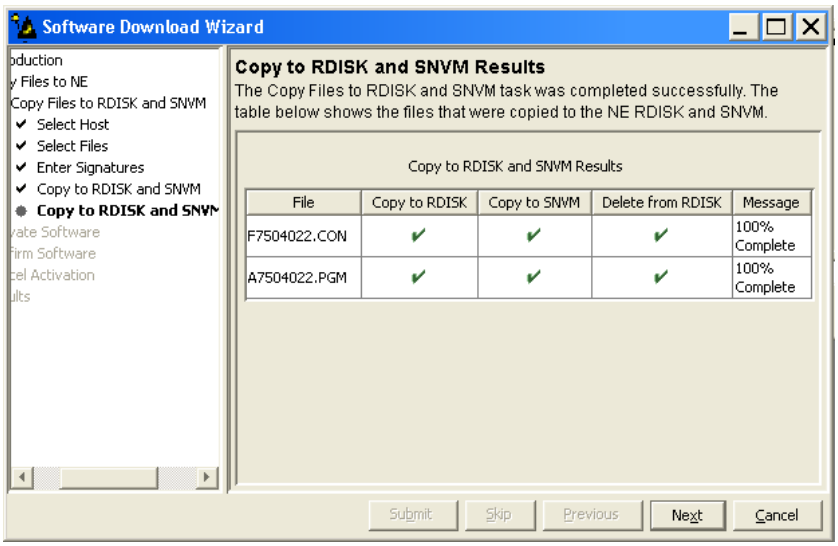


Figure 117: Example of Software Download Wizard Copy to RDISK and SNVM Results Screen

Note: *The F7504022.PGM file must be reloaded to the standby nonvolatile memory of the Remote NE.*

Step 101
Click *Cancel* and then *Yes* to close the wizard.

Step 102
Continue with the next step.

Start the Software Download Wizard at Local NE

Step 103
Switch to the local NE.

Step 104
At the Local NE, delete the software files from the RDISK.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select DLT-FILE command from the *Command Name* drop-down list.
Enter *ALL* in the *AID* field.
Click *Send*.

Do not close the TL1 Command Builder dialog box.

Step 105
Verify the RDISK disk on the Local NE is empty.

NETSMART 500

NE ▸ *TL1 Command Builder*

TL1 Command Builder dialog box opens.

Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.

Enter the program file name or ALL in the AID field.
Click *Send*.

Close the TL1 Command Builder dialog box.

Step 106
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this screen, and each subsequent screen.*

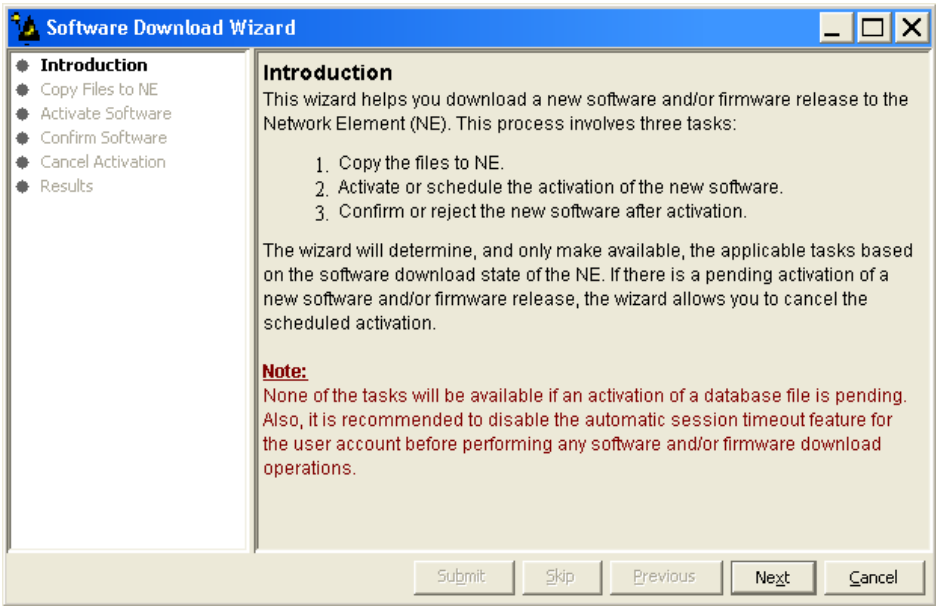


Figure 118: Example Software Download Wizard Introduction Screen

Step 107
Click *Next*.

The *Copy Files to NE* screen appears.

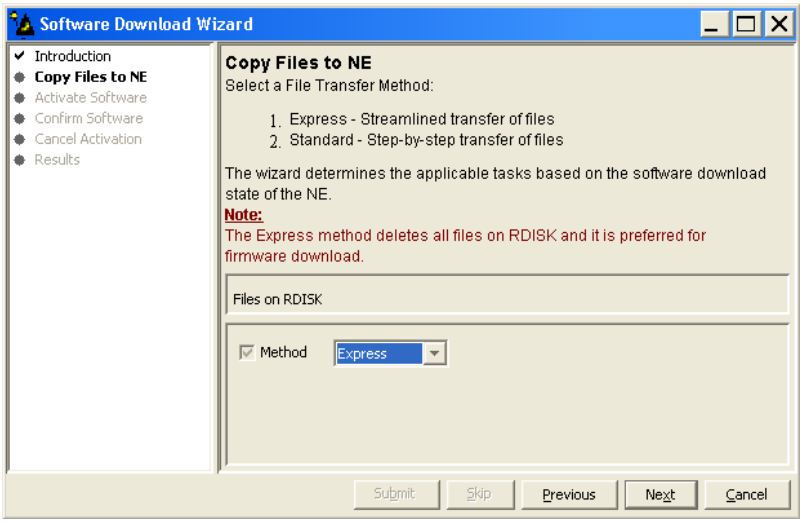


Figure 119: Example Software Download Wizard Copy Files to NE Screen

Step 108
Select *Standard* from the *Method* drop-down list.

Note: *Do not use the Express method at the Local NE. The Express method copies the software files to the RDISK, then to the SNVM, then deletes the software files from the RDISK. This procedure requires that the software files be copied to the RDISK of the Local NE.*

Step 109
Click *Next*.

The *Copy Files to RDISK* screen opens.

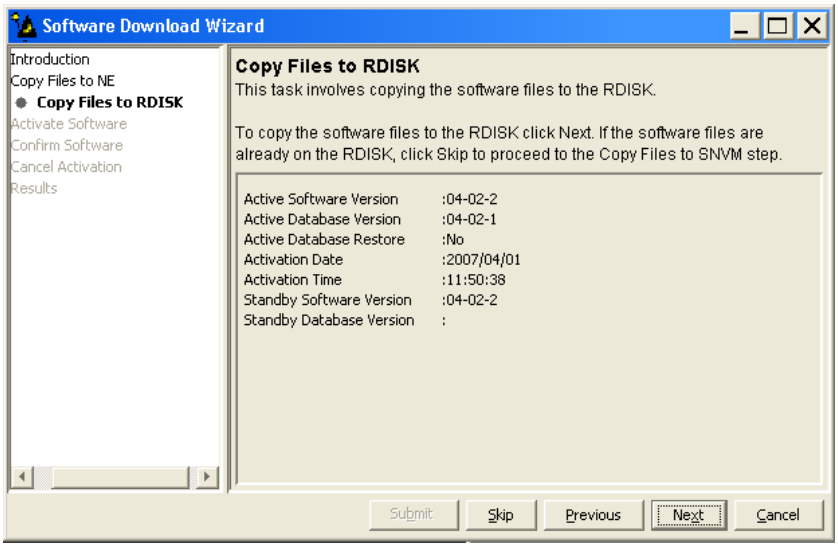


Figure 120: Example Copy Files to RDISK Screen

Step 110
Click *Next*.

The *Select Host* screen opens.

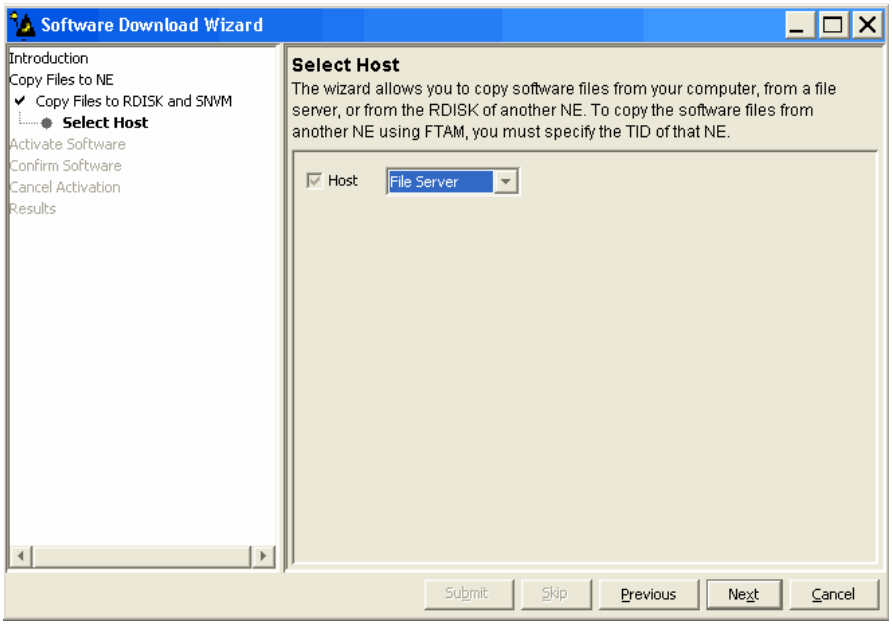


Figure 121: Example Software Download Wizard Select Host Screen

Download Software Program File from Server

Step 111
From the *Host* drop-down list, select *File Server*.

Step 112
Click *Next*.

The *Select FTP Server* screen opens.

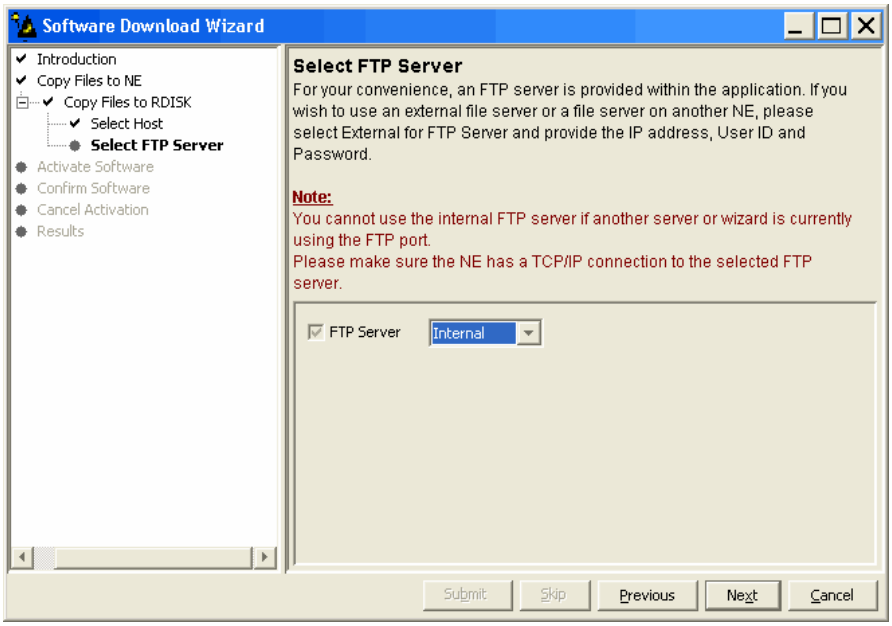


Figure 122: Example Software Download Wizard Select FTP Server Screen

Step 113
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 114
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 115
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

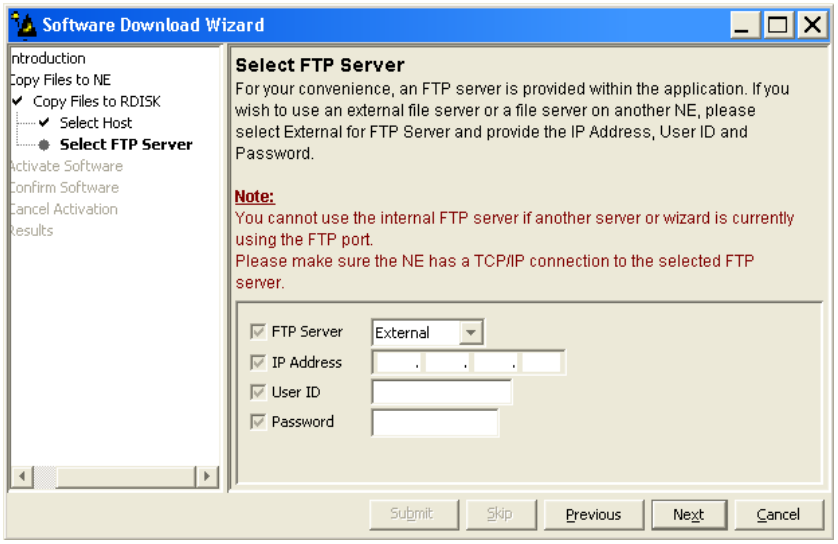


Figure 123: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 116
Click *Next*.

The *Select Files* screen opens.

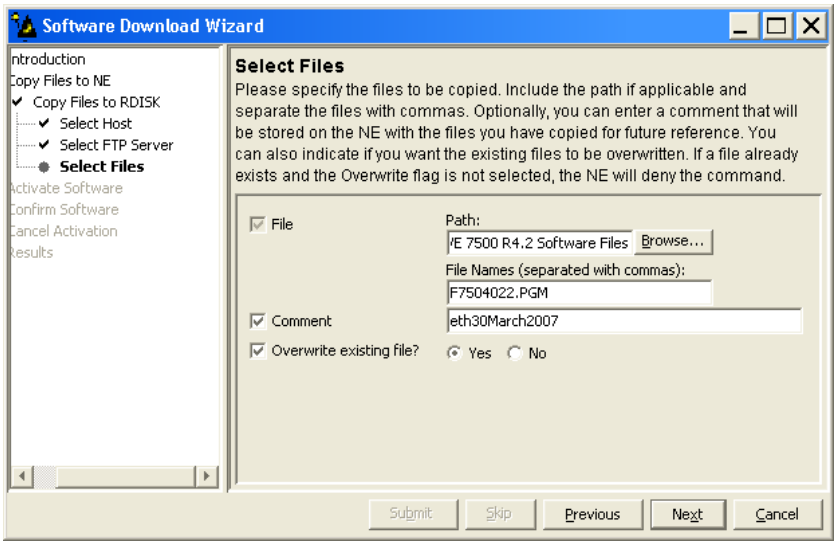


Figure 124: Example Software Download Wizard Select Files Screen

Step 117
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 118
In the *File: File Names (separated with commas)* text box, enter the appropriate file name of the software file: `F7504022.PGM`.

Step 119
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 120
Select *Yes* for the *Overwrite existing file* option.

Step 121
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 115 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

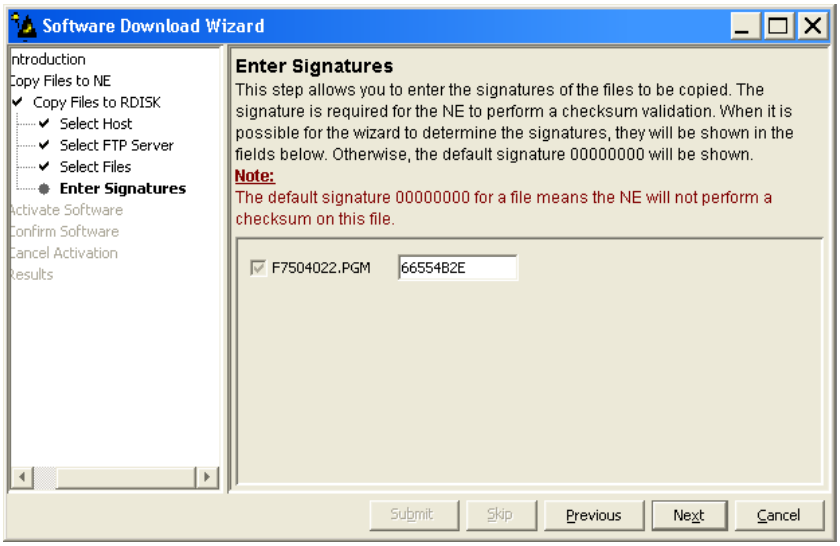


Figure 125: Example Software Download Wizard Enter Signatures Screen

Step 122
Click *Next*.

The *Copy to RDISK* screen opens.

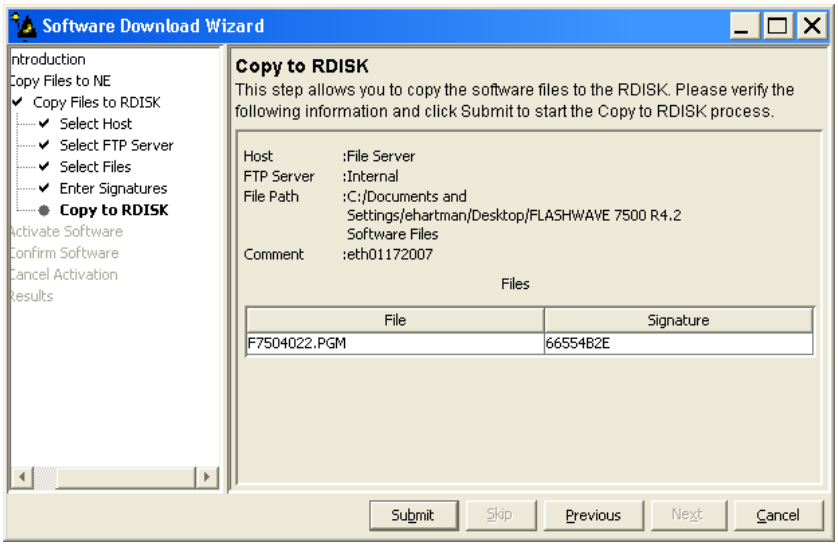


Figure 126: Example Software Download Wizard Copy to RDISK Screen

Step 123
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying for each file.

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

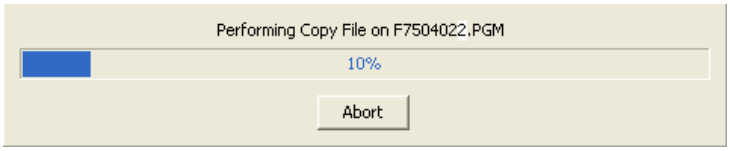


Figure 127: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

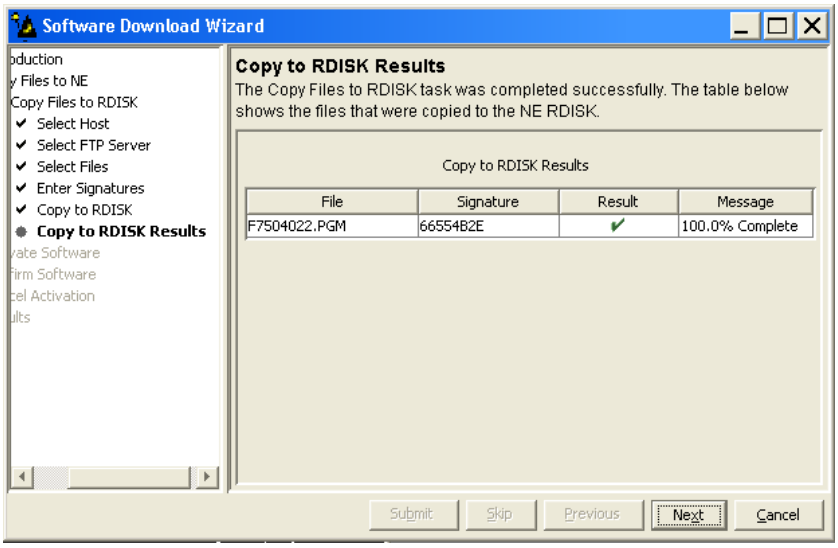


Figure 128: Example Software Download Wizard Copy to RDISK Results Screen

Step 124
Click *Cancel*, then click *Yes* to close the wizard.

Step 125
Continue with the next step.

Start the Software Download Wizard at Remote NE

Step 126
Switch to the Remote NE.

Step 127
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this screen, and each subsequent screen.*

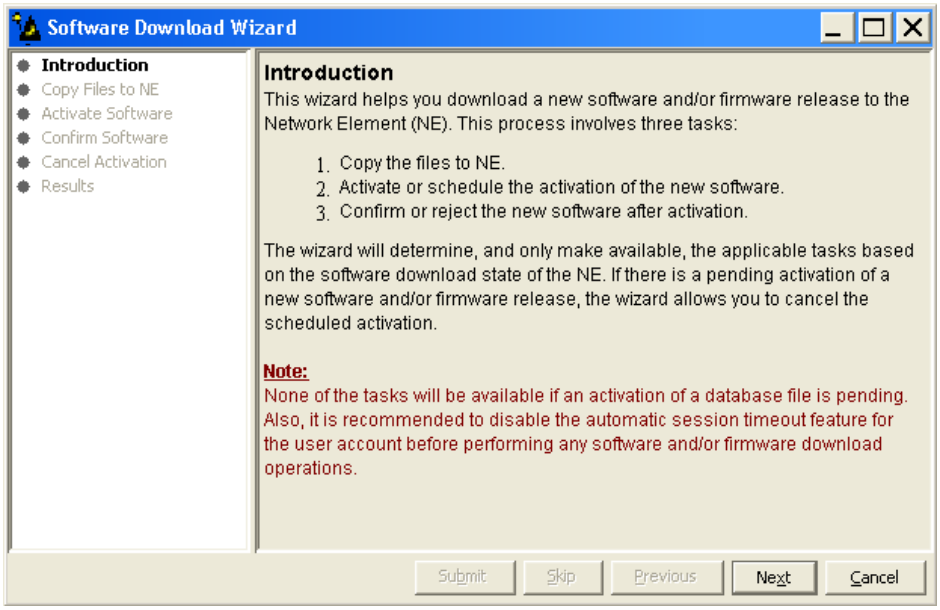


Figure 129: Example Software Download Wizard Introduction Screen

Step 128
Click *Next*.

The *Copy Files to NE* screen appears.

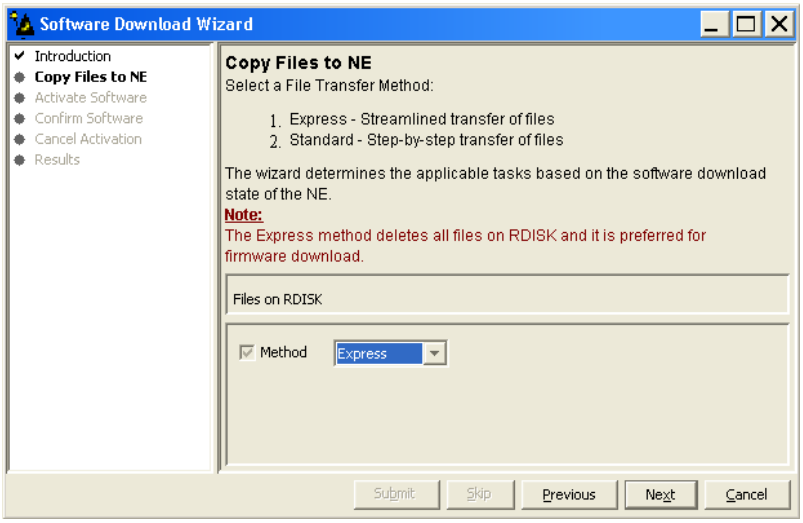


Figure 130: Example Software Download Wizard Copy Files to NE Screen

Step 129
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *The Express method is used to copy the software file from the random access memory disk (RDISK) of the Local NE to the standby nonvolatile memory (SNVM) of the Remote NE. Fujitsu recommends this method because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 130
Click *Next*.

The *Copy Files to RDISK and SNVM* screen appears.

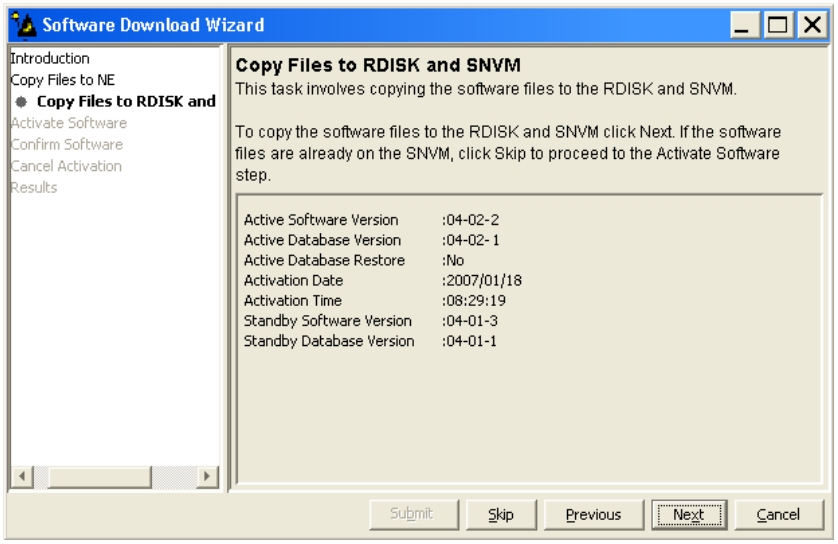


Figure 131: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 131
Click *Next*.

The *Select Host* screen opens.

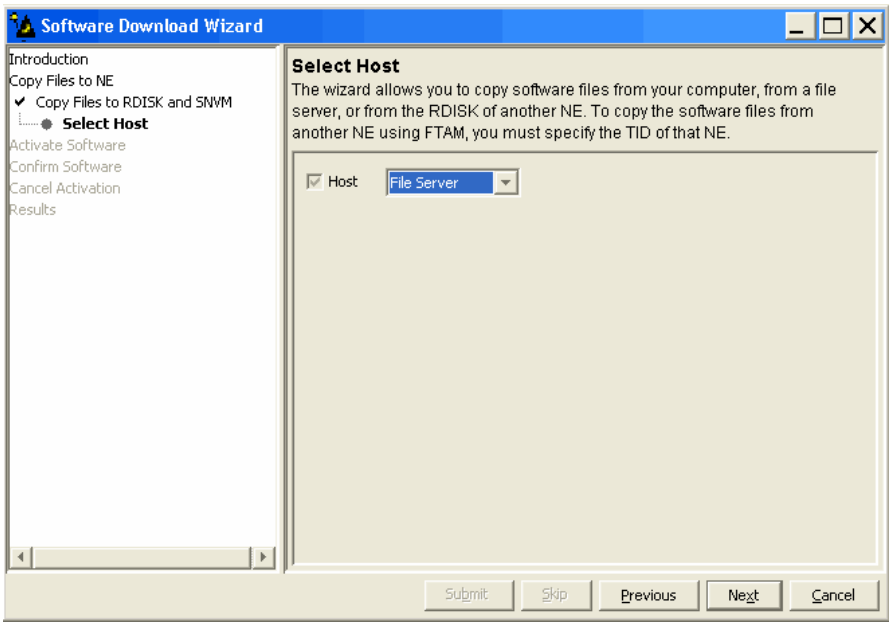


Figure 132: Example Software Download Wizard Select Host Screen

Download Software Program File from Another NE

Step 132
From the *Host* drop-down list, select *Another NE*.

The *Select Host* screen displays an additional field.

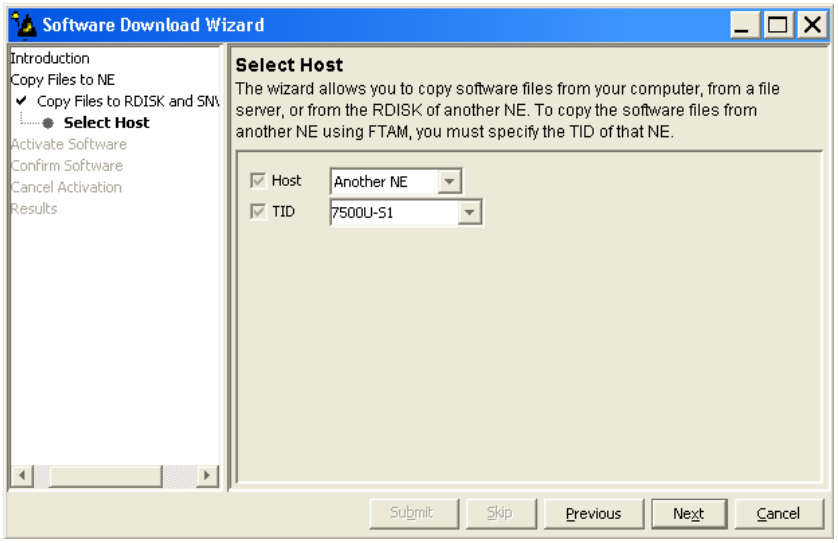


Figure 133: Example Software Download Wizard Select Host–Another NE Selected

Step 133
From the *TID* drop-down list, select the TID of the Local NE.

Step 134
Click *Next*.

The *Select Files* screen appears.

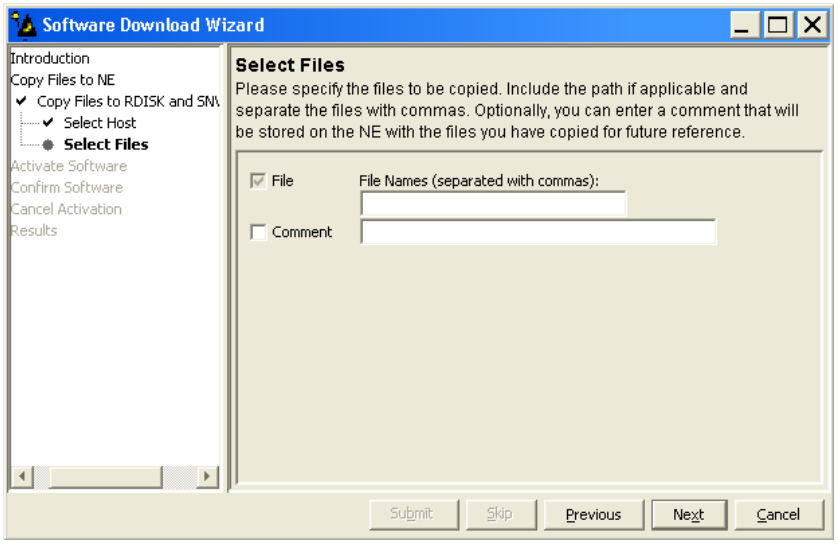


Figure 134: Example Software Download Wizard Select Files Screen

Step 135
In the *File: File Names (separated with commas)* text box, enter the appropriate file name of the software file: `F7504022.PGM`.

Step 136
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 137
Click *Next*.

The *Enter Signatures* screen opens.

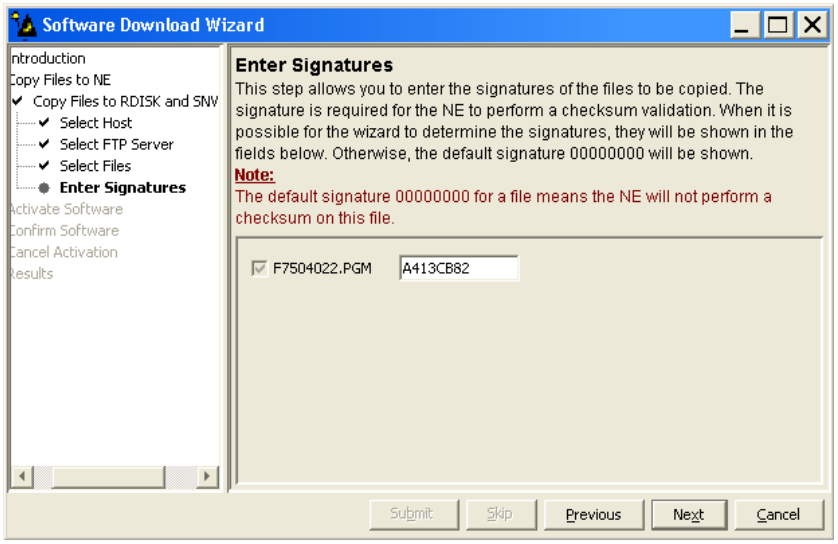


Figure 135: Example Software Download Wizard Enter Signatures Screen

Step 138
Click *Next*.

The *Copy to RDISK and SNVM* screen opens.

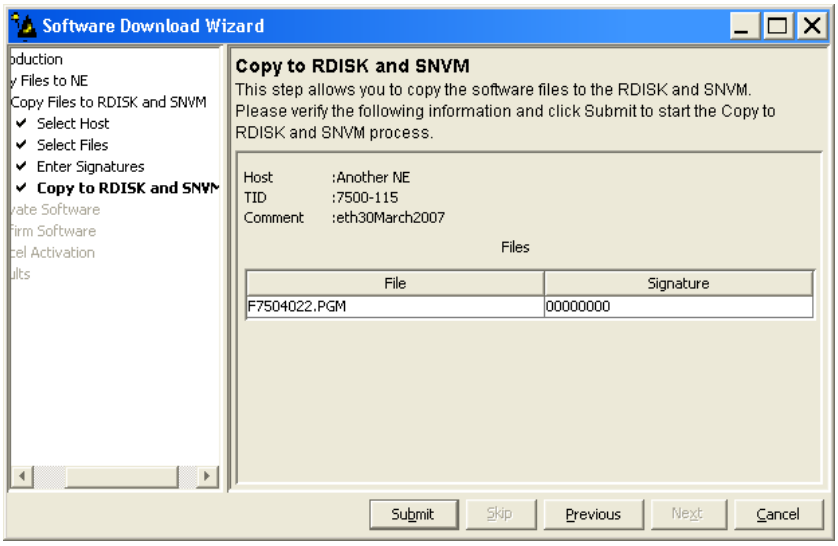


Figure 136: Example Software Download Wizard Copy to RDISK and SNVM Screen

Step 139
Click *Submit*.

A *Performing Copy File* window opens, displaying the progress of the copying for each file (see Figure 76).

Note: *The file may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen opens.

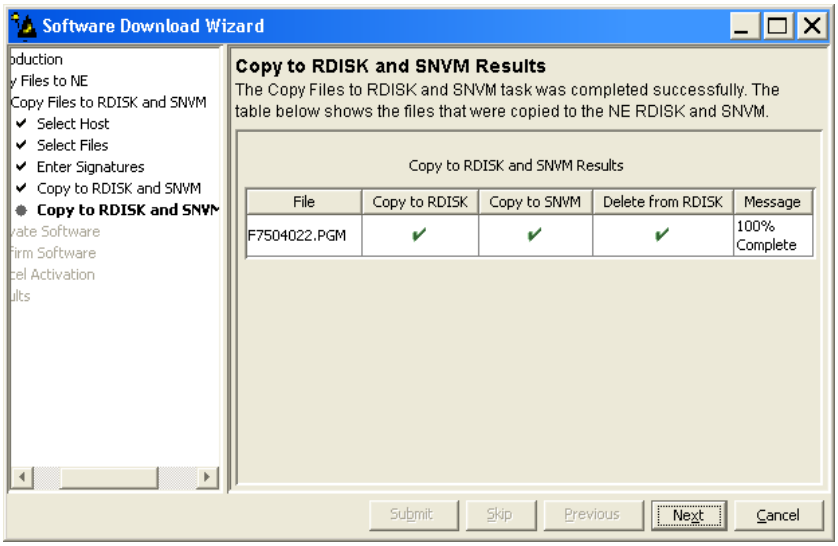


Figure 137: Example Software Download Wizard Copy to RDISK and SNVM Results Screen

Activate Software on Remote NE

Step 140
Click *Next*.

The *Software Activation Parameters* screen opens.

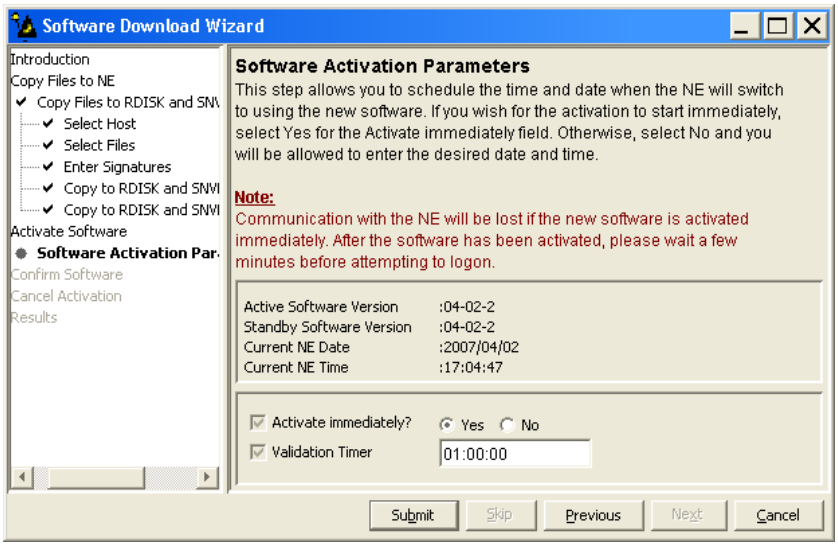


Figure 138: Example Software Download Wizard Software Activation Parameters Screen

Step 141
Do you want to activate the firmware and software immediately?

If YES:
Continue with the next step.

If NO:
Go to Step 148.

Step 142
Verify *Yes* is selected for the *Activate immediately* option.

Step 143
In the *Validation Timer* text box, enter the desired time before the system reverts back to the previous software (the default is 01:00:00 [1 hour]).

Step 144
Click *Submit*.

The *Software Activation Result* screen opens.

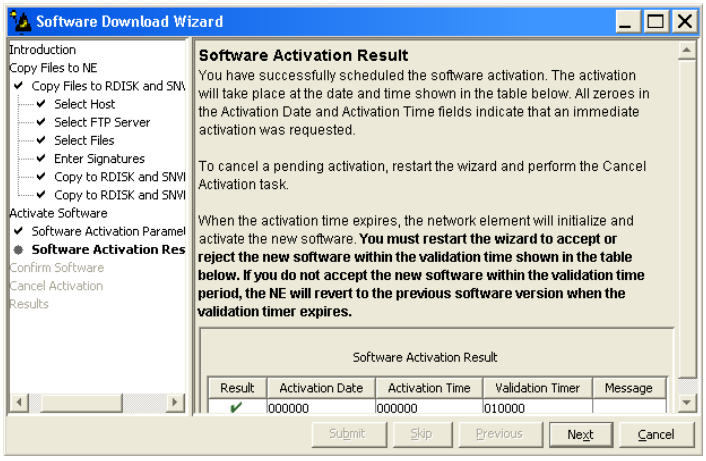


Figure 139: Example Software Download Wizard Software Activation Result Screen

Step 145
Click *Next*.

A *Warning* dialog box opens.

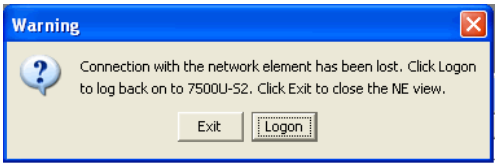


Figure 140: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, a data communication channel failure (DCCFAIL) alarm is raised on the Local NE. The DCCFAIL alarm will clear once the Remote NE resets. You can then log on the Remote NE.*

Step 146
Wait for DCCFAIL alarm to clear on the Local NE, then click *Logon*.

The *Software Activation Result* screen closes, and the Software Download wizard closes.

Step 147
Go to Step 153.

Step 148
Select *No* for the *Activate immediately* option.

The *Software Activation Parameters* screen displays additional fields.

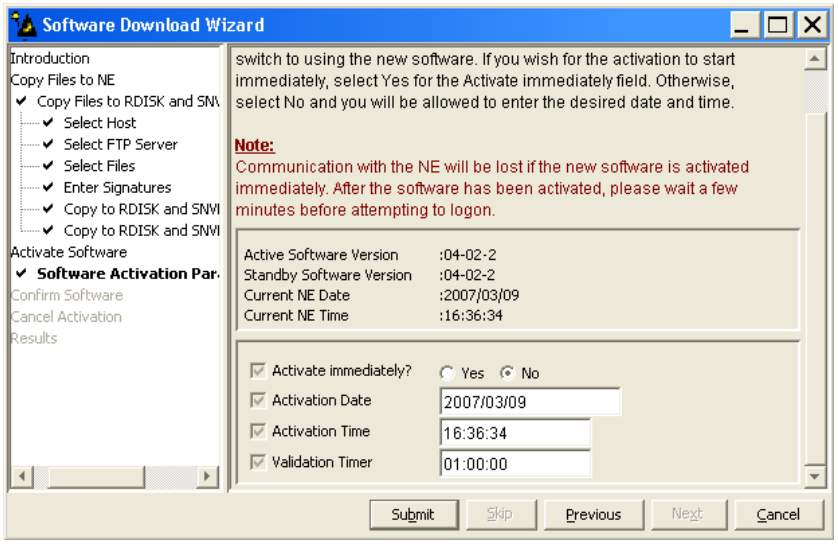


Figure 141: Example Software Activation Parameters–Scheduled Activation

a) Enter the *Activation Date* for the firmware and software activation.

b) Enter the *Activation Time* for the firmware and software activation.

c) Enter the *Validation Time* for the firmware and software activation.

Step 149
Click *Submit*.

The *Software Activation Result* screen opens.

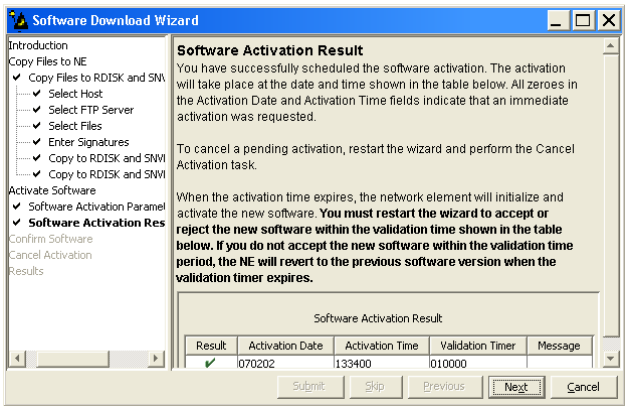


Figure 142: Example Software Download Wizard Software Activation Result Screen

Step 150
Click *Next*.

The *Results* screen opens.

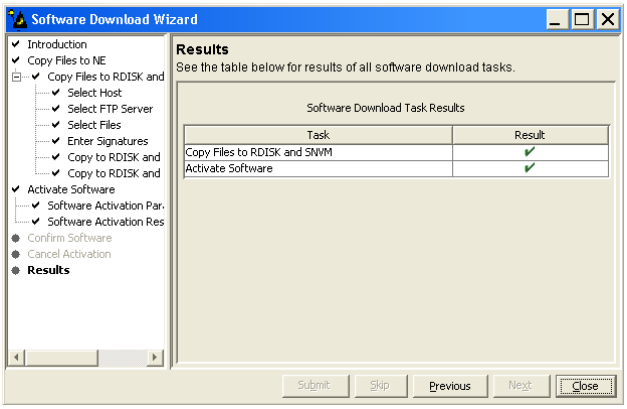


Figure 143: Example Software Download Wizard Results Screen

Step 151
Click *Close*.

The Software Download wizard closes. You may continue working in the NETSMART 500 environment and stay logged on to the Remote NE. When the activation date and time is reached, you are logged off the NE and a *Warning* dialog box appears.

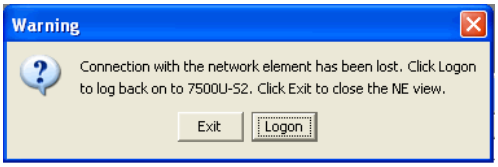


Figure 144: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, a data communication channel failure (DCCFAIL) alarm is raised on the Local NE. The DCCFAIL alarm will clear once the Remote NE resets. You can then log on the Remote NE.*

Step 152
Wait for the DCCFAIL alarm to clear on the Local NE, then click *Logon*.

The NETSMART 500 window closes.

Confirm Software Download

Note: *You must accept the new software load before the validation timer expires. Otherwise, the system software will revert back to the previous load.*

Step 153
Log back on the Remote NE. Refer to Step 3, if necessary.

Note: *Notice that the NOFW condition is cleared.*

Step 154
From the menu bar, select *Wizards* > *Software Download*.

The Software Download wizard starts and the *Introduction* screen opens.

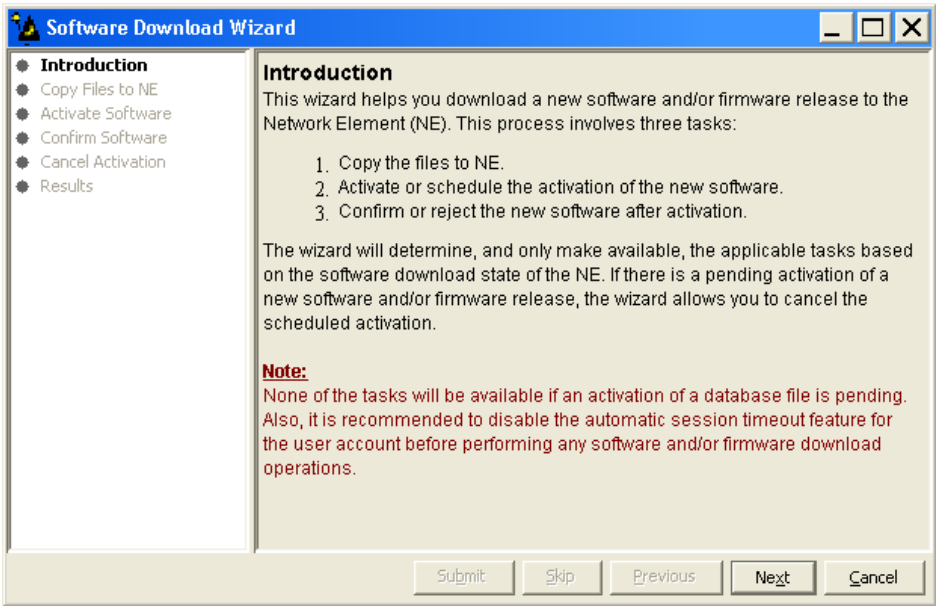


Figure 145: Example Software Download Wizard Introduction Screen

Step 155
Click *Next*.

The *Confirm Software* screen opens.

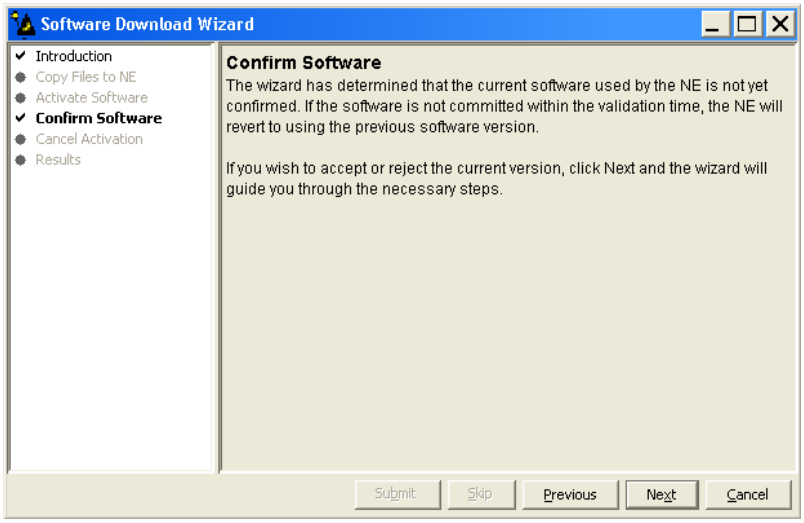


Figure 146: Example Software Download Wizard Confirm Software Screen

Step 156
Click *Next*.

The *Accept/Reject Software* screen opens.

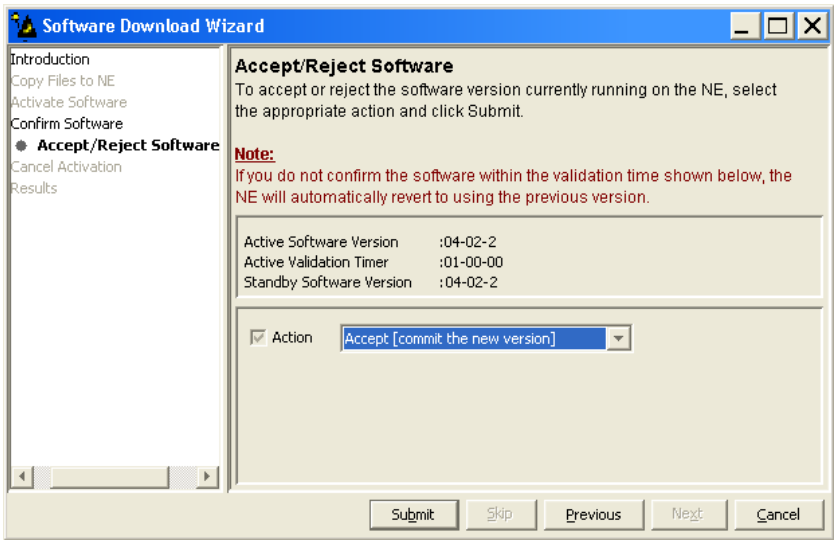


Figure 147: Example Software Download Wizard Accept/Reject Software Screen

Step 157
Verify that the *Accept [commit the new version]* option is selected in the *Action* drop-down list.

Step 158
Click *Submit*.

A progress bar displays while the validation timer is cancelled and the software is accepted.

Once the software is accepted, the *Software Confirmation Result* screen opens.

Note: *The screen may take several minutes to open.*

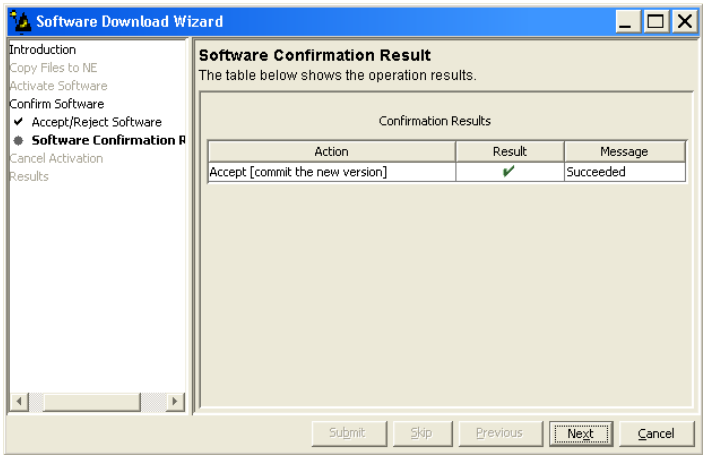


Figure 148: Example Software Download Wizard Software Confirmation Result Screen

Step 159
Click *Next*.

The final *Results* screen opens.

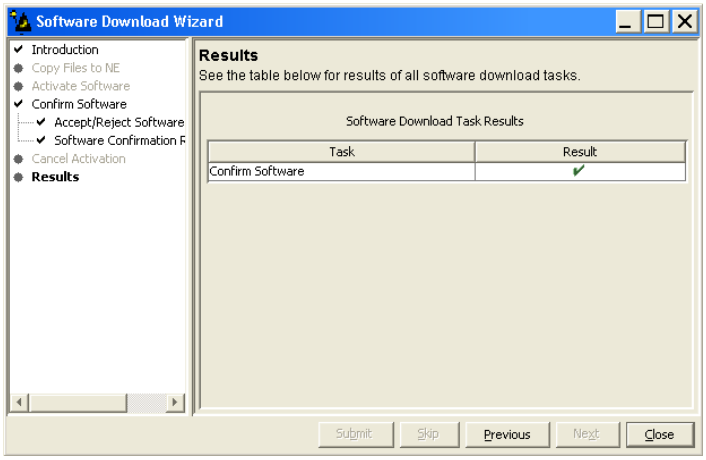


Figure 149: Example Software Download Wizard Results Screen

Step 160
Click *Close*.

The *Results* screen closes and the Software Download wizard closes.

After the system software is activated and the latest firmware file (generic) is downloaded to the system, the system may generate some firmware version mismatch alarms (FVM) against individual plug-in units with incompatible firmware versions.

Step 161
Retrieve alarms and conditions on the NE.

NETSMART 500

NE ▸ *Alarms*

View ▸ *Filter*

Verify that all Fault Types and Severity Levels are selected as reporting.
Click Close.
Close Active Alarms window.

Step 162
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment, for information on clearing FVM alarms). After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

Caution: *Installing new firmware on a plug-in unit programs the programmable hardware on the plug-in unit and can impact traffic associated with the plug-in unit. Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command and should be scheduled at an appropriate time to avoid service interruption. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

If NO:
Proceed to the next step.

Step 163
Log off the NE.

This procedure is complete.

✔ This procedure is complete.

2.5
Upgrading Firmware on Equipment

After the system software is upgraded, the system may generate a firmware version mismatch (FVM) alarm against individual plug-in units with firmware versions that are not compatible with the new system software. The firmware version on plug-in units is not automatically updated during a system software upgrade operation.

If a plug-in unit reports an FVM alarm after a system software upgrade, the firmware on the plug-in unit is incompatible with the new system software and must be upgraded.

Caution: *Upgrading the firmware on a firmware upgradeable unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit at an appropriate time by following local practices.*

The following table lists the firmware downloadable plug-in units for the upgrade from a non-FWDL release to a FWDL release.

Note: *This table shows the most recent issue of the plug-in units shipped from the factory at the time of Release 9.1. The issue number (for example, -I03) indicates the firmware version of the plug-in unit as it left the factory. If a plug-in unit has an earlier issue number, it can still be used in the Release 9.1 system but may need a firmware upgrade to fully support Release 9.1 features.*

Table 10: Firmware Version for Downloadable Units

Unit Name	Part Number	Firmware on Unit
APMA-ASC1	FC9682ASC1-I02	01-01-3
APMA-DRC1	FC9682DRC1-I04	01-01-D
APMA-L2C1	FC9682L2C1-I07	01-01-3
APMA-M2C1	FC9682M2C1-I04	01-01-3
APMA-M2U1	FC9682M2U1-I08	01-01-8
APMA-ULC1	FC9682ULC1-I03	01-01-3
APMA-ULU1	FC9682ULU1-I11	03-01-1
IFMA-8TC1	FC96828TC1-I02	02-01-2
IFMA-8TC2	FC96828TC2-I09	04-01-1
IFMA-GUC1	FC9682GUC1-I17	02-01-2
IFMA-LGB1	FC9682LGB1-I03	01-01-1

Table 10: Firmware Version for Downloadable Units (Cont.)

Unit Name	Part Number	Firmware on Unit
IFMA-BXC1	FC9682BXC1-I05	05-01-4
IFMA-RGC1	FC9682RGC1-I08	03-01-1
IFMA-RGC3	FC9682RGC3-I07	03-01-1
IFMA-U1C1	FC9682U1C1-I10	05-01-3
IFMA-U1C2	FC9682U1C2-I07	03-01-2
IFMA-U2C1	FC9682U2C1-I10	05-01-3
IFMA-U2C2	FC9682U2C2-I03	02-03-1
IFMA-U3C1	FC9682U3C1-I10	05-01-3
IFMA-U3C2	FC9682U3C2-I03	03-01-2
IFMA-U4C1	FC9682U4C1-I03	05-01-3
IFMA-U5C2	FC9682U5C2-I02	01-01-6
IFMA-QUC1	FC9682QUC1-I04	03-01-5
IFMA-QMC1	FC9682QMC1-I04	01-01-C
IFMA-QRC1	FC9682QRC1-I03	01-01-D
IFMA-QUC2	FC9682QUC2	01-01-8
IFMA-QMC2	FC9682QMC2	01-01-7
IFMA-QRC2	FC9682QRC2	01-01-8
IFMA-SMC1	FC9682SMC1-I02	01-01-B
MCMA-RCS1	FC9682RCS1-I05	02-01-1
MDMA-RMC1	FC9682RMC1-I07	01-01-1
MDXP-MDC3	FC9682MDC3-I05	01-01-1
SCMA-SCC4	FC9682SCC4-I09	06-03-1
SFMA-CDC1	FC9682CDC1-I06	01-01-1
SFMA-CMC1	FC9682CMC1-I06	01-01-2
SFMA-RDC1	FC9682RDC1-I03	01-01-2
TCMA-ST31	FC9682ST31-I06	01-01-2

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters.* ***HINT****: Specific information is available by clicking the hyperlinked TL1 command name (for example, ENT-EQPT) in the TL1 column.*

Step 1
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[15]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 2
Retrieve alarms and conditions on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Are any FVM alarms present?

If YES:
Continue with the next step.

[15] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Note: *If any alarms other than FVM, FWFAIL, or FLT are present, clear the alarms before continuing. Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
This procedure is complete.

Step 4
Initialize the alarmed plug-in unit or plug-in units to download and activate program files to the firmware.

TL1	NETSMART 500

`INIT-EQPT:TID:AID:CTAG:::FORCE=Y, OVERWRITE=Y;`
AID:
• Refer to Tables 11 through 12.
Example:
`INIT-EQPT:FUJITSU:OS1-1&OS1-19: CTAG:::FORCE=Y,OVERWRITE=Y;`
	Click the Equipment tab in the tree view.
	Select one or more plug-in units, expanding the tree as necessary.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Operations Dialog*
	Select the Initialize tab.
	Select the Firmware tab.
	Verify that *Yes* is selected for *FORCE*.
	Select *Yes* for *OVERWRITE*.
	Click Initialize.
	A confirmation dialog box opens.
	Click Yes.
	Close the dialog box.

Note: *The firmware can take several minutes to upgrade. The transient condition FWACT will be reported during the upgrade.*

Table 11: Optical Shelf Equipment AIDs for Firmware Downloadable Equipment in Release 4.2

Equipment Name	Equipment Type	Shelf Slot#	AID Format	Equipment AID[16]
Amplifier	APMA-L2C1 APMA-M2C1 APMA-ULC1	1	Shelf#-Slot#	OSn-1
		2		
WSS Core Switch	SFMA-CMC1	3	Shelf#-Slot#	OSn-3
		4		
Mux/Demux	MDMA-RMC1	5	Shelf#-Slot#	OSn-5
		6		

[16] For OSn, n = 1...4

Table 11: Optical Shelf Equipment AIDs for Firmware Downloadable Equipment in Release 4.2 (Cont.)

Equipment Name	Equipment Type	Shelf Slot#	AID Format	Equipment AID[16]
WSS HUB Switch	SFMA-CDC1	7	Shelf#-Slot#	OSn-7
		8		
Optical Supervisory Channel	SCMA-SCC4	9	Shelf#-Slot#	OSn-9
OSC HUB Interconnect	MCMA-RCS1	10	Shelf#-Slot#	OSn-10
Optical Supervisory Channel	SCMA-SCC4	11	Shelf#-Slot#	OSn-11
OSC HUB Interconnect	MCMA-RCS1	12	Shelf#-Slot#	OSn-12
WSS HUB Switch	SFMA-CDC1	13	Shelf#-Slot#	OSn-13
		14		
Mux/Demux	MDMA-RMC1	15	Shelf#-Slot#	OSn-15
		16		
WSS Core Switch	SFMA-CMC1	17	Shelf#-Slot#	OSn-17
		18		
Amplifier	APMA-L2C1 APMA-M2C1 APMA-ULC1	19	Shelf#-Slot#	OSn-19
		20		

Table 12: Tributary Shelf Equipment AIDs for Firmware Downloadable Equipment in Release 4.2

Equipment Name	Equipment Type		Shelf Slot #	AID Format	EquipmentAID[17]
Optical line card (OLC), Regenerator, or FLASHWAVE LIGHTGUARD plug-in unit	Single-wide (any slot): • IFMA-U1 • IFMA-U2 • IFMA-U3 • IFMA-LGB1 • IFMA-RG	Double-wide (odd-numbered slots only): • IFMA-8T • IFMA-8T2 • IFMA-GU • IFMA-RG3 • IFMA-U12 • IFMA-U22 • IFMA-U32	1	Shelf#-Slot#	OSn-1
			2	Shelf#-Slot#	OSn-2
			3	Shelf#-Slot#	OSn-3
			4	Shelf#-Slot#	OSn-4
			5	Shelf#-Slot#	OSn-5
			6	Shelf#-Slot#	OSn-6
			7	Shelf#-Slot#	OSn-7
			8	Shelf#-Slot#	OSn-8
None	n/a		9	Shelf#-Slot#	OSn-9
Sync unit (TCMA-ST31)			10	Shelf#-Slot#	OSn-10

[16] For OSn, n = 1...4
[17] For OSn, n = 10...13, 20...23, 30...33, 40...43, 100, 200, 300, 400

Table 12: Tributary Shelf Equipment AIDs for Firmware Downloadable Equipment in Release 4.2 (Cont.)

Equipment Name	Equipment Type		Shelf Slot #	AID Format	EquipmentAID [17]
None	n/a		11	Shelf#-Slot#	OSn-11
Sync unit (TCMA-ST31)			12	Shelf#-Slot#	OSn-12
OLC, Regenerator, *OR* FLASHWAVE LIGHTGUARD plug-in unit	Single-wide (any slot): • IFMA-U1 • IFMA-U2 • IFMA-U3 • IFMA-LGB1 • IFMA-RG	Double-wide (odd-numbered slots only): • IFMA-8T • IFMA-8T2 • IFMA-GU • IFMA-RG3 • IFMA-U12 • IFMA-U22 • IFMA-U32	13	Shelf#-Slot#	OSn-13
			14	Shelf#-Slot#	OSn-14
			15	Shelf#-Slot#	OSn-15
			16	Shelf#-Slot#	OSn-16
			17	Shelf#-Slot#	OSn-17
			18	Shelf#-Slot#	OSn-18
			19	Shelf#-Slot#	OSn-19
			20	Shelf#-Slot#	OSn-20

Step 5
Verify the firmware is upgraded on the specified plug-in unit or plug-in units.

TL1	NETSMART 500

`RTRV-FWINFO:TID:AID:CTAG;`
AID:
• Refer to Tables 11 through 12.
Example:
`RTRV-FWINFO:FUJITSU:OS1-1&OS1-19:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select the RTRV-FWINFO command from the *Command Name* drop-down list.
	Enter the AID of the unit in the *AID* field.
	Click *Send*.
	Close the TL1 Command Builder dialog box.

Step 6
Retrieve alarms and conditions on the NE.

[17] **For OSn, n = 10...13, 20...23, 30...33, 40...43, 100, 200, 300, 400**

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 7
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Step 8
Log off the NE.

This procedure is complete.

3

Upgrading System Software from Release 4.2 or Later

In this chapter:

3.1 About Release 4.2 or Later System Software Upgrade

This chapter provides instructions to perform the supported software release upgrade path for FLASHWAVE 7500 Release 4.2 or later software as detailed in the following table.

Note: *To upgrade system software prior to Release 4.2, refer to* Upgrading System Software from Release 4.1.

Table 13: Supported Upgrade Paths for Software Release 4.2 and Later

FROM Release	TO Release
Release 4.1.3	Release 4.2 Release 4.2.2
Release 4.2	Release 4.3.3
Release 4.2.2	Release 4.3.3 Release 5.1
Release 4.3.3	Release 5.1
Release 5.1	Release 5.2 Release 5.2.2 Release 6.1 Release 6.1.2 Release 6.1.3
Release 5.2	Release 5.2.2 Release 6.1 Release 6.1.2 Release 6.1.3
Release 5.2.2	Release 6.1 Release 6.1.2 Release 6.1.3 Release 7.1 Release 7.1.3 Release 7.1.4
Release 6.1	Release 6.1.2 Release 6.1.3
Release 6.1.2	Release 6.1.3 Release 7.1 Release 7.1.3 Release 7.1.4 Release 8.1 Release 8.1.2 Release 9.1

Table 13: Supported Upgrade Paths for Software Release 4.2 and Later (Cont.)

FROM Release	TO Release
Release 6.1.3	Release 7.1 Release 7.1.3 Release 7.1.4 Release 8.1 Release 8.1.2 Release 9.1
Release 7.1	Release 7.1.3 Release 7.1.4 Release 8.1 Release 8.1.2 Release 9.1
Release 7.1.3	Release 8.1 Release 8.1.2 Release 9.1
Release 7.1.4	Release 8.1 Release 8.1.2 Release 9.1
Release 8.1	Release 8.1.2 Release 9.1
Release 8.1.2	Release 9.1
Note: *FLASHWAVE 7500 NEs loaded with a software release prior to Release 4 cannot be upgraded to Release 4 or later.* ***Note:*** *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 before being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x, 8.x, or 9.1.*	

Configurations at Release 4.2 or 4.3 cannot be directly upgraded to Release 6.1 or later. For these systems, the procedures in this chapter must be applied twice: first to upgrade to Release 5.1, and then again to upgrade from Release 5.1 to Release 6.1 or later.

Release 8.1 introduces the Firmware Expansion Pack for FLASHWAVE 7500 software. The Expansion Pack allows full support of all FWDL plug-in unit firmware files. The Firmware Expansion Pack also provides future firmware support unrestricted by system processor memory. The Expansion Pack stores the required unit firmware files in the active and standby memory locations on the system processor (MPMA-SHP3/ MPMA-SHP4 and SCMA-SCC4) until they are required, and then the firmware files are downloaded to the appropriate plug-in unit. Refer to Upgrading System Software from Release 4.2 or Later or Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard for information to download Firmware Expansion Pack.

The upgrade procedure does not affect traffic.

Before proceeding with the upgrade procedure, perform or verify the following:

- Ensure that the craft interface device or PC is connected, activated, and set up in the required interface modes as described in Craft and OSS.
- Verify that the user has user privilege code (UPC) Level 4 access and that the automatic time-out option (TMOUTA) is set to N (TL1) or False (NETSMART® 500 network element graphical user interface) as described in System Administration.

Attention: *When Release 7.x, 8.x, or 9.1 software is activated, certain alarms retain the severity setting of the earlier software release. The default severity of the alarms can be changed using the SET-ATTR-<AIDTYPE> command. Refer to the following table.*

Table 14: Default Alarm Severity

Condition Type	Default Alarm Severity					
	Release 4.x	Release 5.x	Release 6.x	Release 7.x	Release 8.x	Release 9.1
CCDOWN	MJ	MN	MN	MN	MN	MN
SONETFLT	NR	NA	NA	NA	NA	NA

3.2 Software Requirements

In this section:

Release 4.2 and 4.3 systems cannot be directly upgraded to Release 6.x or later. For these systems, the procedures in this chapter must be applied twice: first to upgrade to Release 5.1, and then again to upgrade from Release 5.1 to Release 6.x. Upgrading a system to Release 8.1 or later requires a minimum software requirement of Release 6.1.2. This subsection describes the software requirements, software file names, and GISSUE values required for each type of upgrade.

3.2.1 Software Required to Upgrade to Release 5.x

The following table lists the software required to upgrade to Release 5.x.

Table 15: Software Requirements to Upgrade to Release 5.x

Release	Unit	Part Number (CD-ROM)	Description
Release 5.1	CD-ROM	FC9682CR05-I01	FLASHWAVE 7500 Release 5.1 software
Release 5.2	CD-ROM	FC9682CR05-I02	FLASHWAVE 7500 Release 5.2 software
Release 5.2.2	CD-ROM	FC9682CR05-I03	FLASHWAVE 7500 Release 5.2.2 software

The following tables list the system software file names and generic issue (GISSUE) values required to upgrade to Release 5.x.

Table 16: Software File Names and GISSUE Values to Upgrade to Release 5.1

Release	Unit	Value/File Name	Description
Release 5.1	GISSUE	05-01-01	Release 5.1 GISSUE value
	Software generics	F7505011.PGM	Release 5.1 OSL program file
		A7505011.PGM	Release 5.1 firmware program file

Table 16: Software File Names and GISSUE Values to Upgrade to Release 5.1 (Cont.)

Release	Unit	Value/File Name	Description
	Additional software	F7505011.SIG	Release 5.1 signature file
		F7505011.CON	Release 5.1 configuration file
		SWDL.TXT	Release 5.1 software download text file

Table 17: Software File Names and GISSUE Values to Upgrade to Release 5.2

Release	Unit	Value/File Name	Description
Release 5.2	GISSUE	05-02-01	Release 5.2 GISSUE value
	Software generics	F7505021.PGM	Release 5.2 OSL program file
		A7505021.PGM	Release 5.2 firmware program file
	Additional software	F7505021.SIG	Release 5.2 signature file
		F7505021.CON	Release 5.2 configuration file
		SWDL.TXT	Release 5.2 software download text file

Table 18: Software File Names and GISSUE Values to Upgrade to Release 5.2.2

Release	Unit	Value/File Name	Description
Release 5.2.2	GISSUE	05-02-02	Release 5.2.2 GISSUE value
	Software generics	F7505022.PGM	Release 5.2.2 OSL program file
		A7505022.PGM	Release 5.2.2 firmware program file
	Additional software	F7505022.SIG	Release 5.2.2 signature file
		F7505022.CON	Release 5.2.2 configuration file
		SWDL.TXT	Release 5.2.2 software download text file

3.2.2 Software Required to Upgrade to Release 6.x

The following table lists the software required to upgrade to Release 6.x.

Table 19: Software Requirements to Upgrade to Release 6.x

Release	Unit	Part Number (CD-ROM)	Description
Release 6.1	CD-ROM	FC9682CR06-I01	FLASHWAVE 7500 Release 6.1software
Release 6.1.2	CD-ROM	FC9682CR06-I02	FLASHWAVE 7500 Release 6.1.2 software
Release 6.1.3	CD-ROM	FC9682CR06-I03	FLASHWAVE 7500 Release 6.1.3 software

The following tables list the system software file names and generic issue (GISSUE) values required to upgrade to Release 6.x.

Table 20: Software File Names and GISSUE Values to Upgrade to Release 6.1

Release	Unit	Value/File Name	Description
Release 6.1	GISSUE	06-01-01	Release 6.1 GISSUE value
	Software generics	F7506011.PGM	Release 6.1 OSL program file
		A7506011.PGM	First Release 6.1 firmware program file
		B7506011.PGM	Second Release 6.1 firmware program file
	Additional software	F7506011.SIG	Release 6.1 signature file
		F7506011.CON	Release 6.1 configuration file
		SWDL.TXT	Release 6.1 software download text file

Table 21: Software File Names and GISSUE Values to Upgrade to Release 6.1.2

Release	Unit	Value/File Name	Description
Release 6.1.2	GISSUE	06-01-02	Release 6.1.2 GISSUE value
	Software generics	F7506012.PGM	Release 6.1.2 OSL program file
		A7506012.PGM	First Release 6.1.2 firmware program file
		B7506012.PGM	Second Release 6.1.2 firmware program file
	Additional software	F7506012.SIG	Release 6.1.2 signature file
		F7506012.CON	Release 6.1.2 configuration file
		SWDL.TXT	Release 6.1.2 software download text file

Table 22: Software File Names and GISSUE Values to Upgrade to Release 6.1.3

Release	Unit	Value/File Name	Description
Release 6.1.3	GISSUE	06-01-03	Release 6.1.3 GISSUE value
	Software generics	F7506013.PGM	Release 6.1.3 OSL program file
		A7506013.PGM	First Release 6.1.3 firmware program file
		B7506013.PGM	Second Release 6.1.3 firmware program file
	Additional software	F7506013.SIG	Release 6.1.3 signature file
		F7506013.CON	Release 6.1.3 configuration file
		SWDL.TXT	Release 6.1.3 software download text file

3.2.3 Software Required to Upgrade to Release 7.x

The following table lists the software required to upgrade to Release 7.x.

Table 23: Software Requirements to Upgrade to Release 7.x

Release	Unit	Part Number (CD-ROM)	Description
Release 7.1	CD-ROM	FC9682CR07-I01	FLASHWAVE 7500 Release 7.1 software
Release 7.1.3	CD-ROM	FC9682CR07-I03	FLASHWAVE 7500 Release 7.1.3 software
Release 7.1.4	CD-ROM	FC9682CR07-I04	FLASHWAVE 7500 Release 7.1.4 software

The following tables list the system software file names and generic issue (GISSUE) values required to upgrade to Release 7.x.

Table 24: Software File Names and GISSUE Values to Upgrade to Release 7.1

Release	Unit	Value/File Name	Description
Release 7.1	GISSUE	07-01-02	Release 7.1 GISSUE value
	Software generics	F7507012.PGM	Release 7.1 OSL program file
		A7507012.PGM	First Release 7.1 firmware program file
		B7507012.PGM	Second Release 7.1 firmware program file
		C7507012.PGM	Third Release 7.1 firmware program file
	Additional software	F7507012.SIG	Release 7.1 signature file

Table 24: Software File Names and GISSUE Values to Upgrade to Release 7.1 (Cont.)

Release	Unit	Value/File Name	Description
		F7507012.CON	Release 7.1 configuration file
		SWDL.TXT	Release 7.1 software download text file

Table 25: Software File Names and GISSUE Values to Upgrade to Release 7.1.3

Release	Unit	Value/File Name	Description
Release 7.1.3	GISSUE	07-01-03	Release 7.1.3 GISSUE value
	Software generics	F7507013.PGM	Release 7.1.3 OSL program file
		A7507013.PGM	First Release 7.1.3 firmware program file
		B7507013.PGM	Second Release 7.1.3 firmware program file
		C7507013.PGM	Third Release 7.1.3 firmware program file
	Additional software	F7507013.SIG	Release 7.1.3 signature file
		F7507013.CON	Release 7.1.3 configuration file
		SWDL.TXT	Release 7.1.3 software download text file

Table 26: Software File Names and GISSUE Values to Upgrade to Release 7.1.4

Release	Unit	Value/File Name	Description
Release 7.1.4	GISSUE	07-01-04	Release 7.1.4 GISSUE value
	Software generics	F7507014.PGM	Release 7.1.4 OSL program file
		A7507014.PGM	First Release 7.1.4 firmware program file
		B7507014.PGM	Second Release 7.1.4 firmware program file
		C7507014.PGM	Third Release 7.1.4 firmware program file
	Additional software	F7507014.SIG	Release 7.1.4 signature file
		F7507014.CON	Release 7.1.4 configuration file
		SWDL.TXT	Release 7.1.4 software download text file

3.2.4 Software Required to Upgrade to Release 8.x

The following table lists the software required to upgrade to Release 8.x.

Table 27: Software Requirements to Upgrade to Release 8.x

Release	Unit	Part Number (CD-ROM)	Description
Release 8.1	CD-ROM	FC9682CR08-I01	FLASHWAVE 7500 Release 8.1 software
Release 8.1.2	CD-ROM	FC9682CR08-I02	FLASHWAVE 7500 Release 8.1.2 software

The following tables list the system software file names and generic issue (GISSUE) values required to upgrade to Release 8.x.

Table 28: Software File Names and GISSUE Values to Upgrade to Release 8.1

Release	Unit	Value/File Name	Description
Release 8.1	GISSUE	08-01-1	Release 8.1 GISSUE value
	Software generics	F7508011.PGM	Release 8.1 OSL program file
		A7508011.PGM	First Release 8.1 firmware program file
		B7508011.PGM	Second Release 8.1 firmware program file
		C7508011.PGM	Third Release 8.1 firmware program file
	Additional software	F7508011.SIG	Release 8.1 signature file
		F7508011.CON	Release 8.1 configuration file
		SWDL.TXT	Release 8.1 software download text file

Table 29: Software File Names and GISSUE Values to Upgrade to Release 8.1.2

Release	Unit	Value/File Name	Description
Release 8.1.2	GISSUE	08-01-02	Release 8.1.2 GISSUE value
	Software generics	F7508012.PGM	Release 8.1.2 OSL program file
		A7508012.PGM	First Release 8.1.2 firmware program file
		B7508012.PGM	Second Release 8.1.2 firmware program file
		C7508012.PGM	Third Release 8.1.2 firmware program file
	Additional software	F7508012.SIG	Release 8.1.2 signature file
		F7508012.CON	Release 8.1.2 configuration file
		SWDL.TXT	Release 8.1.2 software download text file

The following tables list the Expansion Pack file names for Release 8.x

Attention: *If the Expansion Pack files are downloaded, always download the Z750xxxx.CON file first.*

Table 30: Expansion Pack File Names for Release 8.1

Release	Unit	Value/File Name	Description
Release 8.1	Expansion Pack Software Files	Z7508011.CON	Release 8.1 Expansion Pack configuration file
		Z7508011.PGM	Release 8.1 Expansion Pack firmware program file
		Z7508011.SIG	Release 8.1 Expansion Pack signature file

Table 31: Expansion Pack File Names for Release 8.1.2

Release	Unit	Value/File Name	Description
Release 8.1.2	Expansion Pack Software Files	Z7508012.CON	Release 8.1.2 Expansion Pack configuration file
		Z7508012.PGM	Release 8.1.2 Expansion Pack firmware program file
		Z7508012.SIG	Release 8.1.2 Expansion Pack signature file

3.2.5 Software Required to Upgrade to Release 9.1

The following table lists the software required to upgrade to Release 9.1.

Table 32: Software Requirements to Upgrade to Release 9.1

Release	Unit	Part Number (CD-ROM)	Description
Release 9.1	CD-ROM	FC9682CR09-I01	FLASHWAVE 7500 Release 9.1 software

The following table lists the system software file names and generic issue (GISSUE) values required to upgrade to Release 9.1.

Table 33: Software File Names and GISSUE Values to Upgrade to Release 9.1

Release	Unit	Value/File Name	Description
Release 9.1	GISSUE	09-01-1	Release 9.1 GISSUE value
	Software generics	F7509011.PGM	Release 9.1 OSL program file

Table 33: Software File Names and GISSUE Values to Upgrade to Release 9.1 (Cont.)

Release	Unit	Value/File Name	Description
		A7509011.PGM	First Release 9.1 firmware program file
		B7509011.PGM	Second Release 9.1 firmware program file
		C7509011.PGM	Third Release 9.1 firmware program file
	Additional software	F7509011.SIG	Release 9.1 signature file
		F7509011.CON	Release 9.1 configuration file
		SWDL.TXT	Release 9.1 software download text file

The following table lists the Expansion Pack file names for Release 9.1.

Attention: *If the Expansion Pack files are downloaded, always download the Z750xxxx.CON file first.*

Table 34: Expansion Pack File Names for Release 9.1

Release	Unit	Value/File Name	Description
Release 9.1	Expansion Pack Software Files	Z7509011.CON	Release 9.1 Expansion Pack configuration file
		Z7509011.PGM	First Release 9.1 Expansion Pack firmware program file
		Y7509011.PGM	Second Release 9.1 Expansion Pack firmware program file
		Z7509011.SIG	Release 9.1 Expansion Pack signature file

3.3 Upgrading System Software Using TL1 Commands

In this section:

The following figure shows a flowchart for the subprocedure.

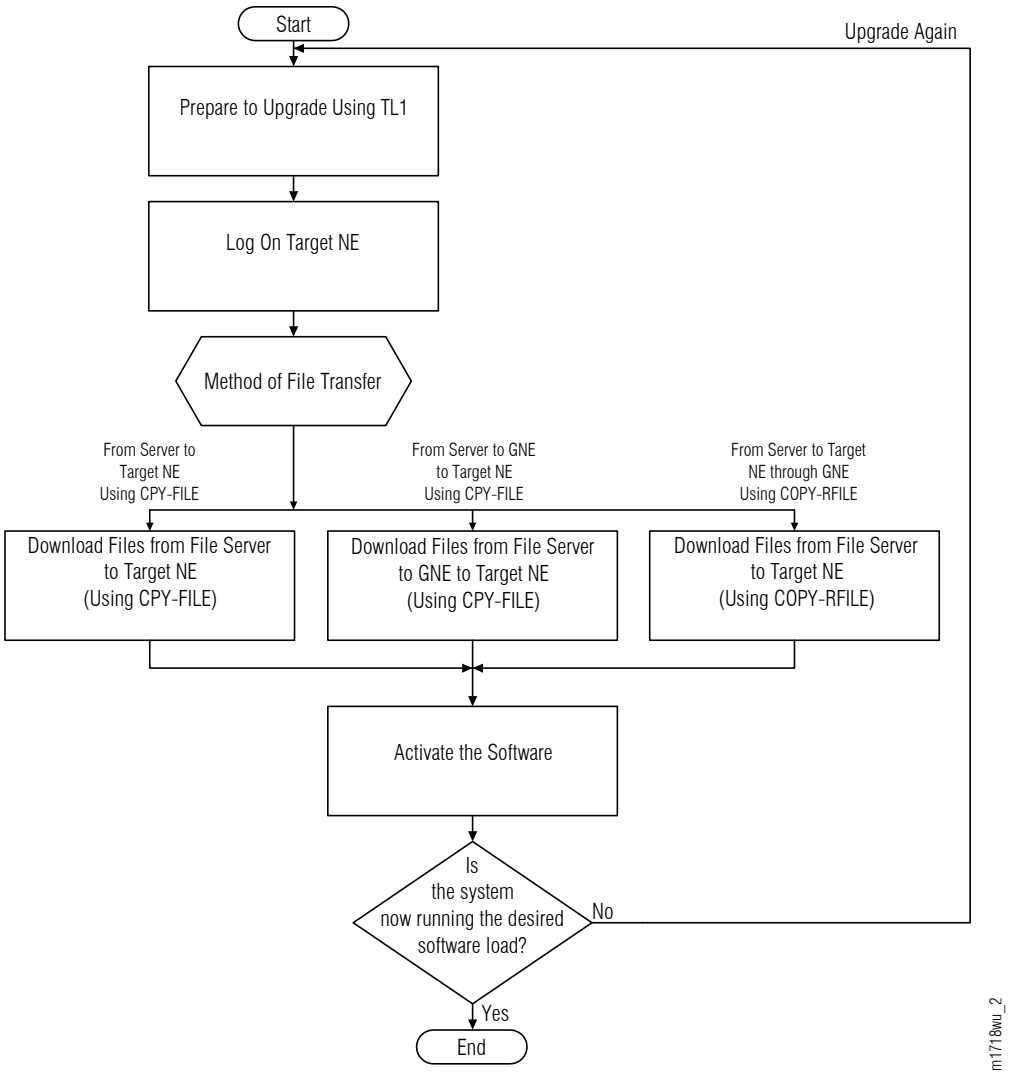


Figure 150: Upgrading System Software Using TL1 Commands (Procedure Flowchart)

Caution: *Do not use this procedure to upgrade systems prior to Release 4.2. To upgrade these systems, refer to Upgrading System Software from Release 4.1 before performing the upgrade to Release 6.1 or later.*

Caution: *After the system software has been upgraded and the latest firmware file (generic) containing the firmware loads for each plug-in unit has been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the TL1 command INIT-EQPT at an appropriate time by following local practices. For more details, refer to Maintenance.*

Caution: *In Release 5.1 of the FLASHWAVE 7500 system, support is discontinued for all 4-channel OLCs except IFMA-SBxx plug-in units (Refer to the following table). Also, support is discontinued for redundant processors introduced in Release 4.2. Ensure that the system to be upgraded does not include any 4-channel OLCs, except IFMA-SB plug-in units, prior to upgrading system software to Release 5.1 and later.*

Table 35: 4-Channel OLCs Not Supported in Release 5.1 and Later

Plug-In Unit
IFMA-8Txx, excluding IFMA-8TC1 and IFMA-8TC2
IFMA-GUxx, excluding IFMA-GUC1
IFMA-HGxx, excluding IFMA-HGC1
IFMA-HLxx, excluding IFMA-HLC1
IFMA-LExx, excluding IFMA-LEC1
IFMA-LLxx, excluding IFMA-LLC1
IFMA-SAxx

Attention: *The procedures in this section are used to download the required files for a system upgrade. These files include the configuration file (F75xxxxx.CON), program file (F75xxxxx.PGM), and native firmware files (A75xxxxx.PGM, B75xxxxx.PGM, and C75xxxxx.PGM). If system software is upgraded to Release 8.1 or later, the Expansion Pack firmware files will also need to be downloaded. After a successful system upgrade to Release 8.1 or later, refer to* Download Firmware Expansion Pack Files Using TL1Commands *or* Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard *to download the Expansion Pack firmware files.*

Software Download Prerequisites

Configurations

To perform software download, connections must exist for file transfer between the node and the file server (repository for software files). The two basic configurations are:

- Configuration 1—The file server connects to the target node through the IP network (see the following figure).

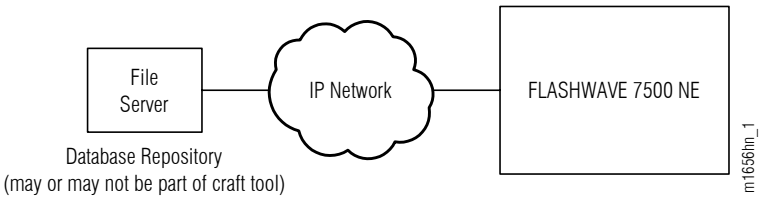


Figure 151: Configuration 1–File Server Connects to Target Node through IP

- Configuration 2– The file server connects to the gateway network element (GNE) through the IP network, and the GNE connects to the target node through SDCC (see the following figure).

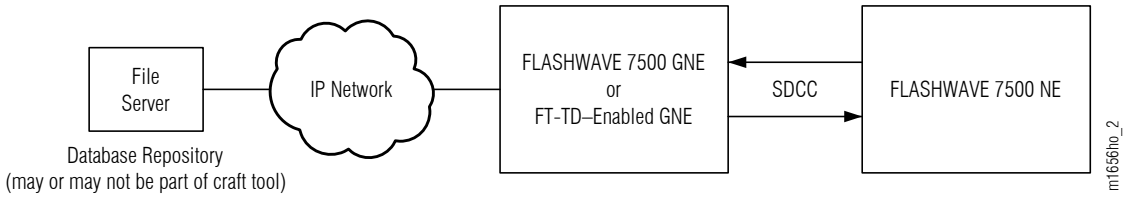


Figure 152: Configuration 2–File Server Connects to GNE through IP, and GNE Connects to Target Node through SDCC

Methods of File Transfer

The FLASHWAVE® 7500 system supports three methods of file transfer. The following table lists the three methods along with the applicable configuration and prerequisites. The procedures in this chapter accommodate all three methods of file transfer.

Table 36: File Transfer Prerequisites

File Transfer Method	Configuration	Prerequisites
File transfer through IP connection using CPY-FILE	Configuration 1 Figure 151	• IP connection between file server and target NE
One-step FT-TD file transfer through GNE using COPY-RFILE	Configuration 2 Figure 152	• IP connection between file server and GNE • SDCC connection between GNE and target NE • GNE is FT-TD enabled. • System software on target NE is Release 5.2 or greater.
Two-step file transfer through GNE using CPY-FILE	Configuration 2 Figure 152	• IP connection between file server and GNE • SDCC connection between GNE and target NE

All releases of the FLASHWAVE 7500 system support file transfer using the CPY-FILE command. Starting with Release 5.2, the FLASHWAVE 7500 system also supports file transfer using the COPY-RFILE command, which implements File Transfer–Translation Device (FT-TD) protocol.

In Configuration 2 applications (Figure 152), the FT-TD method of file transfer is more efficient because file transfer can be accomplished with a single COPY-RFILE command instead of two CPY-FILE commands. Additionally, if COPY-RFILE is used, the GNE may be any FT-TD–enabled gateway NE, not necessarily a FLASHWAVE 7500 NE.

Prerequisites

Before proceeding with this procedure, do the following:

- Select a method of file transfer (Methods of File Transfer) and verify that the prerequisites listed in Table 36 for the chosen method of file transfer are satisfied.
- Ensure that the craft tool is connected and able to log on the target NE. (Refer to Craft and OSS.)

  Note: *If the craft tool connection is through the serial port, the file server must be separate from the craft tool.*
- Verify that the user has user privilege code (UPC) Level 4 access and that the automatic time-out option is set to No as described in Craft and OSS.

3.3.1 Prepare to Upgrade Using TL1

Use this procedure to copy software files from the CD-ROM to the File Transfer Protocol (FTP) server and to collect information about the FTP server in preparation for performing the procedure in Upgrading System Software Using TL1 Commands.

Step 1
Obtain the appropriate CD-ROM, and read the Software Release notes that are packaged on the CD-ROM along with the software files.

If your system is currently running Release 4.2 or 4.3 software, obtain the CD-ROM specified in Table 15. If your system is running Release 5.1 or later, obtain the CD-ROM specified in Table 19.

Step 2
Ensure that an FTP server is set up and available on the craft interface PC, or on another computer, that is available to the FLASHWAVE® 7500 NE through the local management port (LMP) or local communication network (LCN) port.

Note: *If the FTP server connection is through the LMP port, the Transmission Control Protocol/Internet Protocol (TCP/IP) settings of the FTP server must be set to match those listed in* Table: Craft Interface Set Up Procedures *in* Setting Up Craft Interface (TL1 Session through TERM2).

Note: *For instructions on setting up the LCN port, refer to* Setting Up OSS Operations.

Step 3
Record the IP address of the FTP server.

Note: *If the FTP server resides on the craft interface PC, the IP address of the FTP server is the same as the IP address of the craft interface PC.*

Note: *Enter this IP address as the value of SRC in* Download Files from File Server to Target NE (Using CPY-FILE).

```
139.145.23.43
```

Step 4
Record the user name and password to be used for accessing the FTP server.

Note: *The user name and password will be entered as values for keywords FTUID and FTPID in* Download Files from File Server to Target NE (Using CPY-FILE).

```
UID=swdluser, PID=moonrock
```

Step 5
On the FTP server, create a new directory (or locate an existing directory) to contain the software files.

Step 6
Record the path to the directory created (or located) in the previous step.

Note: *The path will be entered as the value of keyword FTPATH in* Download Files from File Server to Target NE (Using CPY-FILE).

```
C:\GENERICS
```

Step 7
Copy the appropriate files required for the specific software upgrade listed in the Software Requirements section from the CD-ROM to the directory you created (or identified) in Step 5.

Step 8
Continue to Log On Target NE.

3.3.2
Log On Target NE

Log on the target NE as follows:

Note: *Default values are shown in bold.*

Step 1
Ensure that the NEM shelf Processor and OSC plug-in units are inserted in the target NE and that the target NE is ready to be upgraded.

Step 2
Ensure that the system does not include any 4-channel OLCs, except IFMA-SB plug-in units. Refer to Upgrading System Software Using TL1 Commands.

Step 3
Close all unrelated applications currently running on your craft interface or PC, and disable the PC screen saver and power save options, if enabled.

Step 4
Log on the target NE.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to N. Refer to* About Release 4.2 or Later System Software Upgrade.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values. The TID, UID, and PID values are not case-sensitive.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For detailed information, refer to* Craft Interface Operations .

TL1

Start a terminal or terminal emulator program (for example, HyperTerminal®).

For **TERM1** (Serial):	For **TERM2** (TCP/IP):
Press CTRL+X.	Establish a Telnet session using IP address 192.168.1.1 and default port 23.
The Welcome screen opens. Press 3 for TL1.	

TL1

```
ACT-USER:TID:UID:CTAG::PID;
```

TID:

- FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)

UID:

- ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)

PID:

- ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)

Example:

```
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;
```

Step 5

Retrieve alarms and conditions on the target NE.

TL1

```
RTRV-COND-ALL:TID::CTAG;
```

Example:

```
RTRV-COND-ALL:FUJITSU::CTAG;
```

Step 6

Are any active alarms or conditions being reported on the target NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Step 7

Choose a method of file transfer and proceed as indicated:

File Transfer Method	Prerequisites	Proceed to
File transfer through IP connection using CPY-FILE	• IP connection between file server and target NE	Download Files from File Server to Target NE (Using CPY-FILE)

File Transfer Method	Prerequisites	Proceed to
One-step FT-TD file transfer through GNE using COPY-RFILE	• IP connection between file server and GNE • SDCC connection between GNE and target NE • GNE is FT-TD enabled • System software on target NE is Release 5.2 or greater	Download Files from File Server to Target NE (Using COPY-RFILE)
Two-step file transfer through GNE using CPY-FILE	• IP connection between file server and GNE • SDCC connection between GNE and target NE	Download Files from File Server to GNE to Target NE (Using CPY-FILE)

Note: *For background information, refer to* Upgrading System Software Using TL1 Commands.

3.3.3
Download Files from File Server to Target NE (Using CPY-FILE)

The following figure shows a flowchart for the subprocedure.

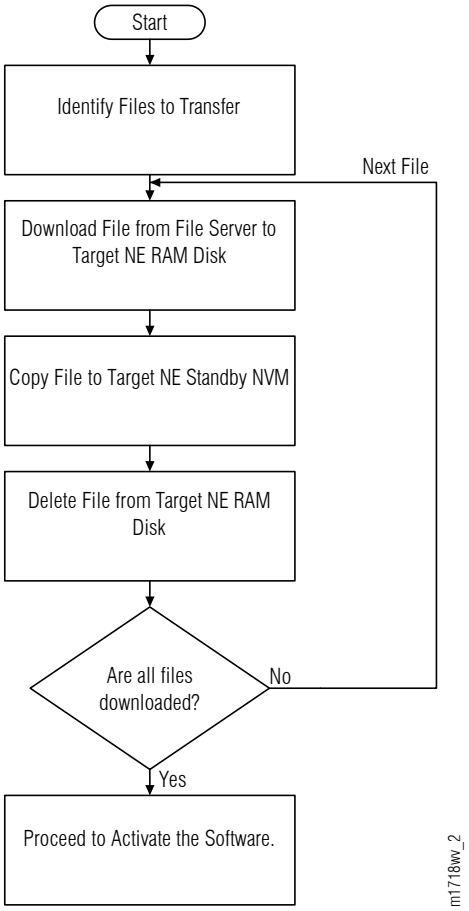


Figure 153: Download Files from File Server to Target NE (Using CPY-FILE) (Subprocedure Flowchart)

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

Before starting this procedure, complete all steps in Prepare to Upgrade Using TL1. The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–*

related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Download files to target NE as follows:

Note: *Default values are shown in bold.*

Identify Files to Transfer

Step 1
Identify and record the configuration, program, and firmware files to download. Refer to the tables in the Software Requirements section for the required system software files required for a specific software upgrade. The following table provides an example of the required software file names:

Example:

Release	Configuration File	Program File	Firmware File(s)
Release 9.1	F7509011.CON	F7509011.PGM	A7509011.PGM B7509011.PGM C7509011.PGM

Step 2
From the set of files identified in the previous step, select a file that has not yet been downloaded.

Note: *Start with any file in the set. The procedure will be performed once for each file to be downloaded.*

Download File from File Server to Target NE RAM Disk

Step 3
Copy the file identified in the previous step from the FTP server to the RAM disk of the target NE.

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction)
- This is the file, identified in the previous step, that you are currently downloading.

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to the following table.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU:139.145.23.43,F7507012.CON,RDISK,F7507012.CON:CTAG:::
OVERWRITE=Y,FTUID=\"swduser\",FTPID=\"moonrock\",FTPATH=\"C:\GENERICS\";
```

Table 37: CPY-FILE Keyword and Domain Input Parameters

Keyword	Domain (Default in Bold)	Description
OVERWRITE[18]	Overwrite files	
	Y	Write over files with the same name at DST
	N	Do not write over files with the same name at DST
COMMENT	\"xxxxx\" **null**	Sets the user-defined comment, where the comment is up to 60 ASCII characters delineated by escape quotes ***Note:*** *The CPY-FILE command is denied if the COMMENT keyword exceeds 60 characters.*
SIGNATURE[19]	8 hex digits **00000000**	Signature code for each file. When more than one file is transferred, signatures are separated with an & character. ***Note:*** *If SIGNATURE is 0 (zero), the file checksum will not be performed.*

[18] OVERWRITE=Y must be specified when transferring a file from the FLASHWAVE 7500 NE to another location when using FTP or FTAM.
[19] The SIGNATURE keyword is ignored when transferring a file from the NE to any other location.

Table 37: CPY-FILE Keyword and Domain Input Parameters (Cont.)

Keyword	Domain (Default in Bold)	Description
FTUID	\"xxxxx\" **null**	UID used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPID	\"xxxxx\" **null**	Password used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPATH	\"xxxxx\" **null**	Path to the control file on the server; up to 40 ASCII characters delineated by escape quotes

Step 4
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Copy File to Target NE Standby NVM

Step 5
Copy the file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- CON (configuration file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,F7507012.CON,STBY,:CTAG::CON:
COMMENT=\"RELEASE_6.1\";
```

Step 6
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Delete File from Target NE RAM Disk

Step 7
Delete the file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
DLT-FILE:FUJITSU:F7507012.CON:CTAG;
```

Step 8
Have you downloaded all files identified in Step 1?

If YES:
Proceed to Activate the Software.

If NO:
Repeat this procedure to download the next file.

✔ This procedure is complete.

3.3.4 Download Files from File Server to Target NE (Using COPY-RFILE)

The following figure shows a flowchart for the subprocedure.

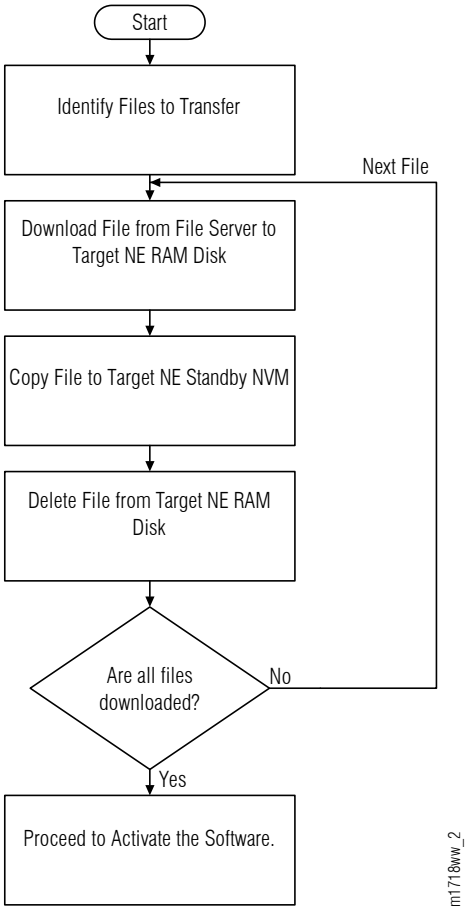


Figure 154: Download Files from File Server to Target NE (Using COPY-RFILE) (Subprocedure Flowchart)

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

Before starting this procedure, complete all steps in Prepare to Upgrade Using TL1. The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–*

related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Download files to target NE as follows:

Note: *Default values are shown in bold.*

Step 1
Verify that active software load is Release 5.2 or greater (GISSUE is 05-02-01 or greater).

TL1

```
RTRV-VERSION:TID::CTAG;
```

Example:
```
RTRV-VERSION:FUJITSU::CTAG;
```

Step 2
Is the active GISSUE value 05-02-01 or higher?

If YES:
Proceed to Step 3.

If NO:
The target node does not support the COPY-RFILE command. Return to Step 7 of Log On Target NE, and choose a different method of file transfer.

Identify Files to Transfer

Step 3
Identify and record the configuration, program, and firmware files to download. Refer to the tables in the Software Requirements section for the required system software files required for a specific software upgrade. The following table provides an example of the required software file names:

Example:

Release	Configuration File	Program File	Firmware File(s)
Release 9.1	F7509011.CON	F7509011.PGM	A7509011.PGM B7509011.PGM C7509011.PGM

Step 4
From the set of files identified in the previous step, select a file that has not yet been downloaded.

Note: *Start with any file in the set. This procedure will be performed once for each file to be downloaded.*

Download File from File Server to Target NE RAM Disk

Step 5
Copy the file identified in the previous step from the FTP server to the RAM disk of the target NE.

TL1

```
COPY-RFILE:TID::CTAG::SWDL,SRCURL,DESTURL,OVERWRITE,FTTDURL;
```

TID:

- Target node SID (not GNE)

SRCURL:

- \"xxxxx\" (URL of the source file on remote file server)
- This is the file, identified in the previous step, that you are currently downloading.

DESTURL:

- \"xxxxx\" (URL of file destination on target node RAM disk)

OVERWRITE:

- YES/**NO**

FTTDURL

- \"xxxxx\" (URL of FT-TD server, GNE)

Example:

```
COPY-RFILE:FUJITSU::CTAG::SWDL,
\"ftp://user1:password1@139.145.23.43/C:\GENERICS\F7507012.CON\",
\"file:///F7507012.CON\",YES,\"fttd://user1:password1@FUJITSU-GNE\";
```

Step 6
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- File name of source file specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Copy File to Target NE Standby NVM

Step 7
Copy the file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- File name of source file specified in previous step

FTYPE:

- CON (configuration file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,F7507012.CON,STBY,:CTAG::CON:
COMMENT=\"RELEASE_6.1\";
```

Step 8
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- File name of source file specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Delete File from Target NE RAM Disk

Step 9
Delete the file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- File name of source file specified in previous step
- **ALL** (null)

Example:

```
DLT-FILE:FUJITSU:F7507012.CON:CTAG;
```

Step 10
Have you downloaded all files identified in Step 3?

If YES:
Proceed to Activate the Software.

If NO:
Repeat this procedure to download the next file.

✔ This procedure is complete.

3.3.5 Download Files from File Server to GNE to Target NE (Using CPY-FILE)

The following figure shows a flowchart for the subprocedure.

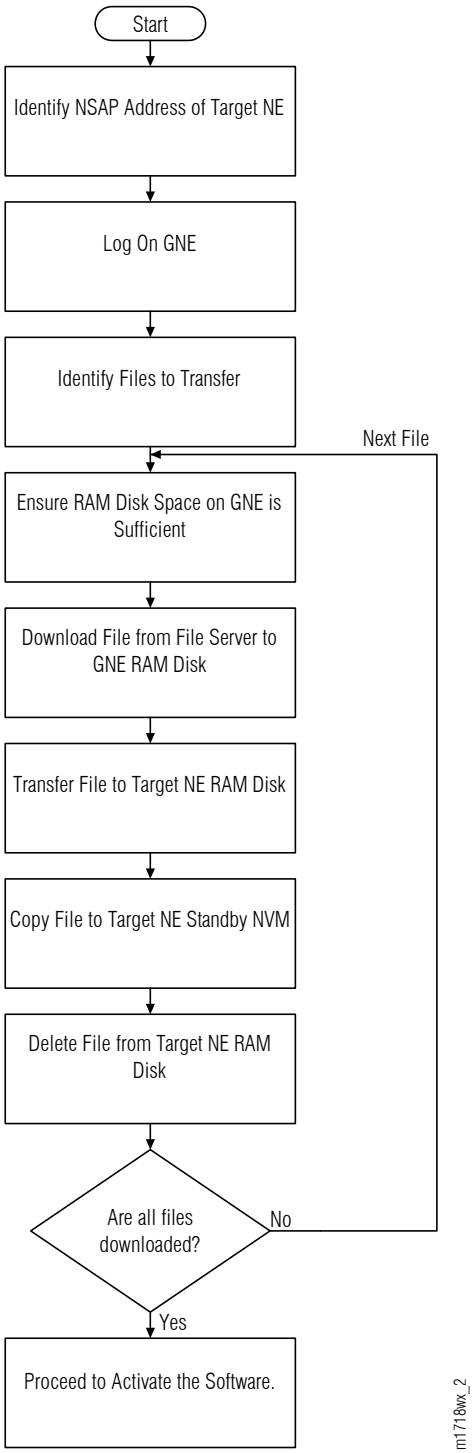


Figure 155: Download Files from File Server to GNE to Target NE (Using CPY-FILE) (Subprocedure Flowchart)

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

Before starting this procedure, complete all steps in Prepare to Upgrade Using TL1. The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Download files to target NE as follows:

Note: *Default values are shown in bold.*

Identify NSAP Address of Target NE

Step 1
Retrieve the AREAADDR and the SYSID of the target NE.

TL1

```
RTRV-NLP:TID::CTAG;
```

TID:

- Target node SID (not GNE)

Example:

```
RTRV-NLP:FUJITSU::CTAG;
```

Response Example:

```
AREAADDR=39840F8000...SYSID=273B84CE...
```

Step 2

Use the AREAADDR and the SYSID retrieved in the previous step to determine the NSAP address of the target NE. Make a record of the NSAP address, which will be used later in Step 9.

Note: *The NSAP address consists of the AREAADDR (26 hex digits), the SYSID (12 hex digits), and the NSEL (always 00, but not displayed).*

If AREAADDR=39840F8000... and SYSID=273B84CE..., then the NSAP address is 39840F8000... 273B84CE...00.

Log On GNE

Step 3

If not already done, log on the GNE. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	
	Comm. Port: COMx (for example, COM2)
	
	Configure: use default[20]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Identify Files to Transfer

Step 4
Identify and record the configuration, program, and firmware files to download. Refer to the tables in the Software Requirements section for the required system software files required for a specific software upgrade. The following table provides an example of the required software file names:

Example:

[20] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Release	Configuration File	Program File	Firmware File(s)
Release 9.1	F7509011.CON	F7509011.PGM	A7509011.PGM B7509011.PGM C7509011.PGM

Step 5
From the set of files identified in the previous step, select a file that has not yet been downloaded.

Note: *Start with any file in the set. This procedure will be performed once for each file to be downloaded.*

Ensure RAM Disk Space on GNE is Sufficient

Step 6
To ensure that sufficient space exists when the file is copied to the GNE RAM disk, view the current contents of the GNE RAM disk.

TL1

```
RTRV-FILE-RDISK:TID::CTAG;
```

Example:
```
RTRV-FILE-RDISK:FUJITSU-GNE::CTAG;
```

Step 7
If necessary, delete files on the GNE RAM disk to ensure sufficient space.

Note: *Ensure that the files on the GNE RAM disk are no longer needed before deleting them.*

TL1

```
DLT-FILE:TID:FILESPEC:CTAG;
```
FILESPEC:

- Name of file to delete (maximum of 12 alphanumeric characters with no format restrictions) or ALL

Example:
```
DLT-FILE:FUJITSU-GNE:ALL:CTAG;
```

Download File from File Server to GNE RAM Disk

Step 8
Copy the file from the remote file system to the RAM disk on the GNE.

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

TID:

- GNE SID

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction)
- This is the file, identified in Step 5, that you are currently downloading.

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to the following table.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU-GNE:139.145.23.43,F7507012.CON,RDISK,F7507012.CON:CTAG:::
OVERWRITE=Y,FTUID=\"swdluser\",FTPID=\"moonrock\",FTPATH=\"C:\GENERICS\";
```

Table 38: CPY-FILE Keyword and Domain Input Parameters

Keyword	Domain (Default in Bold)	Description
OVERWRITE[21]	Overwrite files	
	Y	Write over files with the same name at DST
	N	Do not write over files with the same name at DST
COMMENT	\"xxxxx\" **null**	Sets the user-defined comment, where the comment is up to 60 ASCII characters delineated by escape quotes ***Note:*** *The CPY-FILE command is denied if the COMMENT keyword exceeds 60 characters.*
SIGNATURE[22]	8 hex digits **00000000**	Signature code for each file. When more than one file is transferred, signatures are separated with an & character. ***Note:*** *If SIGNATURE is 0 (zero), the file checksum will not be performed.*
FTUID	\"xxxxx\" **null**	UID used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes

[21] OVERWRITE=Y must be specified when transferring a file from the FLASHWAVE 7500 NE to another location when using FTP or FTAM.
[22] The SIGNATURE keyword is ignored when transferring a file from the NE to any other location.

Table 38: CPY-FILE Keyword and Domain Input Parameters (Cont.)

Keyword	Domain (Default in Bold)	Description
FTPID	\"xxxxx\" **null**	Password used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPATH	\"xxxxx\" **null**	Path to the control file on the server; up to 40 ASCII characters delineated by escape quotes

Transfer File to Target NE RAM Disk

Step 9
Transfer the file from the GNE RAM disk to the target node RAM disk.

TL1

```
CPY-FILE:TID:RDISK,SRCFILE,NETADDR,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

TID:

- GNE SID

SRCFILE:

- Name assigned to file at the copy source (GNE RAM disk) (same as DSTFILE in the previous step); maximum of 12 alphanumeric characters with no format restrictions

NETADDR:

- NSAP address of the target node (from Step 2)

DSTFILE:

- Name assigned to file at the copy destination (target node RAM disk); maximum of 12 alphanumeric characters with no format restrictions

KEYWORD=DOMAIN:

- Refer to Table 38.

Example:

```
CPY-FILE:FUJITSU-GNE:RDISK,F7507012.CON,39840F8000...273B84CE...00,
F7507012.CON:CTAG:::OVERWRITE=Y;
```

Step 10
On the target NE, verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Copy File to Target NE Standby NVM

Step 11
Copy the file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- CON (configuration file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,F7507012.CON,STBY,:CTAG::CON:
COMMENT=\"RELEASE_6.1\";
```

Step 12
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Delete File from Target NE RAM Disk

Step 13
Delete the file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
DLT-FILE:FUJITSU:F7507012.CON:CTAG;
```

Step 14
Have you downloaded all files identified in Step 4?

If YES:
Proceed to Activate the Software.

If NO:
Repeat this procedure to download the next file.

✔ This procedure is complete.

3.3.6 Activate the Software

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Step 1
Activate the software and accept the firmware file in standby memory.

Note: *For a generic issue switch to take place, the three keywords GISSUE, ACTDAT, and ACTTM must be specified. The VALTM keyword is optional.*

Note: *Refer to Software Requirements for the appropriate GISSUE value for the required system software.*

TL1

```
INIT-SYS:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- Refer to the following table for keyword and domain input parameters.

Example:

```
INIT-SYS:FUJITSU::CTAG:::GISSUE=06-01-1,ACTDAT=00-00-00,ACTTM=00-00-00,
VALTM=01-00-00;
```

Table 39: INIT-SYS Keyword and Domain Input Parameters for SWDL

Keyword	Domain (Default in Bold)	Description
GISSUE	xx-yy-z	Generic issue number: • xx = 00…99 • yy = 00…99 • z = 0…9, A…Z
ACTDAT[23]	yymmdd	Activation date (year-month-day): • yy = 00…99 • mm = 01…12 • dd = 01…31
ACTTM[2324]	hhmmss	Activation time (hour-minute-second): • hh = 00…23 • mm = 00…59 • ss = 00…59
VALTM[2325]	hh-mm-ss **00-45-00**	Validation time (hour-minute-second): • hh = 00…99 • mm = 00…59 • ss = 00…59 Minimum time is 45 minutes.
Note: *For a generic issue switch to take place, GISSUE, ACTDAT and ACTTM must be specified. The VALTM keyword is optional.*		

The user is automatically logged off once activation starts.

Step 2

Wait approximately 10 minutes to allow the NE to reset and adjust to the new software and firmware file. When the FAIL/SVCE LED on the NEM Shelf Processor unit lights green, log on the NE. Refer to Step 4 of Log On Target NE, if necessary.

Note: *During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 3

Retrieve and verify software version information.

[23] For a generic issue switch to take place, GISSUE, ACTDAT, and ACTTM must be specified. The VALTM keyword is optional.
[24] Only one scheduled activation of date and time is allowed. The INIT-SYS command is denied if a previous INIT-SYS command was entered with either a software generic or a database activation request.
[25] The timer is started after the new release of software is activated and expires after a duration of hhmmss (minimum of 15 minutes). If the timer is not canceled with the CANC-VALTM command, its expiration causes the system to revert back to the previous release of software.

TL1

```
RTRV-VERSION:TID:AID:CTAG;
```

AID:

- ACT, STBY, **ALL**

Example:

```
RTRV-VERSION:FUJITSU::CTAG;
```

Step 4
Retrieve alarms and conditions on the NE.

TL1

```
RTRV-COND-ALL:TID::CTAG;
```

Example:

```
RTRV-COND-ALL:FUJITSU::CTAG;
```

Step 5
Are any new unexpected active alarms or conditions being reported on the NE?

If YES:
Go to the next step.

If NO:
Go to Step 9.

Step 6
If unable to determine if this is expected behavior, reject the new software before the validation timer expires.

TL1

```
CANC-VALTM:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- ACCEPT=**Y**, N

Example:

```
CANC-VALTM:FUJITSU::CTAG:::ACCEPT=N;
```

Step 7
Contact Fujitsu Technical Support (1-800-USE-FTAC [1-800-873-3822]) to determine how to proceed.

Step 8
Go to Step 15.

Step 9
Accept the new software and firmware file before the validation timer expires.

Note: *The NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units go out approximately 5 minutes after the new software and firmware loads are accepted.*

TL1

```
CANC-VALTM:TID::CTAG:::KEYWORD=DOMAIN;
```

KEYWORD=DOMAIN:

- ACCEPT=**Y**, N

Example:

```
CANC-VALTM:FUJITSU::CTAG;
```

After the system software is activated and the latest firmware file (generic) is downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions.

Step 10
Retrieve alarms and conditions on the NE.

TL1

```
RTRV-COND-ALL:TID::CTAG;
```

Example:

```
RTRV-COND-ALL:FUJITSU::CTAG;
```

Step 11
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment for information on clearing FVM alarms). After all alarms and conditions are cleared (or accounted for), proceed to the following step.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

Caution: *Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command and should be scheduled at an appropriate time to avoid service interruption. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

If NO:
Proceed to the following step.

Step 12
Is the system now running Release 6.1 or later system software?

Note: *Release 4.2 and 4.3 systems cannot be directly upgraded to Release 6.1. For these systems, the procedures in this chapter must be applied twice: first to upgrade to Release 5.1, and then again to upgrade from Release 5.1 to Release 6.1.*

If YES:
Proceed to the next step.

If NO:
Repeat the procedure (Upgrading System Software Using TL1 Commands) to upgrade to Release 6.1.

Step 13
Is the system now running Release 8.x or Release 9.1 system software?

If YES:
Go to Step 15.

If NO:
Proceed to the next step.

Step 14
Does the system need to be upgraded to Release 8.x or Release 9.1 system software?

Note: *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 prior to being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x, 8.x, or 9.1.*

If YES:
Repeat the procedure (Upgrading System Software Using TL1 Commands) to upgrade to Release 8.x or 9.1.

If NO:
This procedure is complete.

Step 15
Should the Expansion Pack files be downloaded now?

Attention: *The Expansion Pack files are required for Release 8.x or 9.1. The Expansion Pack firmware files allow for full support of all FWDL plug-in unit firmware files.*

If YES:
Go to Download Firmware Expansion Pack Files Using TL1Commands or Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard.

If NO:
This procedure is complete.

3.4 Upgrading System Software Using NETSMART 500 Software Download Wizard

In this section:

About NETSMART 500 Software Download Wizard for System Software Upgrade

The NETSMART 500 Software Download wizard assists you in upgrading system software for a FLASHWAVE 7500 NE. For assistance, call the Fujitsu Technical Assistance Center at 1-800-USE-FTAC (1-800-873-3822).

Caution: *Do not use this procedure to upgrade systems prior to Release 4.2. To upgrade these systems, refer to Upgrading System Software from Release 4.1, before performing the upgrade to Release 6.1.*

Caution: *After the system software has been upgraded and the latest firmware file (generic) containing the firmware loads for each plug-in unit has been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the TL1 command INIT-EQPT at an appropriate time by following local practices. For more details, refer to Maintenance.*

Caution: *In Release 5.1 of the FLASHWAVE 7500 system, support is discontinued for all 4-channel OLCs except IFMA-SBxx plug-in units (Refer to the following table). Also, support is discontinued for redundant processors introduced in Release 4.2. Ensure that the system to be upgraded does not include any 4-channel OLCs, except IFMA-SB plug-in units, prior to upgrading system software to Release 5.1 and later.*

Attention: *The NETSMART 500 Software Download Wizard is used to download the required files for a system upgrade. These files include the configuration file (F75xxxxx.CON), program file (F75xxxxx.PGM) and native firmware files (A75xxxxx.PGM, B75xxxxx.PGM, and C75xxxxx.PGM). If system software is upgraded to Release 8.1, the Expansion Pack firmware files will also need to be downloaded. After a successful system upgrade to Release 8.1, refer to Download Firmware Expansion Pack Files Using TL1Commands or Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard to download Expansion Pack firmware files.*

Table 40: 4-Channel OLCs Not Supported in Release 5.1 and Later

Plug-In Unit
IFMA-8Txx, excluding IFMA-8TC1 and IFMA-8TC2

Table 40: 4-Channel OLCs Not Supported in Release 5.1 and Later (Cont.)

Plug-In Unit
IFMA-GUxx, excluding IFMA-GUC1
IFMA-HGxx, excluding IFMA-HGC1
IFMA-HLxx, excluding IFMA-HLC1
IFMA-LExx, excluding IFMA-LEC1
IFMA-LLxx, excluding IFMA-LLC1
IFMA-SAxx

Note: *Refer to NETSMART 500 User Guide, for instructions on the wizard interface.*

The Software Download wizard assists you in:

- Downloading the software and the firmware to the NE
- Activating or scheduling the activation of the new software
- Confirming or rejecting the new software after activation

The wizard determines the applicable tasks based on the software download state and makes available only the applicable tasks.

Note: *These tasks are not available if the NE is pending activation of a new software or database file.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a software download (SWDL) is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Prepare to Upgrade Using the Software Download Wizard

Use the procedure in Prepare to Upgrade Using TL1 to copy software files from the CD-ROM to the File Transfer Protocol (FTP) server and to collect information about the FTP server in preparation for performing the procedure in Upgrading System Software Using NETSMART 500 Software Download Wizard.

3.4.1 Upgrade System Software from Server Using Software Download Wizard

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters.*

To download and activate system software using the NETSMART 500 Software Download wizard, perform the following steps:

Log On

Step 1
Ensure that the NEM Shelf Processor and OSC plug-in units are inserted in the NE and that the NE is powered up.

Step 2
Log on the NE.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to False. Refer to* About Release 4.2 or Later System Software Upgrade.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For detailed information, refer to* Craft Interface Operations .

NETSMART 500

To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select *NE > Logon*.

Note: *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.*

The NE Logon dialog box opens.
Make the following selections:

For **TERM2** (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 graphical user interface.*

Step 3
Retrieve alarms and conditions on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 4
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment for information on clearing FVM alarms). After all alarms and conditions are cleared (or accounted for), proceed to the following task.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to the following task.

Continue with next task ►

Download Software

Step 5
From the menu bar, select *Wizards* > *Software Download*.

Note: *When progressing through the screens in the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

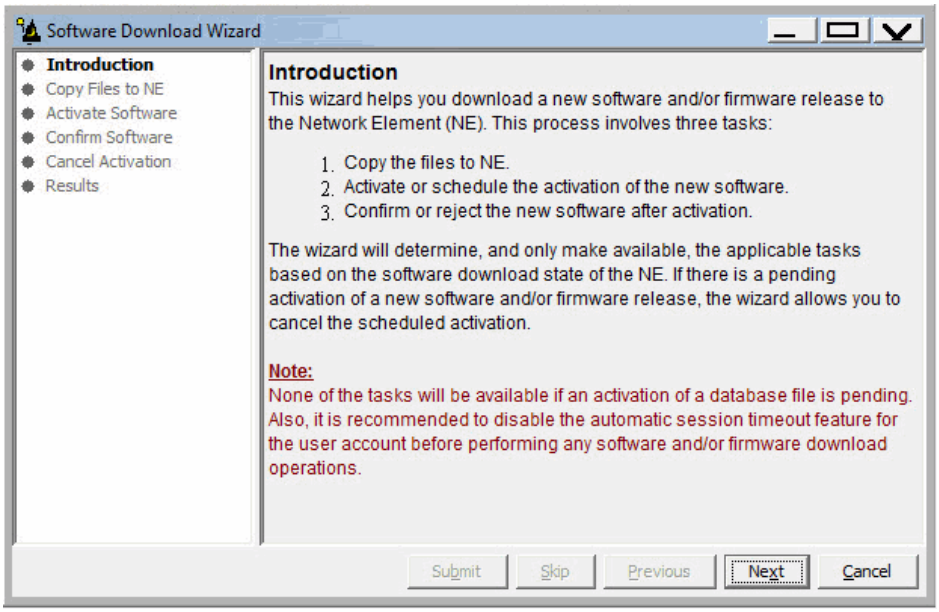


Figure 156: Example Software Download Wizard Introduction Screen

Step 6
Click *Next*.

The *Copy Files to NE* screen opens.

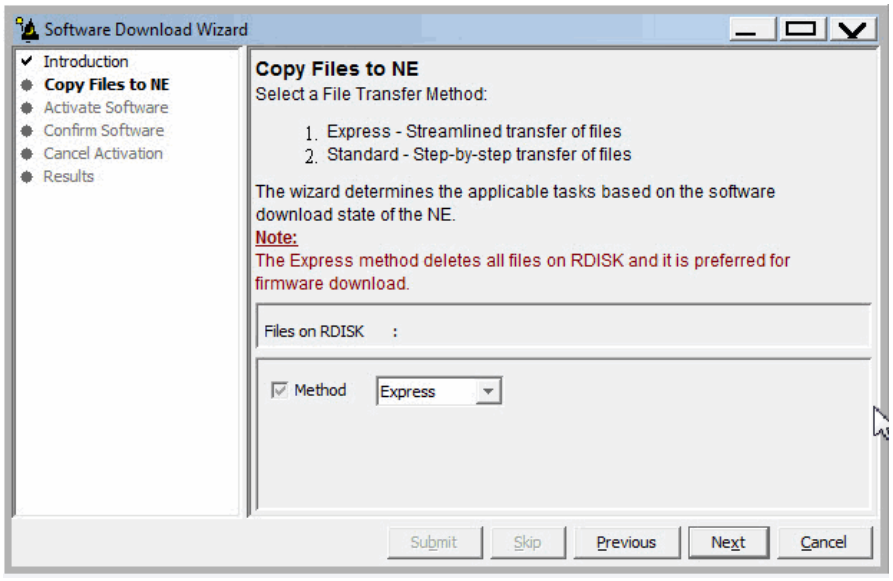


Figure 157: Example Software Download Wizard Copy Files to NE Screen

Step 7
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *This procedure documents the Express method only. Fujitsu recommends this method for software download because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 8
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

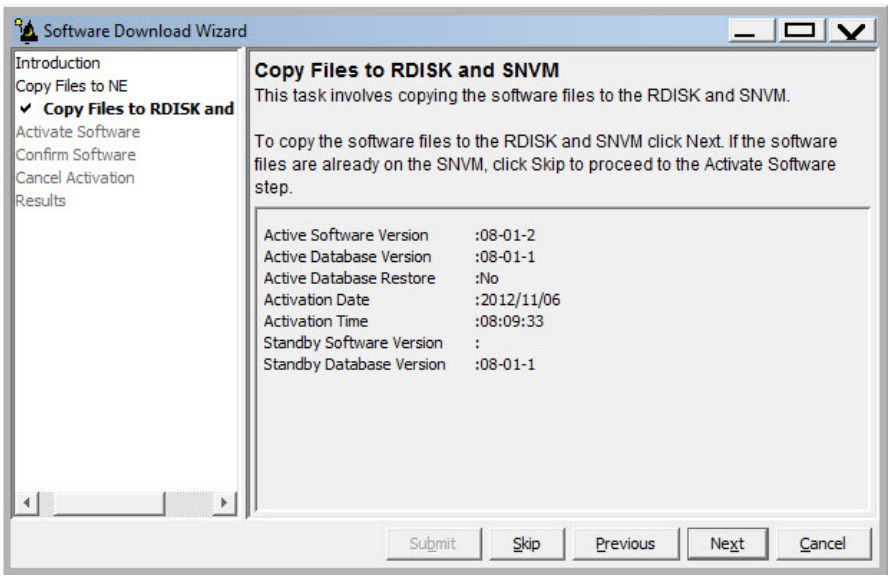


Figure 158: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 9
Verify that the *Active Software Version* is *04-02-2* (or later). Then click *Next*.

Note: *The current software must be Release 4.2 (or later). If the software is an earlier release, perform the procedures in* Upgrading System Software from Release 4.1*, before performing the upgrade to Release 6.1.*

The *Select Host* screen opens.

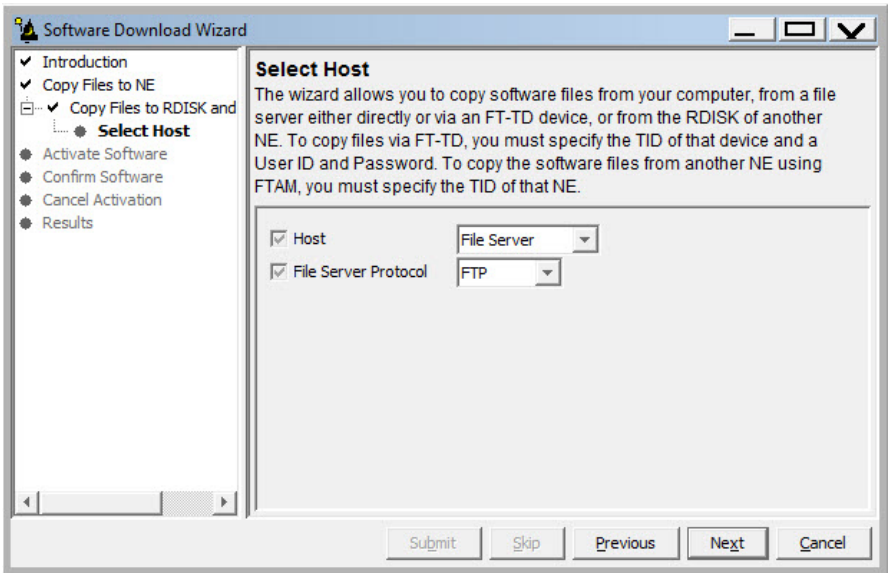


Figure 159: Example Software Download Wizard Select Host Screen

Step 10
Verify File Server is selected in the *Host* drop-down list.

Refer to Upgrade System Software from Another NE Using Software Download Wizard to download software from another NE.

Step 11
Click *Next*.

The *Select FTP Server* screen opens.

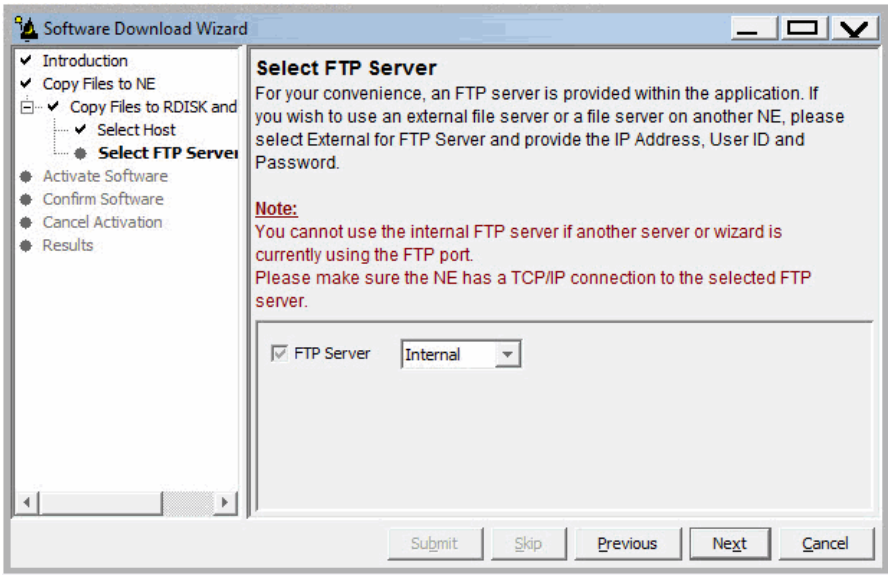


Figure 160: Example Software Download Wizard Select FTP Server Screen

Step 12
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 13
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 14
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

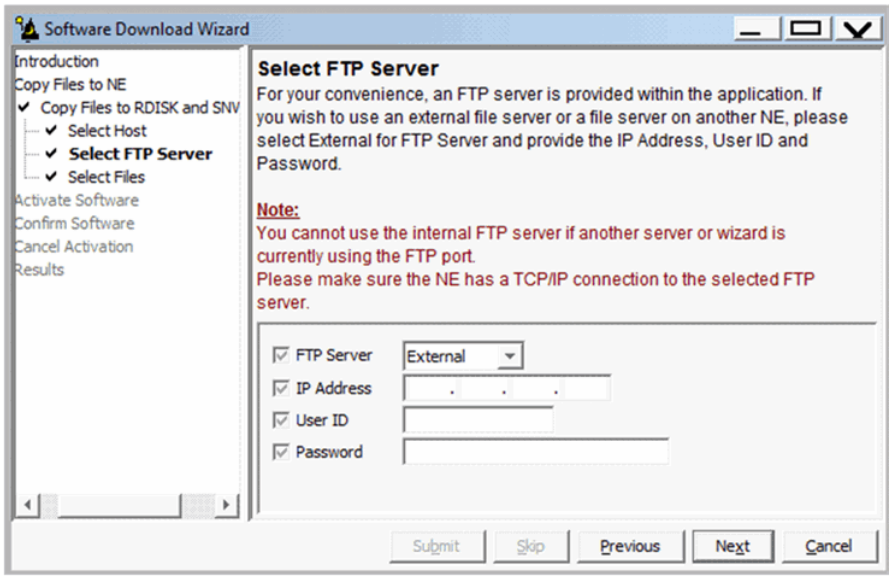


Figure 161: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 15
Click *Next*.

The *Select Files* screen opens.

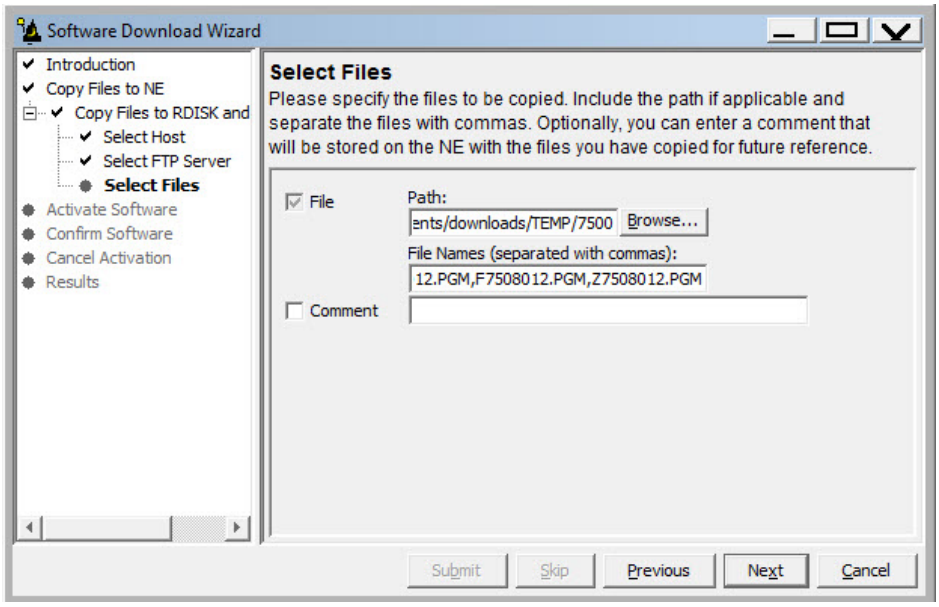


Figure 162: Example Software Download Wizard Select Files Screen

Step 16
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 17
In the *File: File Names (separated with commas)* text box, enter the following file names:

- *F7509011.CON*
- *F7509011.PGM*
- *A7509011.PGM*
- *B7509011.PGM*
- *C7509011.PGM*

Attention: *The NETSMART 500 Software Download Wizard is used to download the required files for a system upgrade. These files include the configuration file (F75xxxxx.CON), the program file (F75xxxxx.PGM), and the native firmware files (A75xxxxx.PGM, B75xxxxx.PGM, and C75xxxxx.PGM). If system software is being upgraded to Release 8.1, the Expansion Pack firmware files will also need to be downloaded. After a successful system upgrade to Release 8.1, refer to* Download Firmware

Expansion Pack Files Using TL1Commands *or* Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard *to download Expansion Pack firmware files.*

Step 18
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 19
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 14 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000), by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

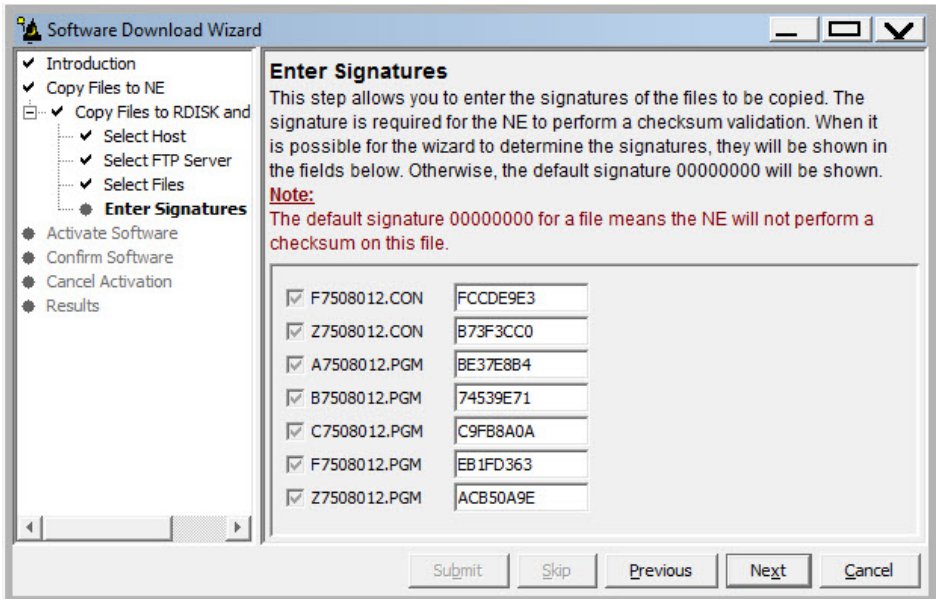


Figure 163: Example Software Download Wizard Enter Signatures Screen

Step 20
Click *Next*.

The *Copy to RDISK and SNVM* screen opens.

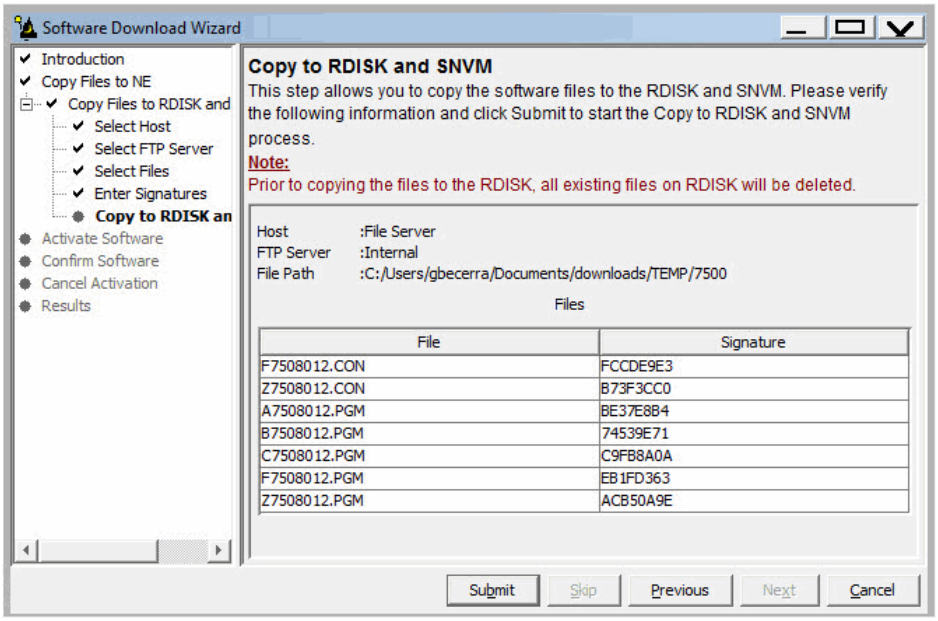


Figure 164: Example Software Download Wizard Copy to RDISK and SNVM Screen

Step 21
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying for each file.

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

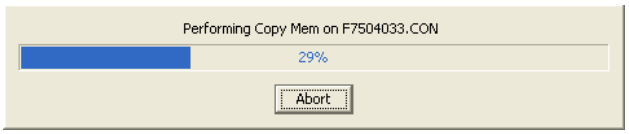


Figure 165: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen opens.

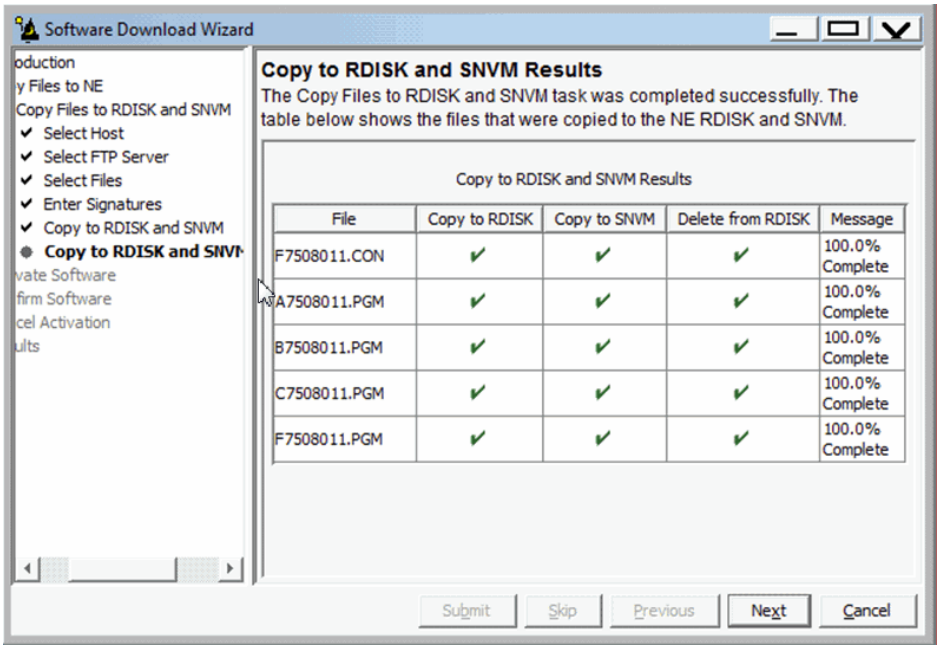


Figure 166: Example Software Download Wizard Copy to RDISK and SNVM Results Screen

Activate Software

Step 22
Click *Next*.

The *Activate Software* screen opens.

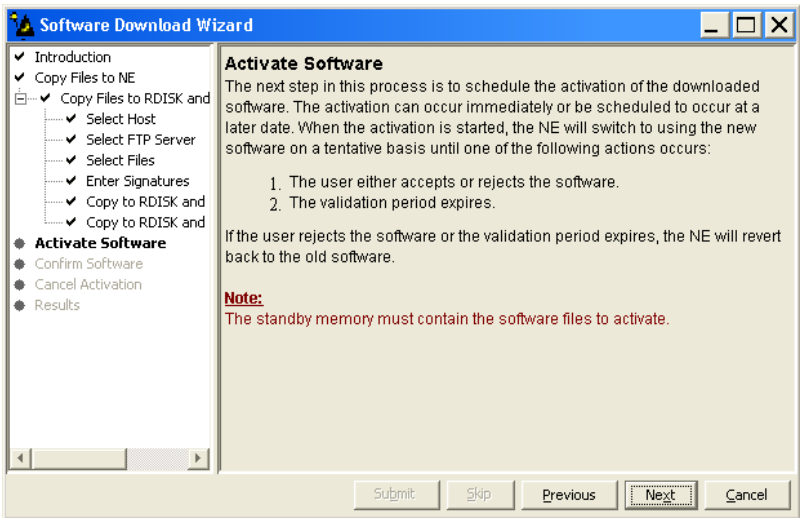


Figure 167: Example Software Download Wizard Activate Software Screen

Step 23
Click *Next*.

The *Software Activation Parameters* screen opens.

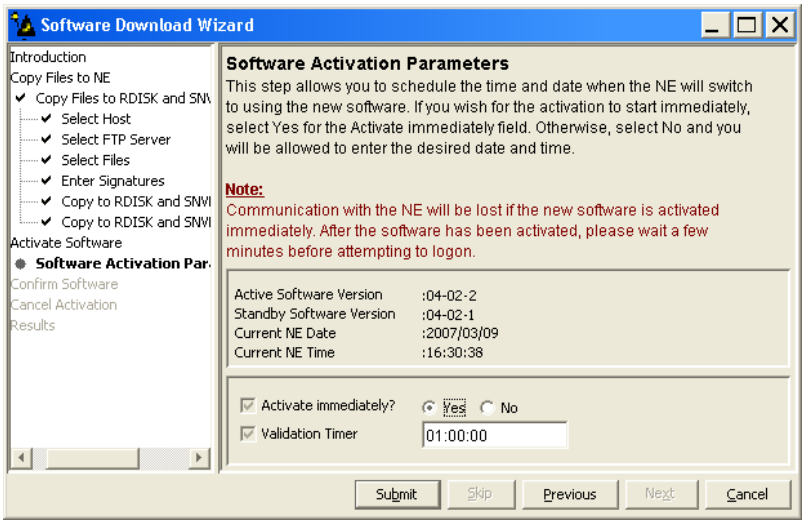


Figure 168: Example Software Download Wizard Software Activation Parameters Screen

Step 24
Do you want to activate the firmware and software immediately?

If YES:
Continue with the next step.

If NO:
Go to Step 31.

Step 25
Verify *Yes* is selected for the *Activate immediately* option.

Step 26
In the *Validation Timer* text box, enter the desired time before the system reverts back to the previous software (the default is 01:00:00 [1 hour]).

Step 27
Click *Submit*.

The *Software Activation Result* screen opens.

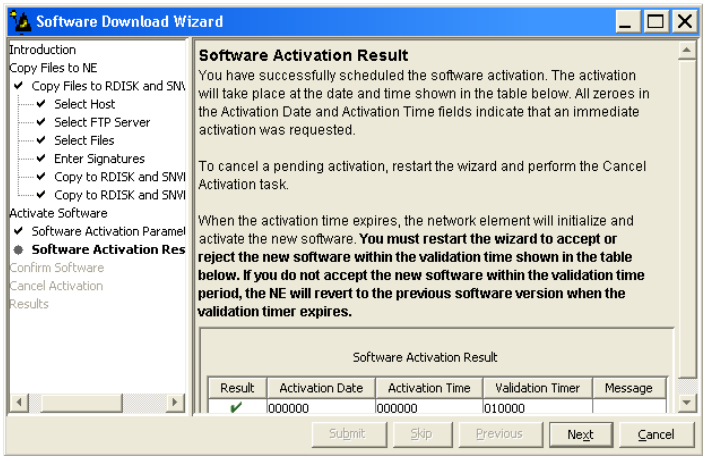


Figure 169: Example Software Download Wizard Software Activation Result Screen

Step 28
Click *Next*.

A *Warning* dialog box opens.

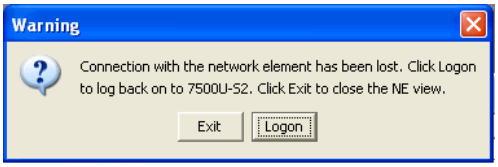


Figure 170: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 29
Click *Logon*.

The *Software Activation Result* screen closes, and the Software Download wizard closes.

Step 30
Go to Step 36.

Step 31
Select *No* for the *Activate immediately* option.

The *Software Activation Parameters* screen displays additional fields.

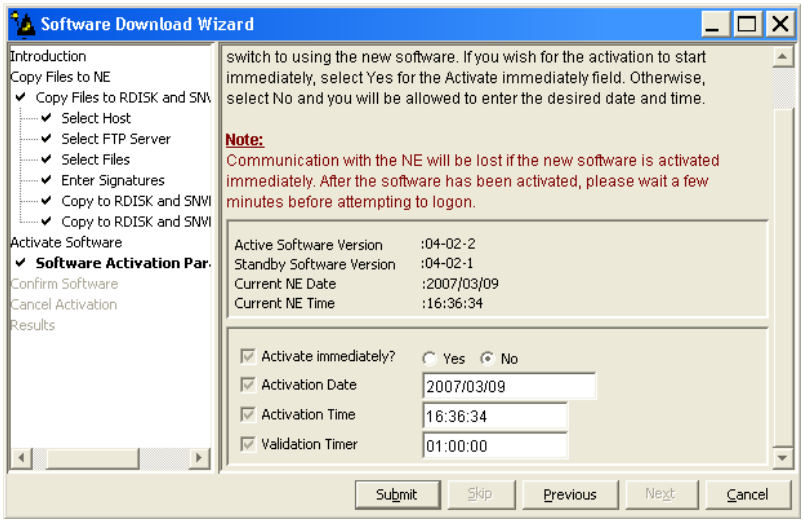


Figure 171: Example Software Activation Parameters–Scheduled Activation

a) Enter the *Activation Date* for the firmware and software activation.

b) Enter the *Activation Time* for the firmware and software activation.

c) Enter the *Validation Time* for the firmware and software activation.

Step 32
Click *Submit*.

The *Software Activation Result* screen opens.

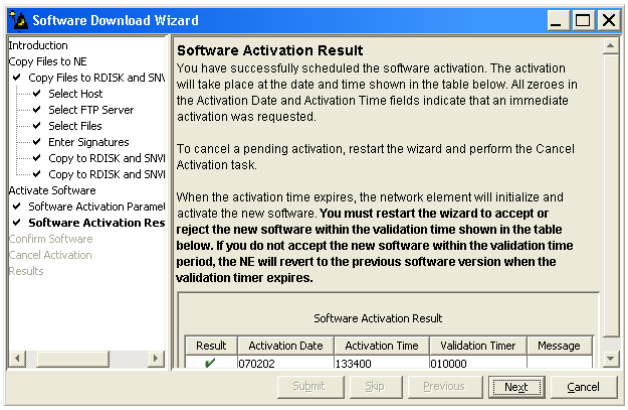


Figure 172: Example Software Download Wizard Software Activation Result Screen

Step 33
Click *Next*.

The *Results* screen opens.

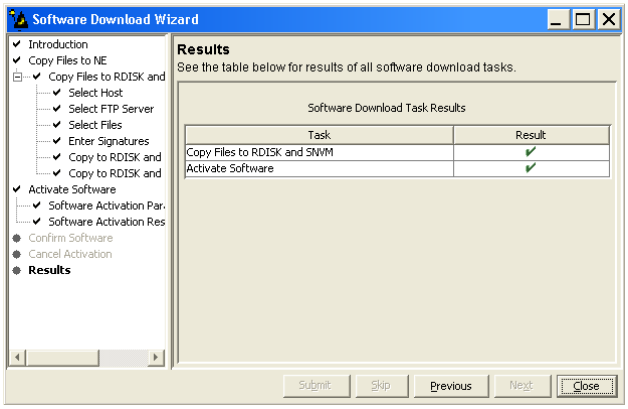


Figure 173: Example Software Download Wizard Results Screen

Step 34
Click *Close*.

The Software Download wizard closes. You may continue working in the NETSMART 500 environment and stay logged on to the NE. When the activation date and time is reached, you are logged off the NE and a *Warning* dialog box appears.

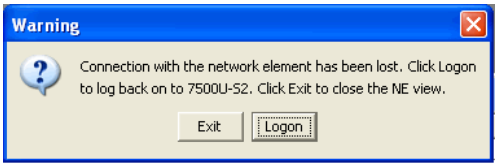


Figure 174: Example of a Typical Warning Dialog Box

Step 35
Click *Logon*.

The NETSMART 500 window closes.

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Confirm Software Download

Note: *You must accept the new software load before the validation timer set in* Step 26 *expires. Otherwise, the system software will revert back to the previous load.*

Step 36
Log back on the NE. Refer to Step 2, if necessary.

Step 37
From the menu bar, select *Wizards* > *Software Download*.

The Software Download wizard starts, and the *Introduction* screen opens.

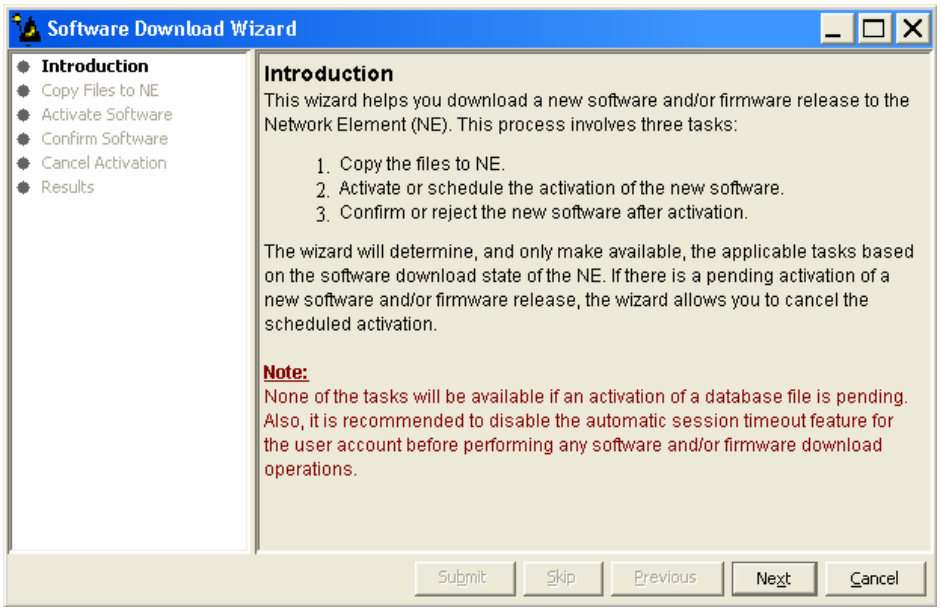


Figure 175: Example Software Download Wizard Introduction Screen

Step 38
Click *Next*.

The *Confirm Software* screen opens.

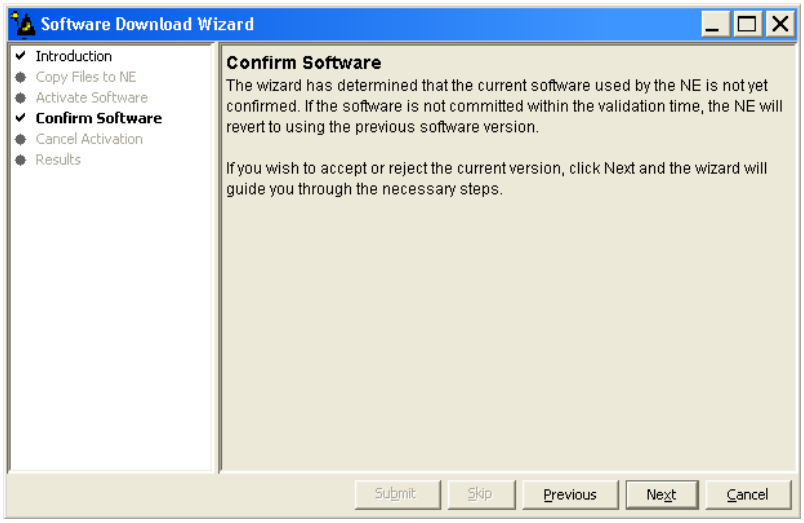


Figure 176: Example Software Download Wizard Confirm Software Screen

Step 39
Click *Next*.

The *Accept/Reject Software* screen opens.

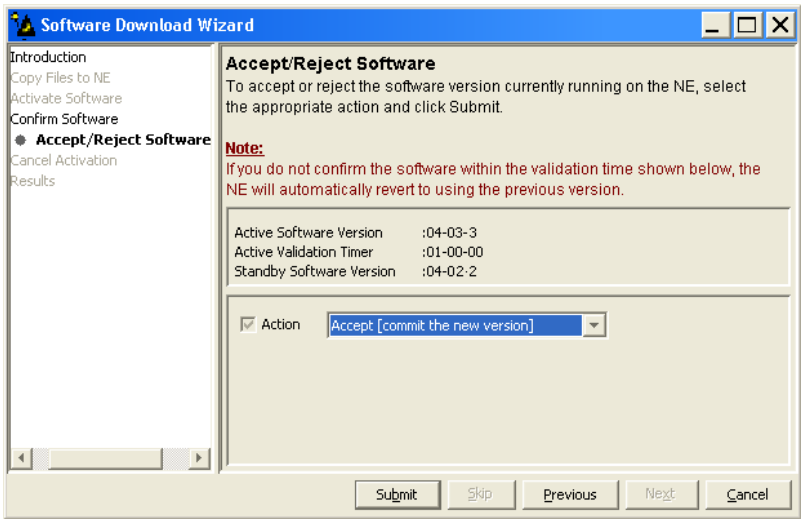


Figure 177: Example Software Download Wizard Accept/Reject Software Screen

Step 40
Verify that the *Accept [commit the new version]* option is selected in the *Action* drop-down list.

Step 41
Click *Submit*.

A progress bar displays while the validation timer is cancelled and the software is accepted.

Once the software is accepted, the *Software Confirmation Result* screen opens.

Note: *The screen may take several minutes to open.*

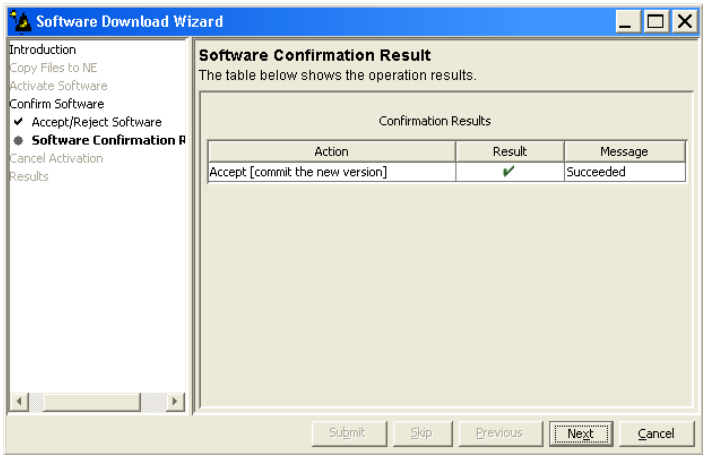


Figure 178: Example Software Download Wizard Software Confirmation Result Screen

Step 42
Click *Next*.

The final *Results* screen opens.

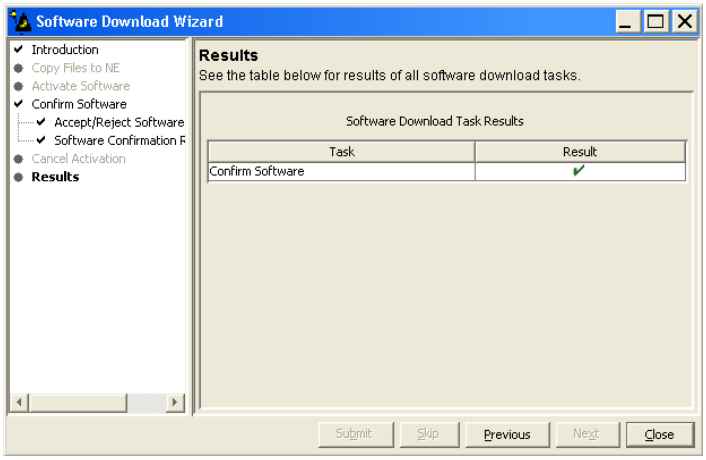


Figure 179: Example Software Download Wizard Results Screen

Step 43
Click *Close*.

The *Results* screen closes and the Software Download wizard closes.

After the system software is activated and the latest firmware file (generic) is downloaded to the system, the system may generate some firmware version mismatch alarms (FVM) against individual plug-in units with incompatible firmware versions.

Step 44
Retrieve alarms and conditions on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 45
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment, for information on clearing FVM alarms. After all alarms and conditions are cleared (or accounted for), proceed to Step 46.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

Caution: *Installing new firmware on a plug-in unit programs the programmable hardware on the plug-in unit and can impact traffic associated with the plug-in unit. Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command and should be scheduled at an appropriate time to avoid service interruption. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

If NO:
Proceed to the next step.

Step 46
Is the system now running the required system software?

Note: *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 before being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x or 8.x.*

If YES:
Proceed to the next step.

If NO:
Repeat the procedures in Upgrading System Software Using NETSMART 500 Software Download Wizard and Upgrade System Software from Server Using Software Download Wizard to upgrade to the required system software.

Step 47
Is the system now running Release 8.1 system software?

If YES:
Proceed to the next step.

If NO:
Log off the NE. This procedure is complete.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to confirm.

Step 48
Should the Expansion Pack files be downloaded now?

Attention: *The Expansion Pack files are required for Release 8.1. The Expansion Pack firmware files allow for full support of all FWDL plug-in unit firmware files.*

If YES:
Go to Download Firmware Expansion Pack Files Using TL1Commands or Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard.

If NO:
Log off the NE. This procedure is complete.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to confirm.

✔ This procedure is complete.

3.4.2 Upgrade System Software from Another NE Using Software Download Wizard

Caution: *After the system software has been upgraded and the latest firmware file (generic) containing the firmware loads for each plug-in unit has been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the TL1 command INIT-EQPT at an appropriate time by following local practices. For more details, refer to* Maintenance.

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters.*

Perform the following steps to download and activate system software to a remote NE from a local NE using the NETSMART 500 Software Download wizard:

Log On Local and Remote NEs

Step 1
Ensure that the NEM Shelf Processor and OSC plug-in units are inserted in the NEs and the NEs are powered up.

Step 2
Ensure that the systems do not include any 4-channel OLCs, except IFMA-SB plug-in units. Refer to Table 40.

Step 3
Log on both NEs.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to No.*

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values. The TID, UID, and PID values are not case-sensitive.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For detailed information, refer to FNC-7500-0042-272A, System Operations, Section 3.2, Craft Interface Operations [p. 3-3].*

NETSMART 500

To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select *NE > Logon*.

Note: *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.*

The NE Logon dialog box opens.
Make the following selections:

For **TERM1** (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial

Comm. Port: COMx (for example, COM2)

Configure: use default[26]

For **TERM2** (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: *Refer to FNC-0500-0050-010, NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 4
Retrieve alarms and conditions on the Local and Remote NEs.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

[26] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 5
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Step 6
Delete all files from the RAM disk (RDISK) of the Local NE and Remote NE.

TL1	NETSMART 500

`DLT-FILE:TID:AID:CTAG;`
AID:
• ALL
Example:
`DLT-FILE:FUJITSU:F7505011.PGM:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select DLT-FILE command from the *Command Name* drop-down list.
	Enter *ALL* in the *AID* field.
	Click *Send*.
	Do not close the TL1 Command Builder dialog box.

Step 7
Verify the RDISK on the Local NE and Remote NE is empty.

TL1	NETSMART 500

`RTRV-FILE-RDISK:TID:AID:CTAG;`
AID:
• **ALL**
Example:
`RTRV-FILE-RDISK:FUJITSU:ALL:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.
	Enter the program file name or ALL in the AID field.
	Click *Send*.
	Close the TL1 Command Builder dialog box.

Start the Software Download Wizard at Local NE

Step 8
Switch to the local NE.

Step 9
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this and each subsequent screen.*

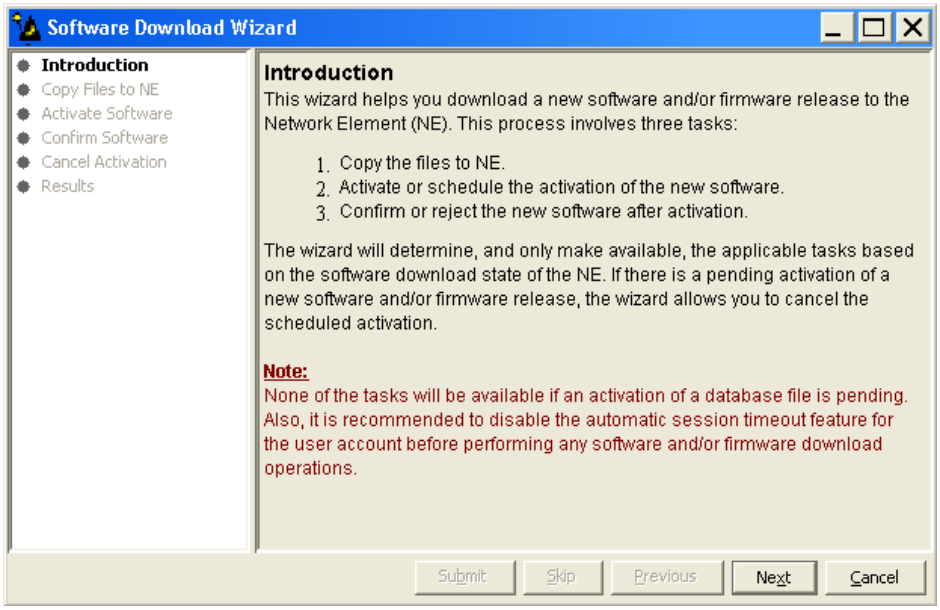


Figure 180: Example Software Download Wizard Introduction Screen

Step 10
Click *Next*.

The *Copy Files to NE* screen appears.

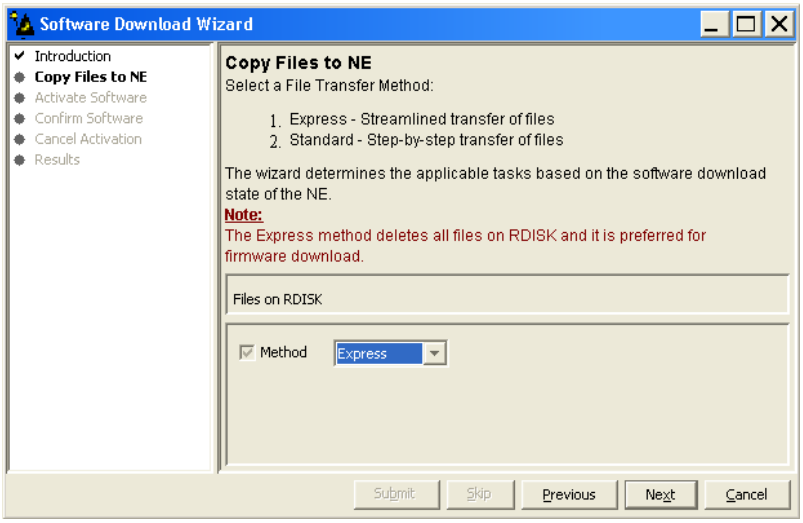


Figure 181: Example Software Download Wizard Copy Files to RDISK Screen

Step 11
Select *Standard* from the *Method* drop-down list.

Note: *Do not use the Express method at the Local NE. The Express method copies the software files to the RDISK, then to the SNVM, then deletes the software files from the RDISK. This procedure requires that the software files are copied to only the RDISK of the Local NE.*

Step 12
Click *Next*.

The *Copy Files to RDISK* screen opens.

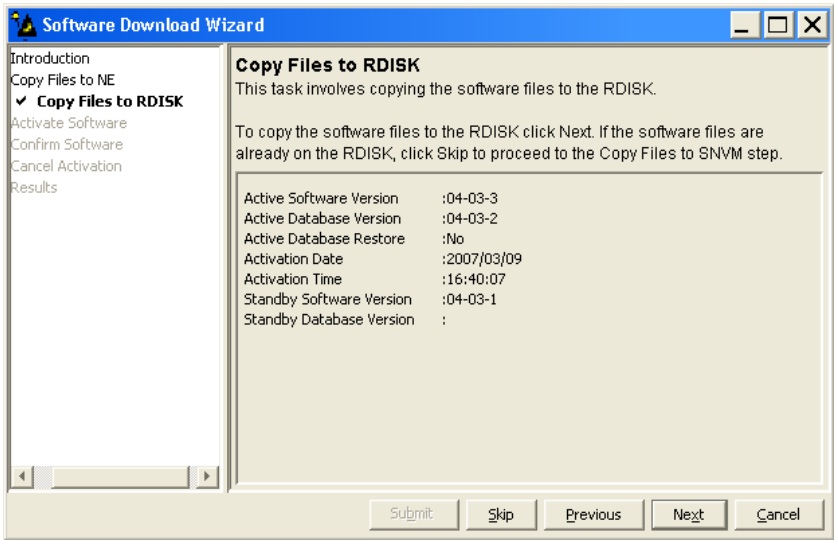


Figure 182: Example Software Download Wizard Copy Files to RDISK Screen

Step 13
Click *Next*.

The *Select Host* screen opens.

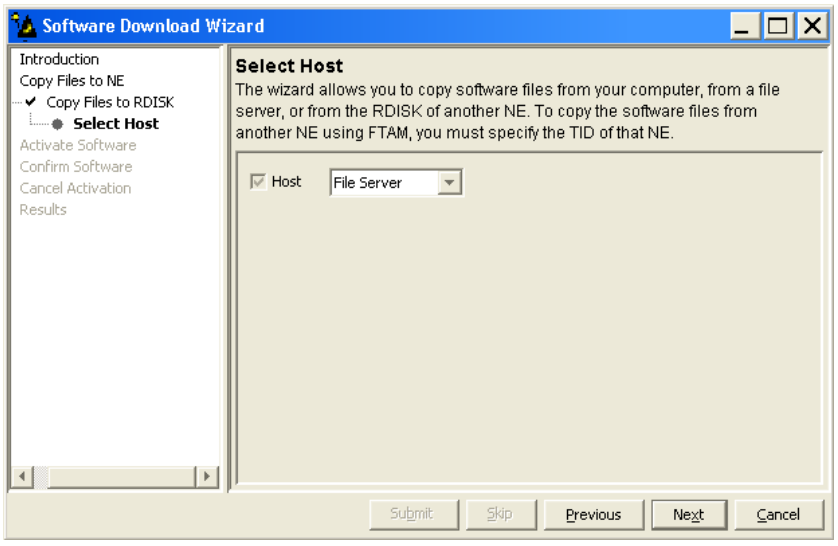


Figure 183: Example Software Download Wizard Select Host Screen

Download Software Configuration and Firmware Files from Server

Step 14
From the *Host* drop-down list, select *File Server*.

Step 15
Click *Next*.

The *Select FTP Server* screen opens.

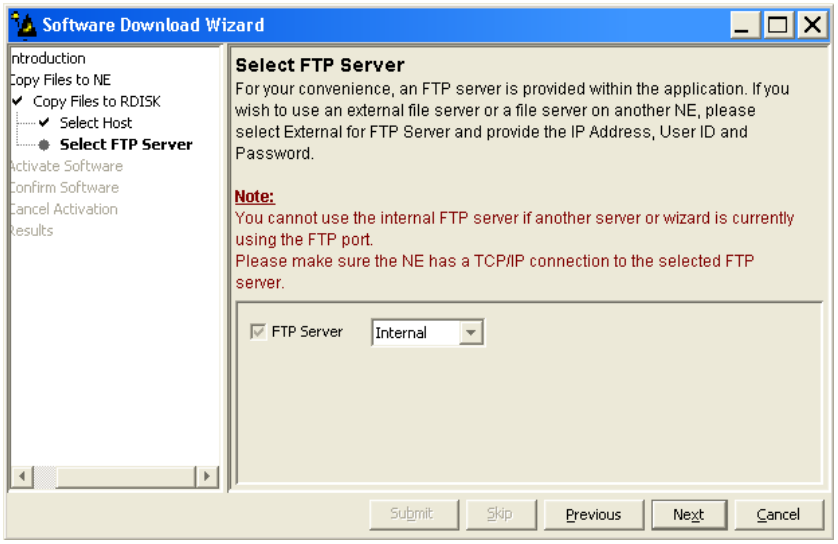


Figure 184: Example Software Download Wizard Select FTP Server Screen

Step 16
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 17
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 18
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

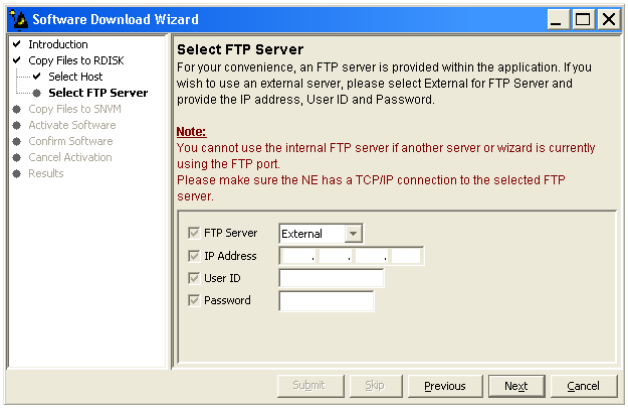


Figure 185: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 19
Click *Next*.

The *Select Files* screen opens.

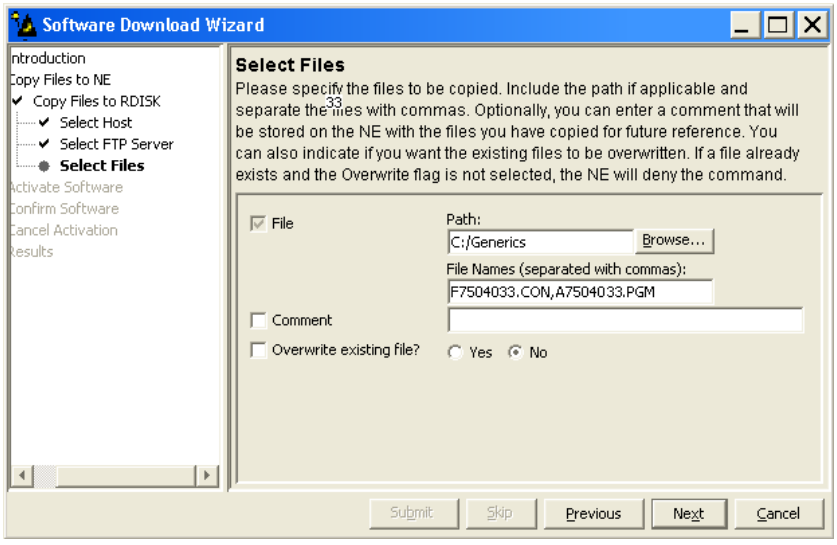


Figure 186: Example Software Download Wizard Select Files Screen

Step 20
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 21
In the *File: File Names (separated with commas)* text box, enter the following file names, separated by a comma:

- F75xxxxx.CON
- A75xxxxx.PGM

Step 22
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 23
Select *Yes* for the *Overwrite existing file* option.

Step 24
Click *Next*.

Note: *The software download may take up to several minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in* Step 18 *or the files are being copied from another NE, the signature fields will be populated with zeros (00000000) by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

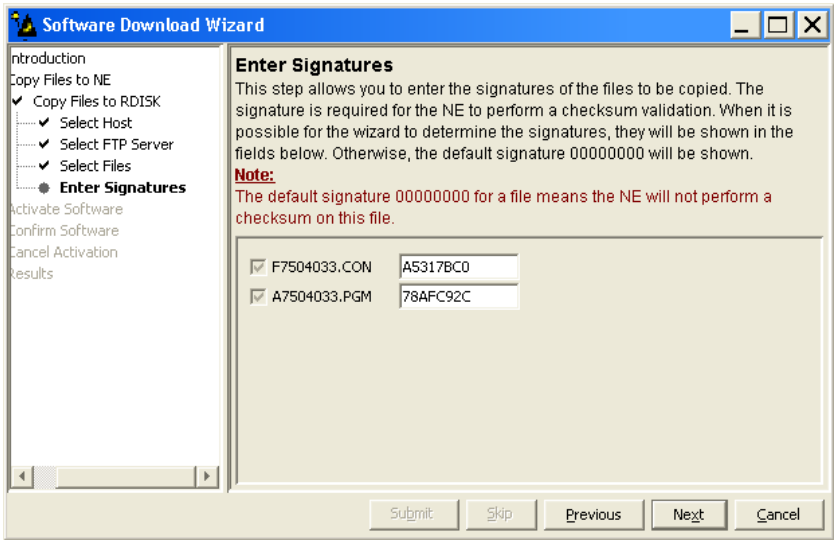


Figure 187: Example Software Download Wizard Enter Signatures Screen

Step 25
Click *Next*.

The *Copy to RDISK* screen opens.

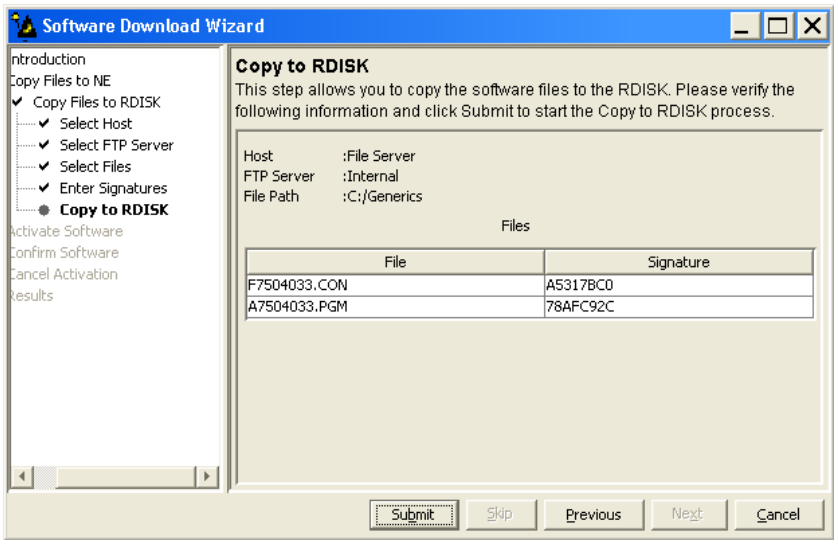


Figure 188: Example Software Download Wizard Copy to RDISK and SNVM Screen

Step 26
Click *Submit*.

A *Performing Copy File* dialog box opens, displaying the progress of the copying of software files from the server to the RDISK of the Local NE.

Note: *The files take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

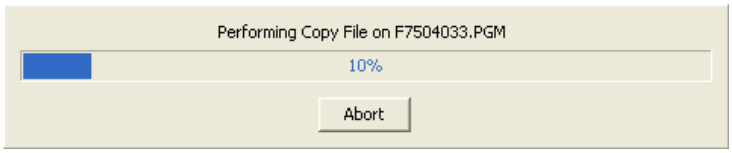


Figure 189: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

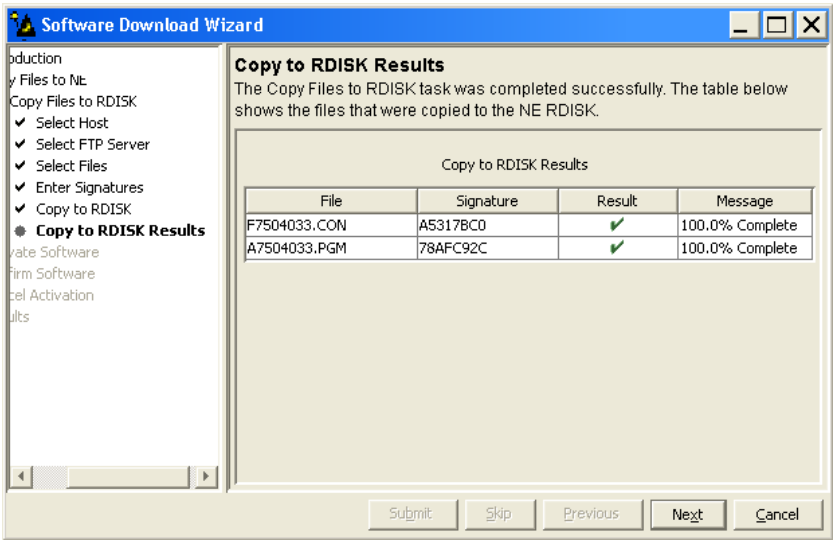


Figure 190: Example Software Download Wizard Copy to RDISK Results Screen

Step 27
Click *Cancel*, and then click *Yes* to close the wizard.

Step 28
Continue with the next step.

Start the Software Download Wizard at Remote NE

Step 29
Switch to the Remote NE.

Step 30
From the menu bar, select *Wizards* > *Software Download*.

Note: *When progressing through the screens in the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

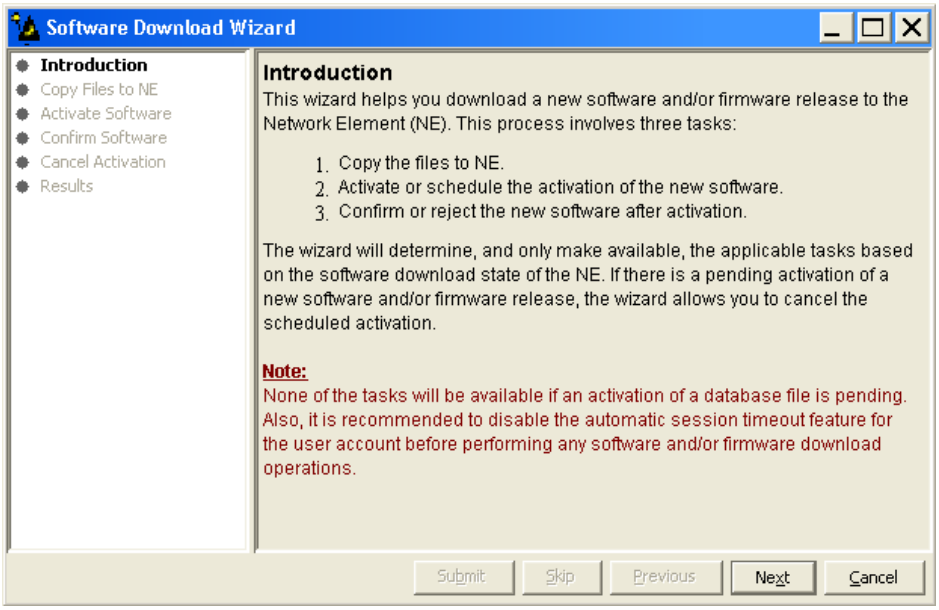


Figure 191: Example Software Download Wizard Introduction Screen

Step 31
Click *Next*.

The *Copy Files to NE* screen opens.

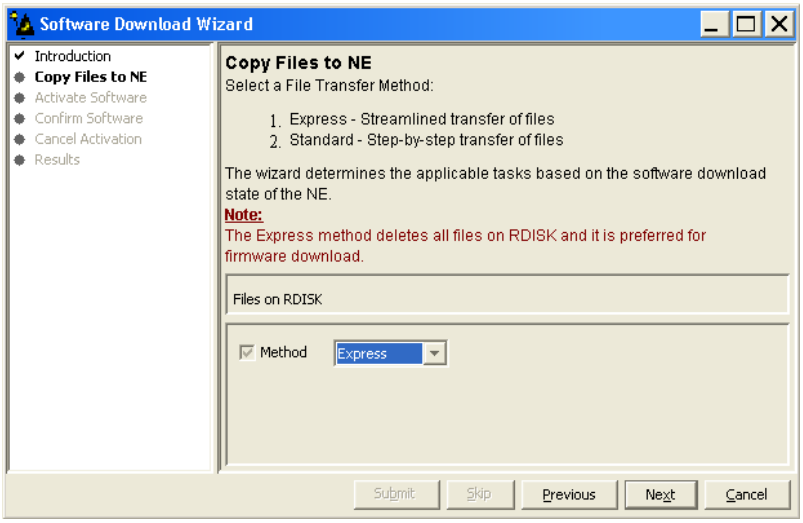


Figure 192: Example Software Download Wizard Copy Files to NE Screen

Step 32
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *The Express method is used to copy the software file from the random access memory disk (RDISK) of the Local NE to the standby nonvolatile memory (SNVM) of the Remote NE. Fujitsu recommends this method because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 33
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

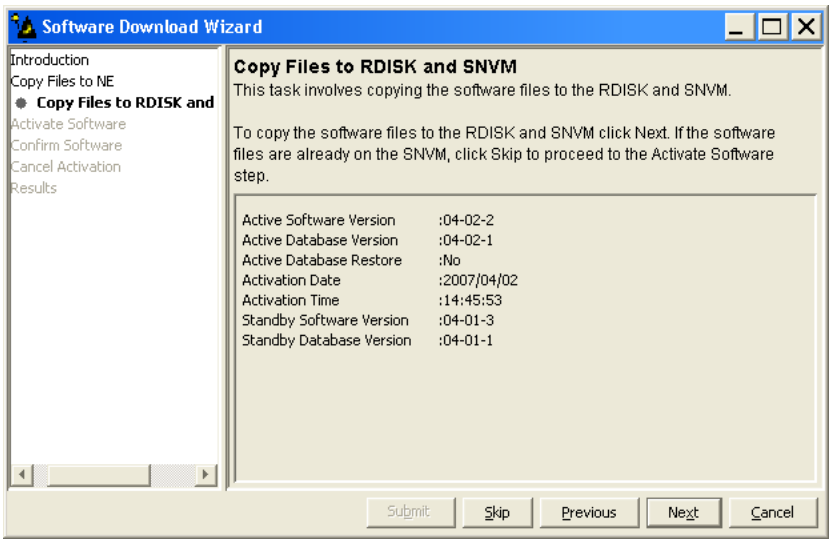


Figure 193: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 34
Verify that the *Active Software Version* is *04-02-2* (or later). Then click *Next*.

Note: *The current software must be Release 4.2 (or later). If the software is an earlier release, perform the procedures in* Upgrading System Software from Release 4.1*, before performing the upgrade to Release 6.1.*

The *Select Host* screen opens.

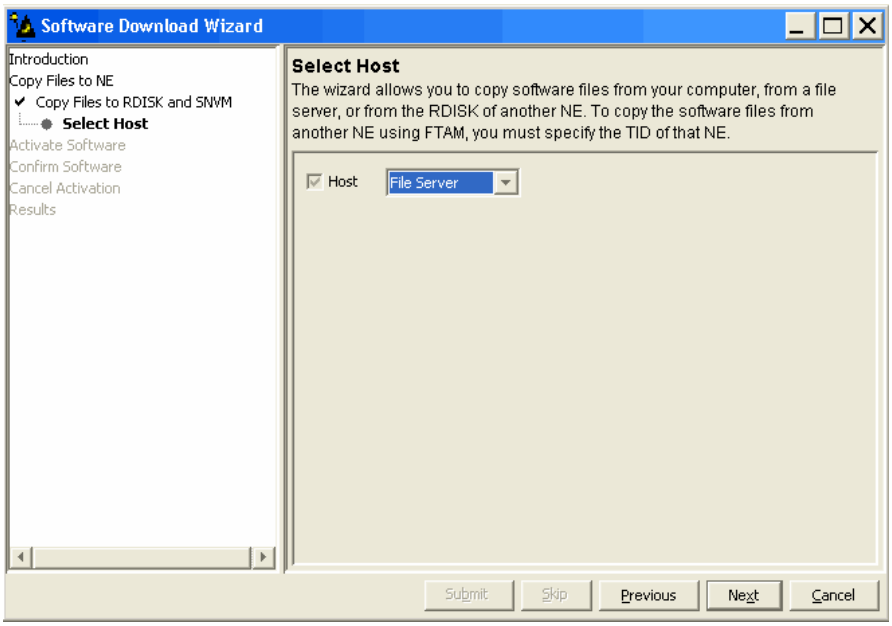


Figure 194: Example Software Download Wizard Select Host Screen

Download Firmware and Software Files from Another NE

Step 35
From the *Host* drop-down list, select *Another NE*.

The *Select Host* screen displays an additional field.

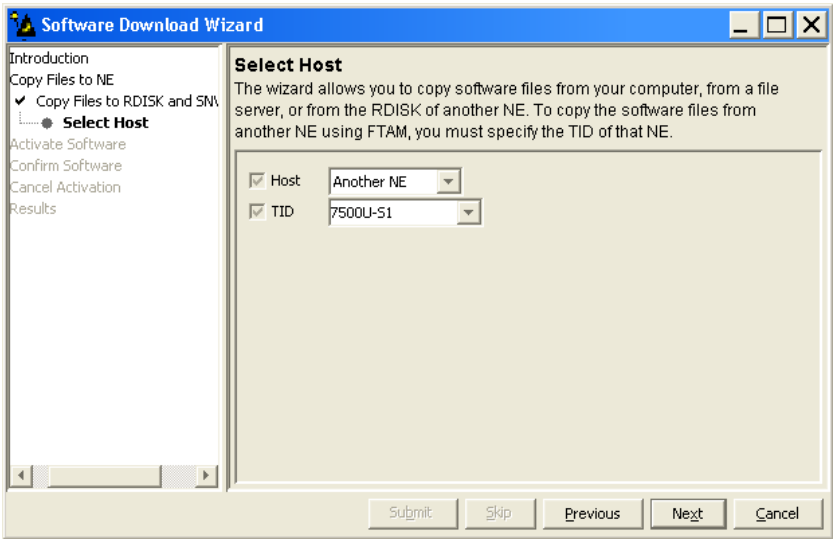


Figure 195: Example Software Download Wizard Select Host–Another NE Selected

Step 36
From the *TID* drop-down list, select the TID of the Local NE.

Step 37
Click *Next*.

The *Select Files* screen appears.

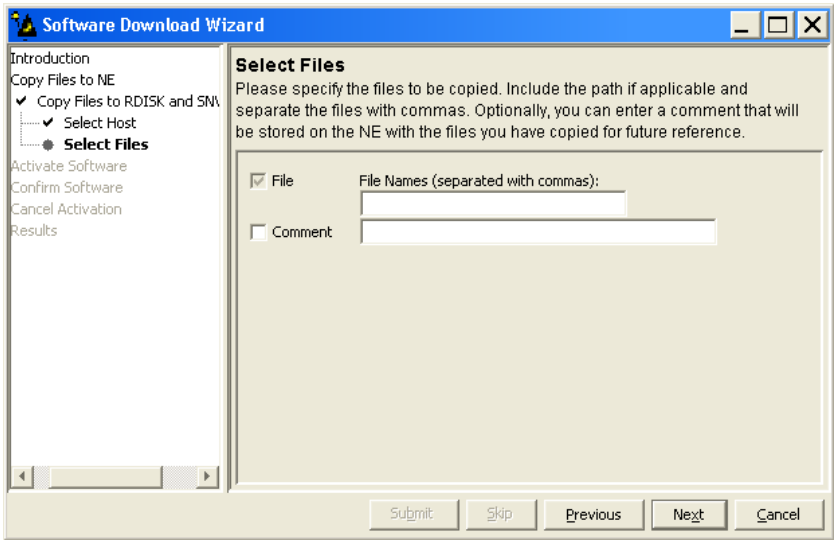


Figure 196: Example Software Download Wizard Select Files Screen

Step 38
In the *File: File Names (separated with commas)* text box, enter the following file names separated with a comma:

- F75xxxxx.CON
- A75xxxxx.PGM

Attention: *The NETSMART 500 Software Download Wizard is used to download the required files for a system upgrade. These files include the configuration file (F75xxxxx.CON), program file (F75xxxxx.PGM), and native firmware files (A75xxxxx.PGM, B75xxxxx.PGM, and C75xxxxx.PGM). If system software is being upgrading to Release 8.1, the Expansion Pack firmware files will also need to be downloaded. After a successful system upgrade to Release 8.1, refer to* Download Firmware Expansion Pack Files Using TL1Commands *or* Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard *to download Expansion Pack firmware files.*

Step 39
In the *Comment* text box, enter comments.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 40
Click *Next*.

The *Enter Signatures* screen appears.

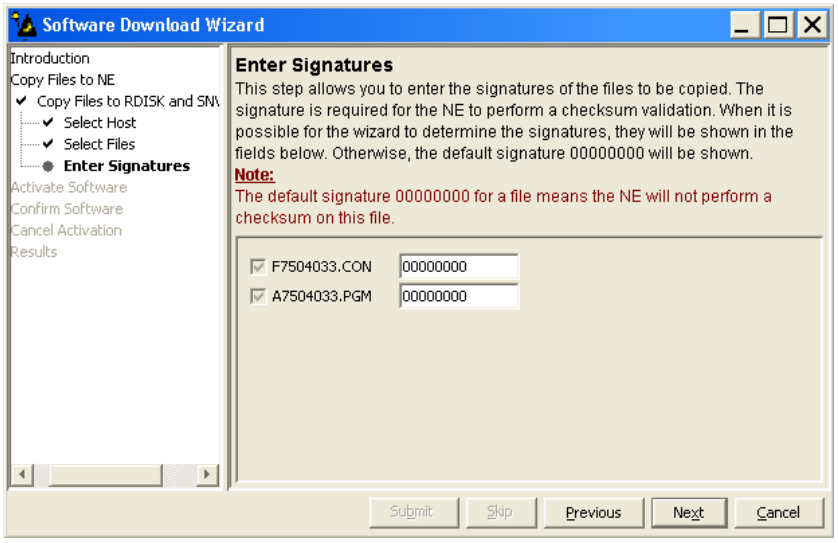


Figure 197: Example Software Download Wizard Enter Signatures Screen

Note: *When the files are being copied from another NE, the signature fields are populated with zeros by default (00000000). In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

Step 41
Click *Next*.

The *Copy to RDISK and SNVM* screen appears.

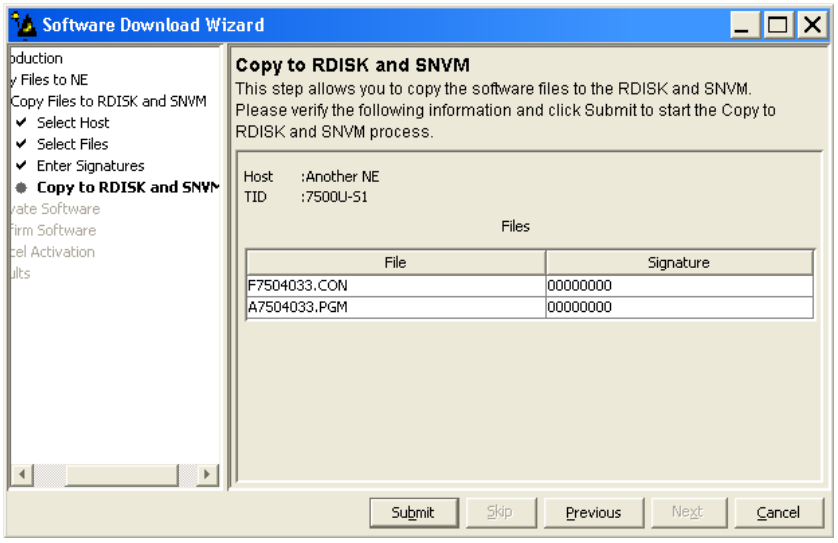


Figure 198: Example Software Download Wizard Copy to RDISK Screen

Step 42
Click *Submit*.

A *Performing Copy File* window opens, displaying the progress of the copying of software files from the RDISK of the Local NE to the RDISK and SNVM of the Remote NE.

Note: *The files can take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

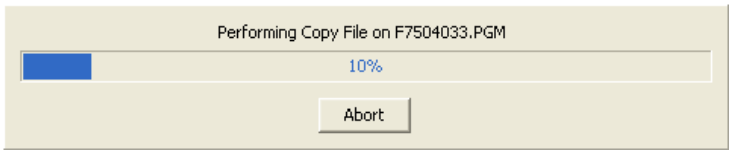


Figure 199: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen appears.

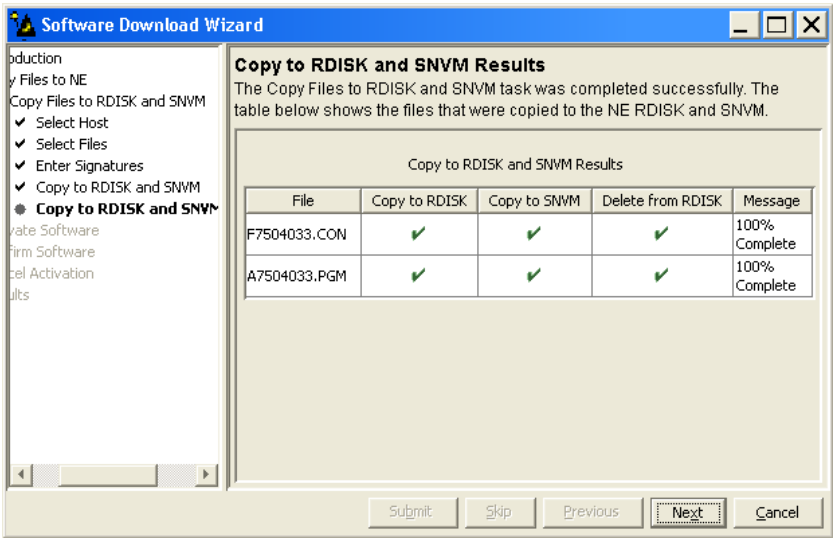


Figure 200: Example of Software Download Wizard Copy to RDISK Results Screen

Step 43
Click *Cancel*, then *Yes* to close the Software Download Wizard.

The Express mode deletes the software files from the RDISK once the files are copied to the SNVM on the Remote NE. The software files must now be deleted from the RDISK of the Local NE.

Step 44
Continue with the next step.

Delete Program File from RDISK of Local NE

Step 45
Verify the RDISK disk on the Remote NE is empty.

TL1	NETSMART 500

`RTRV-FILE-RDISK:TID:AID:CTAG;`
AID:
• **ALL**
Example:
`RTRV-FILE-RDISK:FUJITSU:ALL:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.
	Enter the program file name or ALL in the AID field.
	Click *Send*.
	Close the TL1 Command Builder dialog box.

Step 46
Switch to the Local NE.

Step 47
At the Local NE, delete the software files from the RDISK.

TL1	NETSMART 500

`DLT-FILE:TID:AID:CTAG;`
AID:
• ALL
Example:
`DLT-FILE:FUJITSU:F7505011.PGM:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select DLT-FILE command from the *Command Name* drop-down list.
	Enter *ALL* in the *AID* field.
	Click *Send*.
	Do not close the TL1 Command Builder dialog box.

Step 48
Verify the RDISK disk on the Local NE is empty.

TL1	NETSMART 500

`RTRV-FILE-RDISK:TID:AID:CTAG;`
AID:
• **ALL**
Example:
`RTRV-FILE-RDISK:FUJITSU:ALL:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select RTRV-FILE-RDISK command from the *Command Name* drop-down list.
	Enter the program file name or ALL in the AID field. Click *Send*.
	Close the TL1 Command Builder dialog box.

Start the Software Download Wizard at Local NE

Step 49
From the menu bar, select *Wizards* > *Software Download*.

Note: *In progressing through the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

Note: *Fujitsu recommends maximizing the screen to facilitate access to all the information on this and each subsequent screen.*

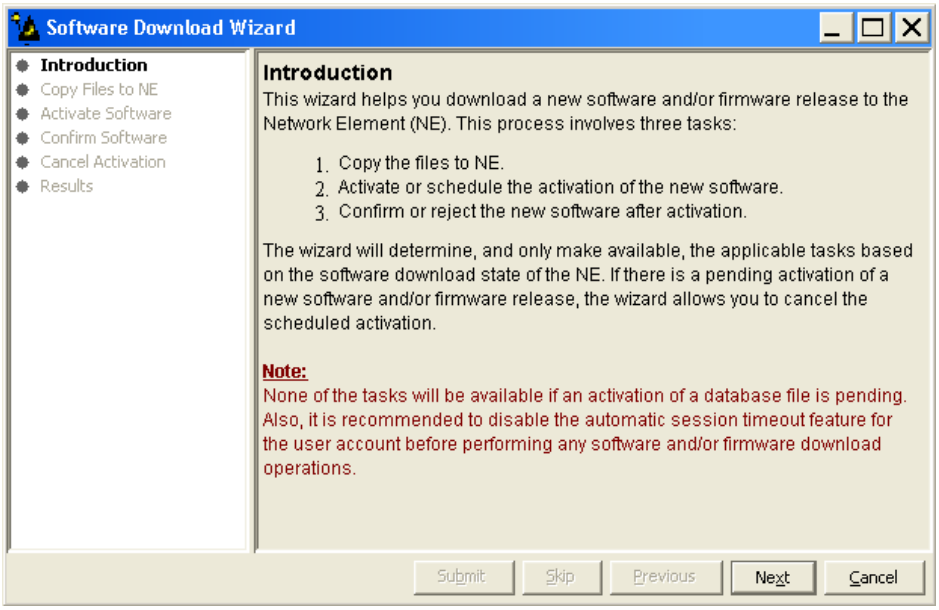


Figure 201: Example Software Download Wizard Introduction Screen

Step 50
Click *Next*.

The *Copy Files to RDISK* screen appears.

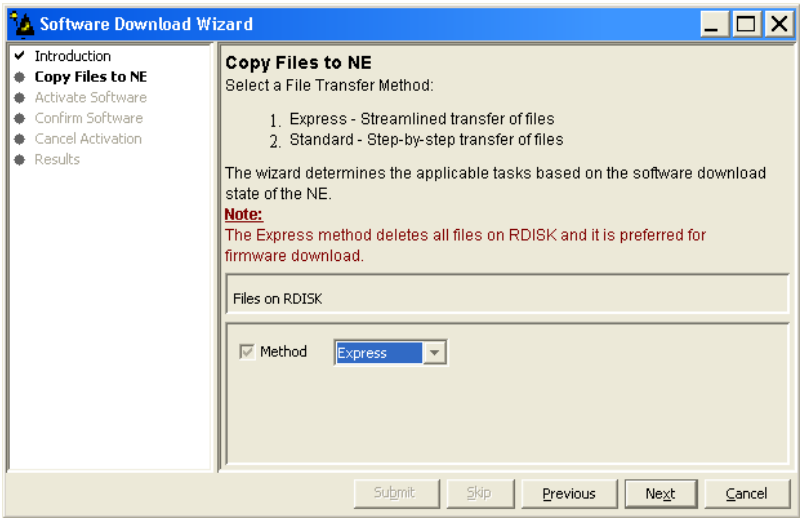


Figure 202: Example Software Download Wizard Copy Files to RDISK Screen

Step 51
Select *Standard* from the *Method* drop-down list.

Note: *Do not use the Express method at the Local NE. The Express method copies the software files to the RDISK, then to the SNVM, then deletes the software files from the RDISK. This procedure requires that the software files are copied only to the RDISK of the Local NE.*

Step 52
Click *Next*.

The *Copy Files to RDISK* screen opens.

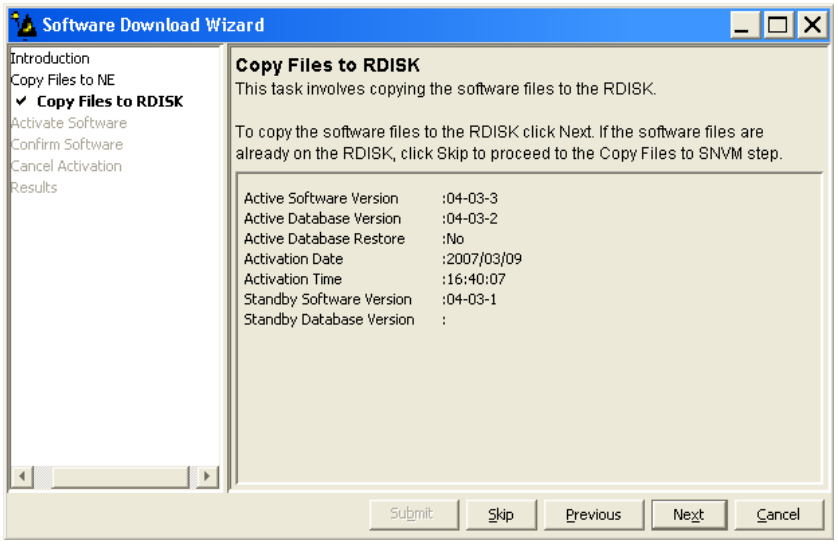


Figure 203: Example Software Download Wizard Copy Files to RDISK Screen

Step 53
Click *Next*.

The *Select Host* screen opens.

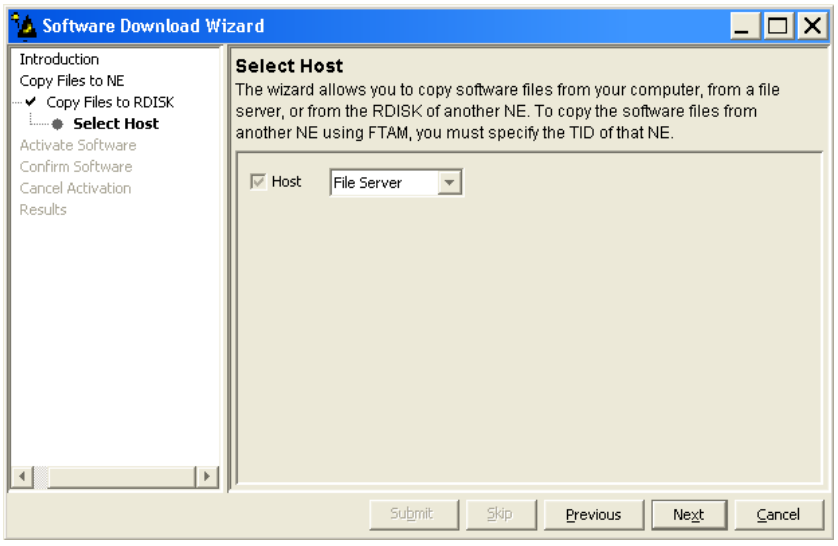


Figure 204: Example Software Download Wizard Select Host Screen

Download Software Program File from Server

Step 54
From the *Host* drop-down list, select *File Server*.

Step 55
Click *Next*.

The *Select FTP Server* screen opens.

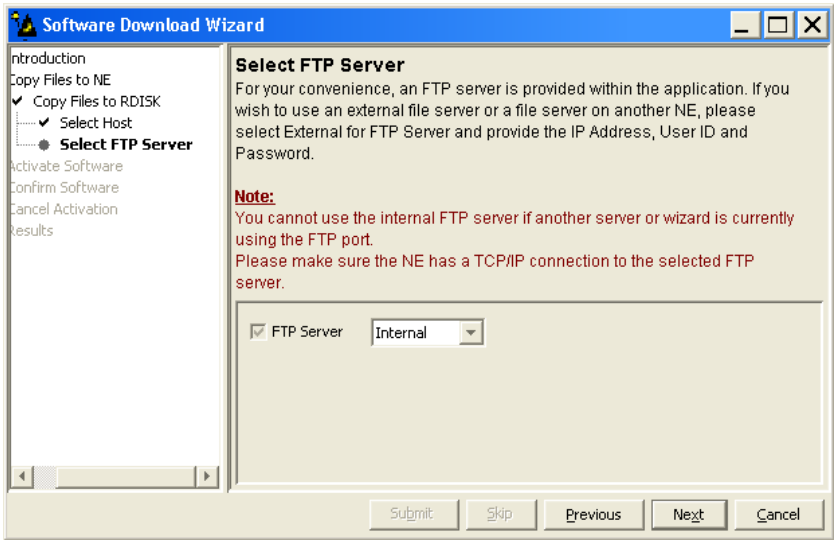


Figure 205: Example Software Download Wizard Select FTP Server Screen

Step 56
Are the software files located on an internal FTP server or an external FTP server (refer to Prepare to Upgrade Using TL1)?

Internal FTP server–Continue with the next step.

External FTP server–Skip the next step.

Step 57
From the *FTP Server* drop-down list, select *Internal* and skip the next step.

Step 58
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

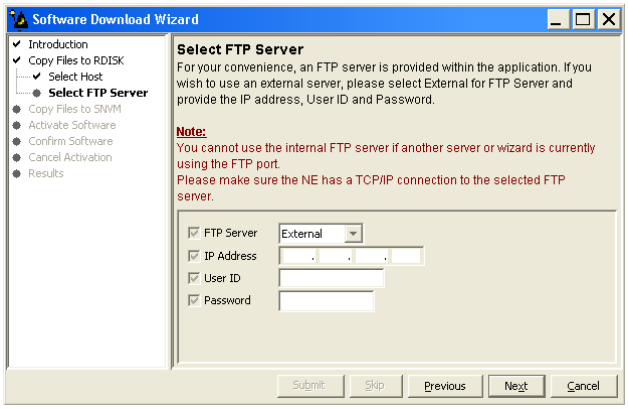


Figure 206: Example Software Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 59
Click *Next*.

The *Select Files* screen opens.

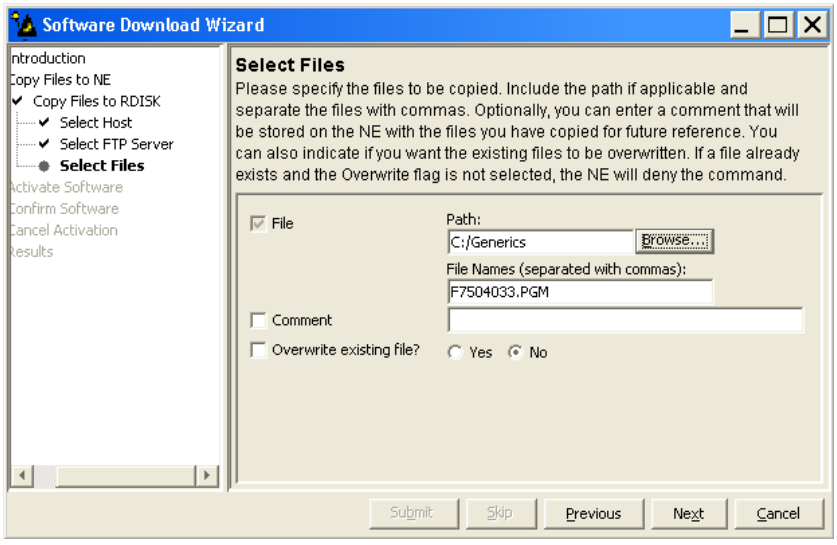


Figure 207: Example Software Download Wizard Select Files Screen

Step 60
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 61
In the *File: File Names (separated with commas)* text box, enter F75xxxxx.PGM, B75xxxxx.PGM, or C75xxxxx.PGM (Release 7.1 or later), depending on which files have been previously downloaded.

Step 62
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 63
Select *Yes* for the *Overwrite existing file* option.

Step 64
Click *Next*.

Note: *The software download may take up to several minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected in Step 58 or the files are being copied from another NE, the signature fields will be populated with zeros (00000000) by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

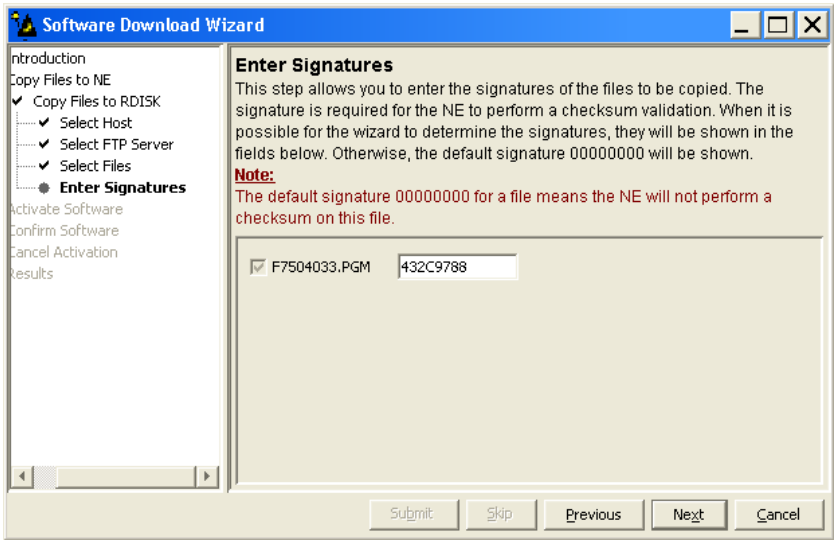


Figure 208: Example Software Download Wizard Enter Signatures Screen

Step 65
Click *Next*.

The *Copy to RDISK* screen opens.

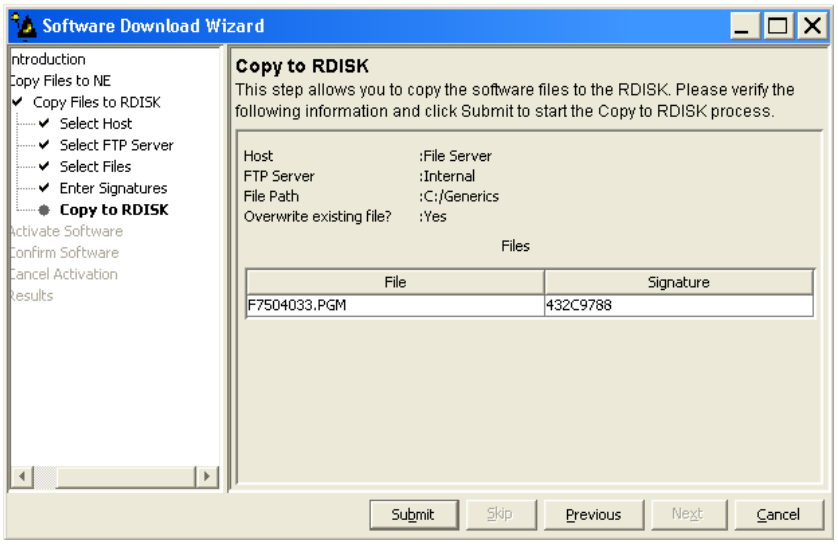


Figure 209: Example Software Download Wizard Copy to RDISK Screen

Step 66
Click *Submit*.

A *Performing Copy File* window opens, displaying the progress of the copying of software file from the server to the RDISK of the Local NE.

Note: *The file takes up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

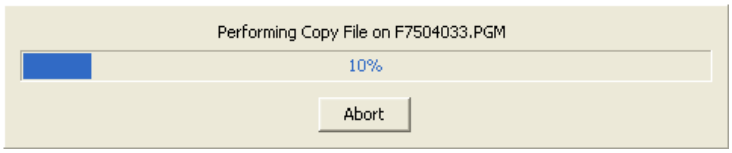


Figure 210: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK Results* screen opens.

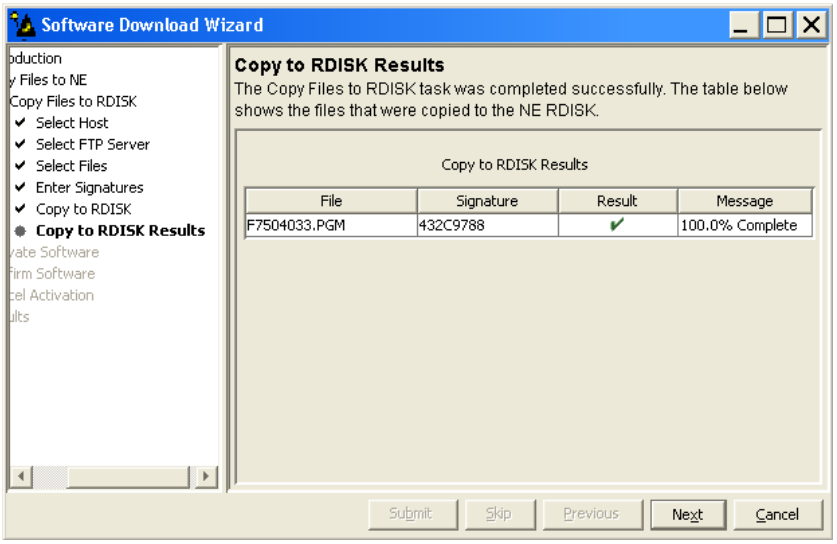


Figure 211: Example Software Download Wizard Copy to RDISK Results Screen

Step 67
Click *Cancel*, then *Yes* to close the wizard.

Step 68
Continue with the next step.

Start the Software Download Wizard at Remote NE

Step 69
Switch to the Remote NE.

Step 70
From the menu bar, select *Wizards* > *Software Download*.

Note: *When progressing through the screens in the Software Download wizard, the current screen may momentarily gray before the next screen opens.*

The Software Download wizard starts and the *Introduction* screen opens.

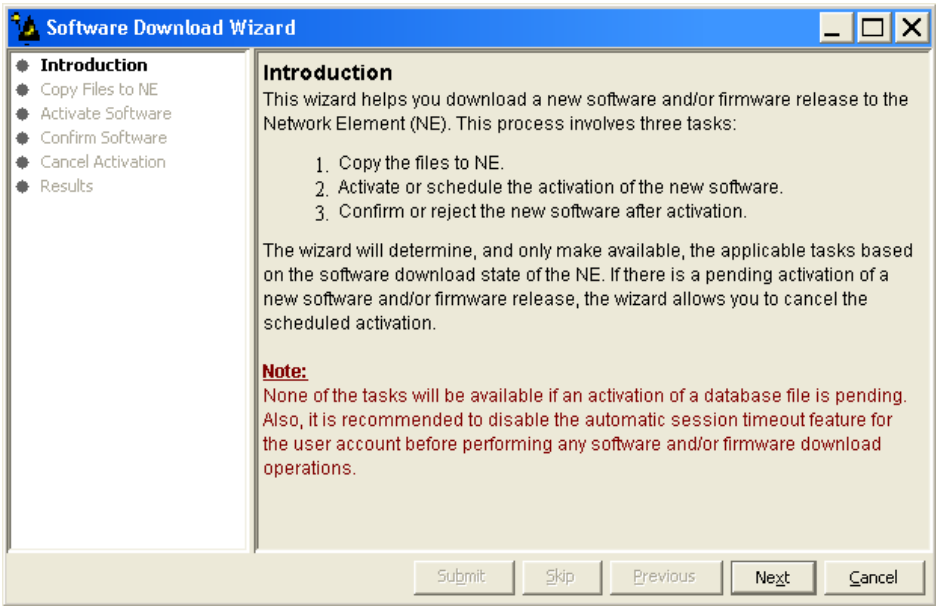


Figure 212: Example Software Download Wizard Introduction Screen

Step 71
Click *Next*.

The *Copy Files to NE* screen opens.

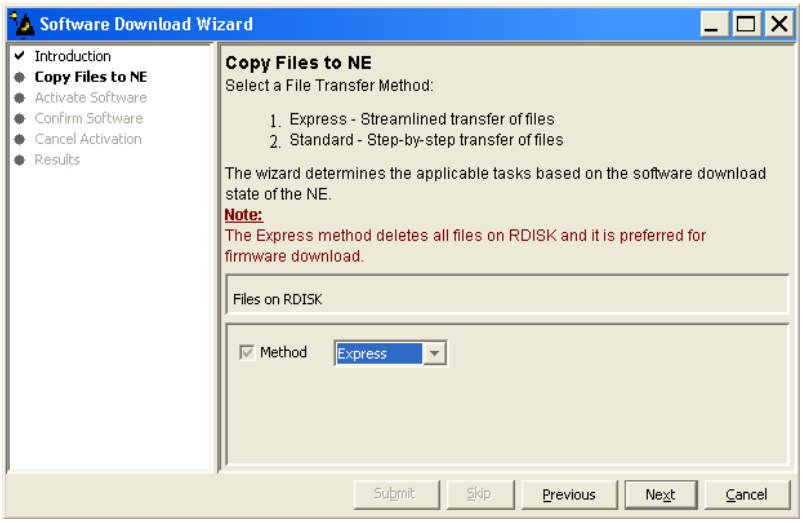


Figure 213: Example Software Download Wizard Copy Files to NE Screen

Step 72
Verify that the *Express* option is selected in the *Method* drop-down list.

Note: *The Express method is used to copy the software file from the random access memory disk (RDISK) of the Local NE to the standby nonvolatile memory (SNVM) of the Remote NE. Fujitsu recommends this method because it automatically deletes unnecessary files to make space for new files on the random access memory disk (RDISK) and standby nonvolatile memory (SNVM).*

Step 73
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

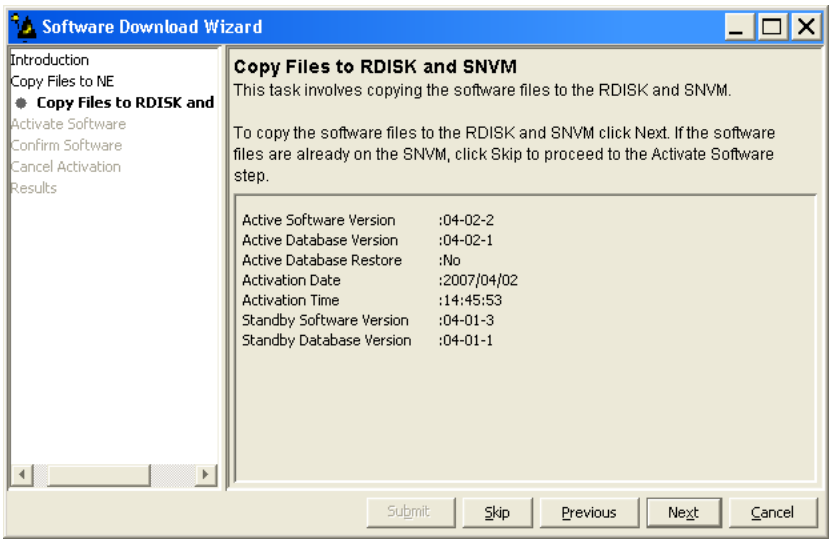


Figure 214: Example Software Download Wizard Copy Files to RDISK and SNVM Screen

Step 74
Verify that the *Active Software Version* is *04-02-2* (or later), and then click *Next*.

Note: *The current software must be Release 4.2 (or later). If the software is an earlier release, perform the procedures in* Upgrading System Software from Release 4.1*, before performing the upgrade to Release 6.1.*

The *Select Host* screen opens.

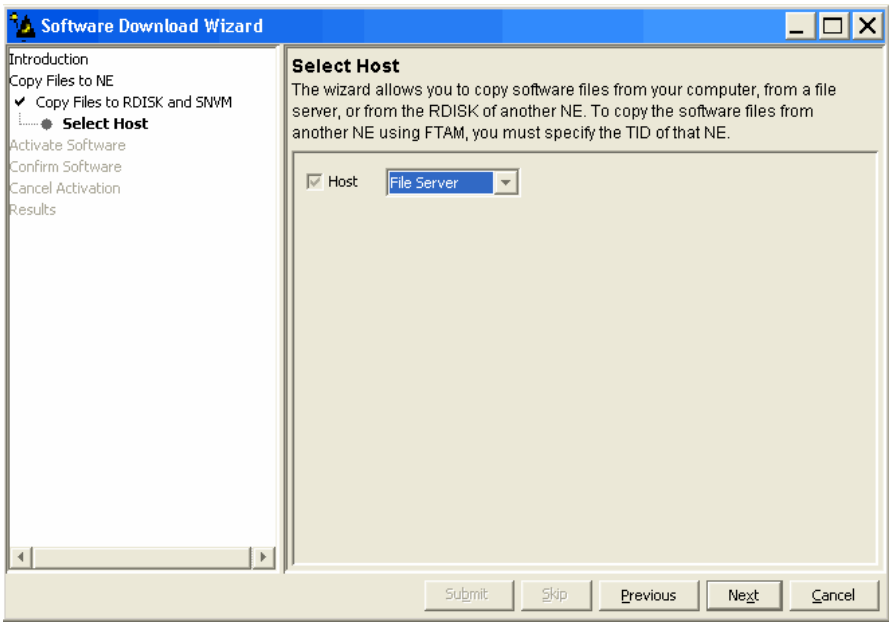


Figure 215: Example Software Download Wizard Select Host Screen

Download Software Program File from Another NE

Step 75
From the *Host* drop-down list, select *Another NE*.

The *Select Host* screen displays an additional field.

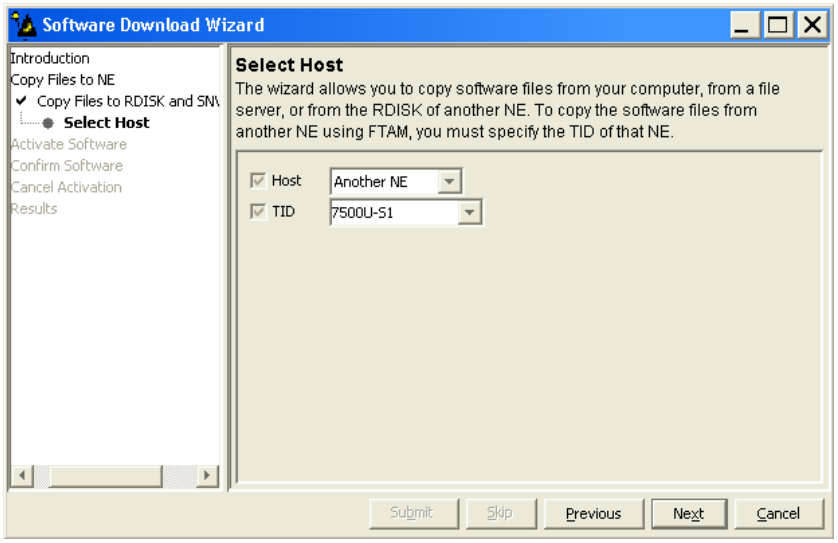


Figure 216: Example Software Download Wizard Select Host–Another NE Selected

Step 76
From the *TID* drop-down list, select the TID of the Local NE.

Step 77
Click *Next*.

The *Select Files* screen appears.

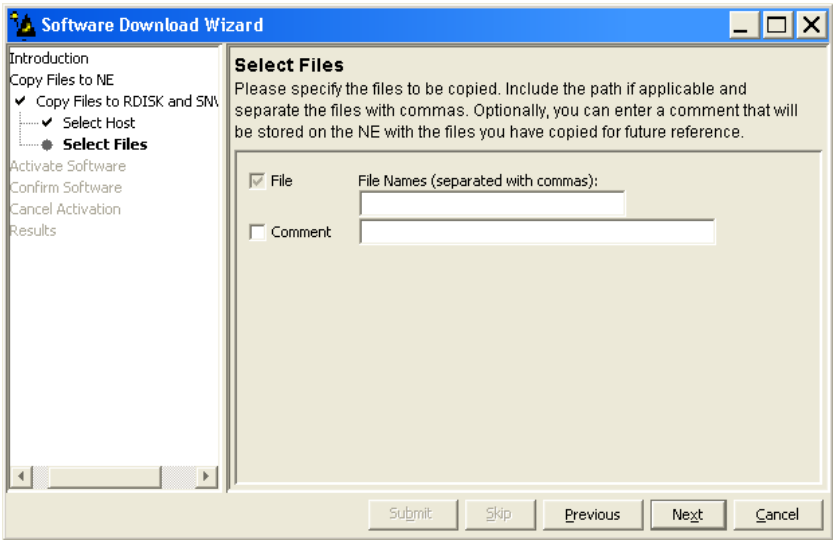


Figure 217: Example Software Download Wizard Select Files Screen

Step 78
Is the system being upgraded to a release earlier than Release 5.2?

If YES:
In the *File* text box, enter the file name of the software file separated by a comma (for example, F7504021.PGM).

If NO:
Each file must be downloaded separately. Enter the file name of the first software file for download (for example, F7507012.PGM), and make a note of the other firmware file (for example, B7507012.PGM) to be downloaded later.

Step 79
In the *Comment* text box, enter comments.

Note: *Fujitsu recommends the user's name (or initials) and the date of upgrade.*

Step 80
Click *Next*.

The *Enter Signatures* screen appears.

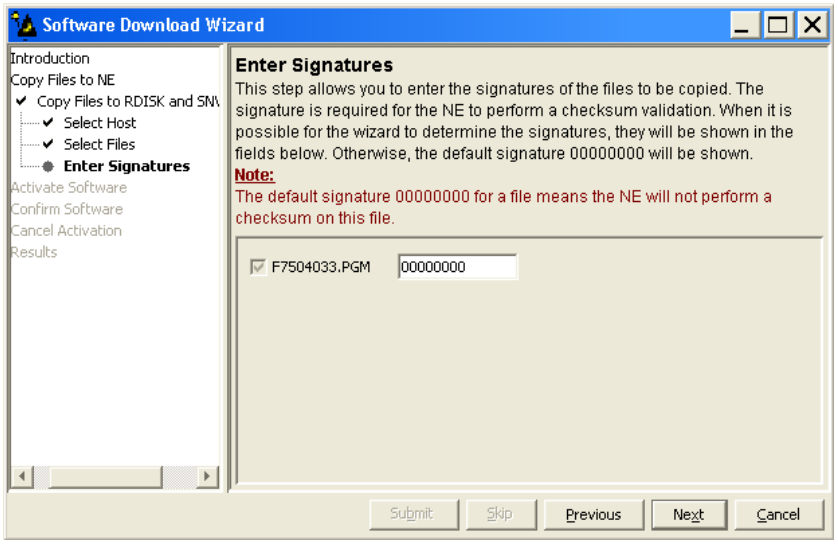


Figure 218: Example Software Download Wizard Enter Signatures Screen

Note: *When the files are being copied from another NE, the signature fields are populated with zeros by default (00000000). In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

Step 81
Click *Next*.

The *Copy to RDISK and SNVM* screen appears.

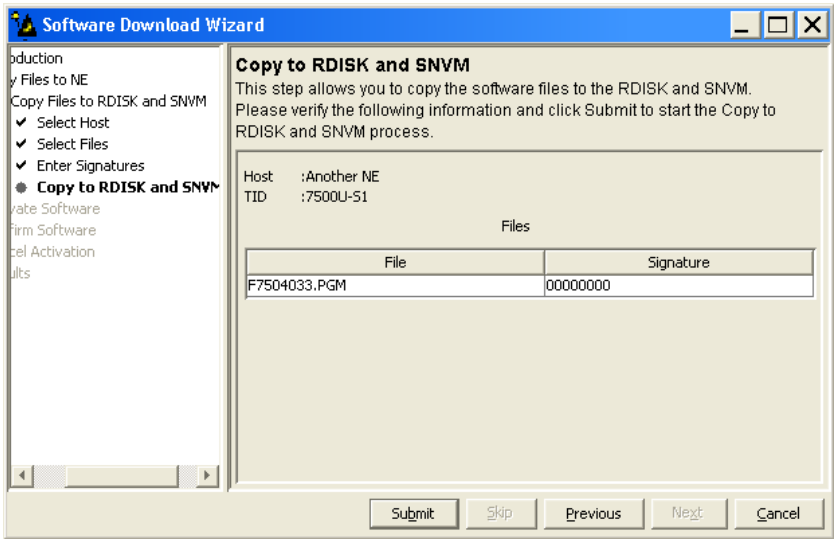


Figure 219: Example Software Download Wizard Copy to RDISK Screen

Step 82
Click *Submit*.

A *Performing Copy File* window opens, displaying the progress of the copying of the software program file from the RDISK of the Local NE.

Note: *The file can take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

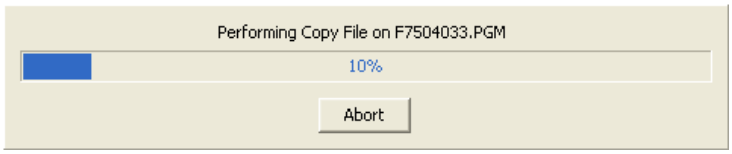


Figure 220: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen opens.

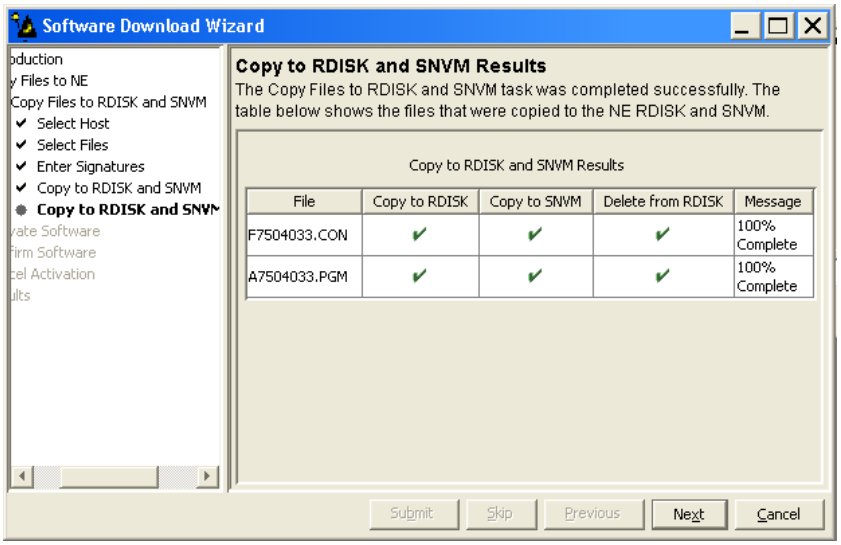


Figure 221: Example Software Download Wizard Copy to RDISK Results Screen

Step 83
Have all the necessary software files been successfully downloaded?

If YES:
Go to Step 85.

If NO:
Click Cancel and then Exit to close the wizard. Proceed to the next step.

Step 84
Repeat Steps 46 through 82 to download the other software files (F75xxxxx.PGM, B75xxxxx.PGM, and C75xxxxx.PGM [Release 7.1 or later]). Then continue with the next step.

Note: *Refer to the tables in the Software Requirements section for the required system software files required for a specific software upgrade.*

Activate Software

Step 85
Click *Next*.

The *Activate Software* screen opens.

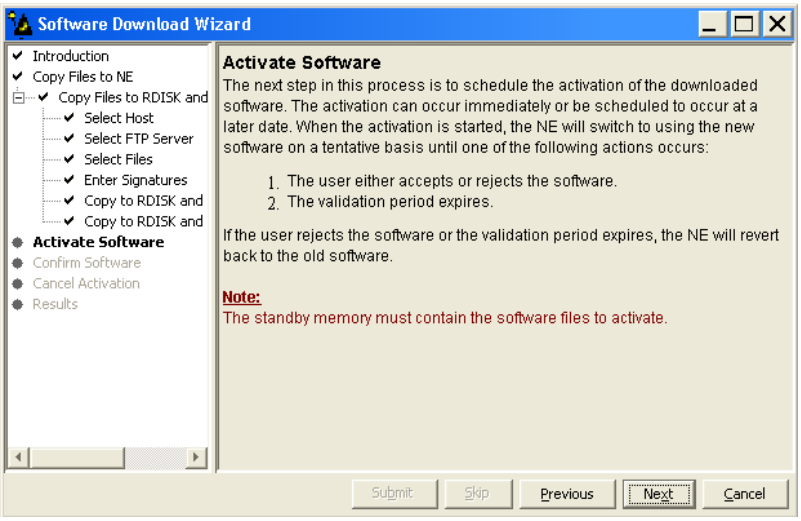


Figure 222: Example Software Download Wizard Activate Software Screen

Step 86
Click *Next*.

The *Software Activation Parameters* screen opens.

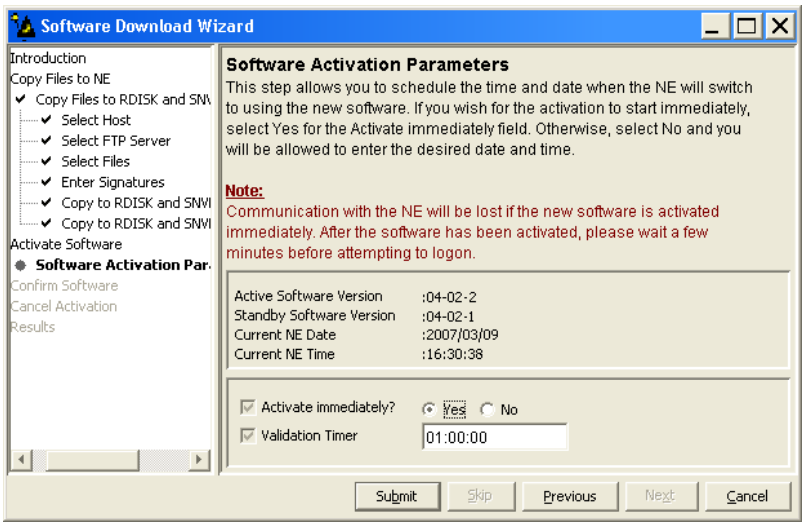


Figure 223: Example Software Download Wizard Software Activation Parameters Screen

Step 87
Do you want to activate the firmware and software immediately?

If YES:
Continue with the next step.

If NO:
Go to Step 94.

Step 88
Verify *Yes* is selected for the *Activate immediately* option.

Step 89
In the *Validation Timer* text box, enter the desired time before the system reverts back to the previous software (the default is 01:00:00 [1 hour]).

Step 90
Click *Submit*.

The *Software Activation Result* screen opens.

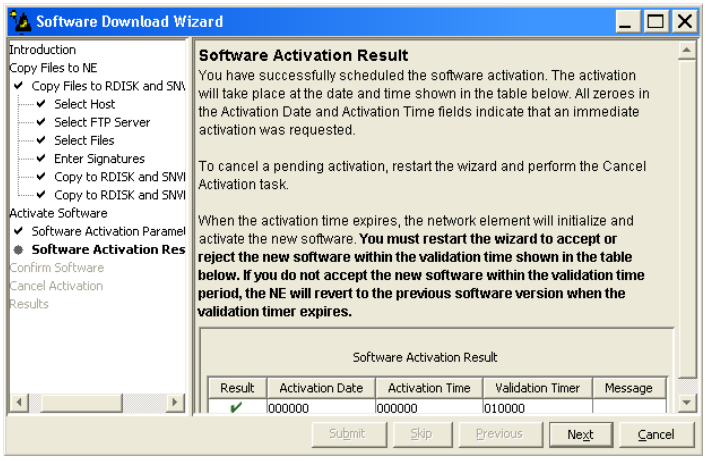


Figure 224: Example Software Download Wizard Software Activation Result Screen

Step 91
Click *Next*.

A *Warning* dialog box opens.

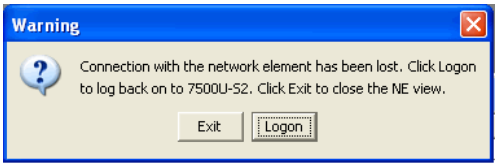


Figure 225: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 92
Wait for software reset (NEM FAIL/SVC LED is green and NOT READY LED is amber), then click *Logon*.

The *Software Activation Result* screen closes, and the Software Download wizard closes.

Step 93
Go to Step 99.

Step 94
Select *No* for the *Activate immediately* option.

The *Software Activation Parameters* screen displays additional fields.

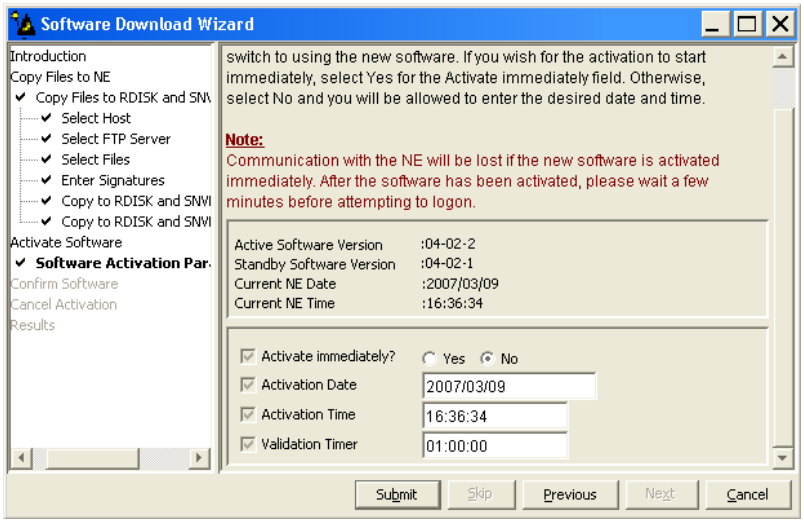


Figure 226: Example Software Activation Parameters–Scheduled Activation

a) Enter the *Activation Date* for the firmware and software activation.

b) Enter the *Activation Time* for the firmware and software activation.

c) Enter the *Validation Time* for the firmware and software activation.

Step 95
Click *Submit*.

The *Software Activation Result* screen opens.

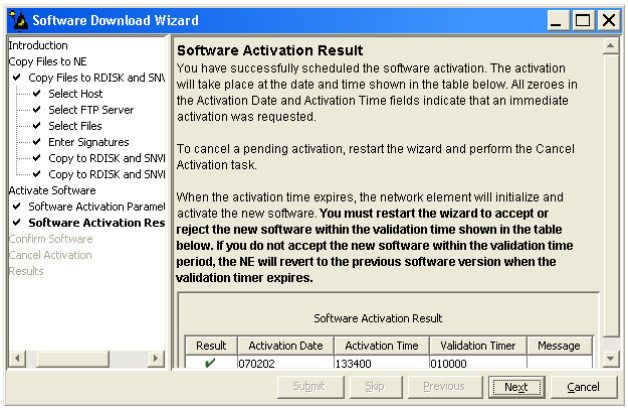


Figure 227: Example Software Download Wizard Software Activation Result Screen

Step 96
Click *Next*.

The *Results* screen opens.

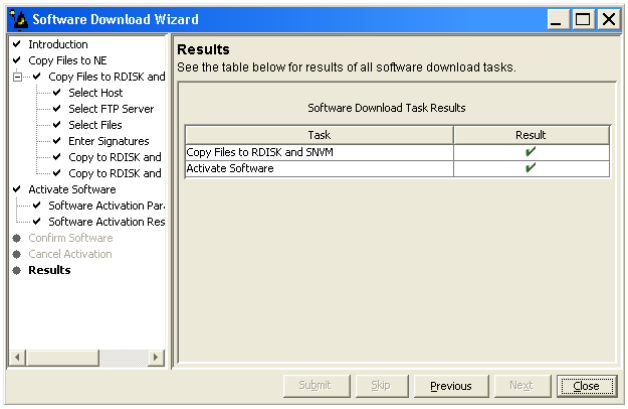


Figure 228: Example Software Download Wizard Results Screen

Step 97
Click *Close*.

The Software Download wizard closes. You may continue working in the NETSMART 500 environment and stay logged on to the Remote NE. When the activation date and time is reached, you are logged off the NE and a *Warning* dialog box appears.

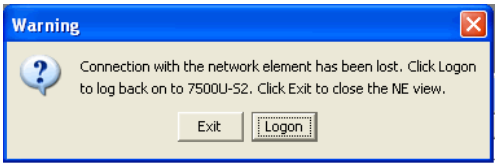


Figure 229: Example of a Typical Warning Dialog Box

Attention: *The NE takes approximately 10 minutes to reset before allowing another logon. During this time, the NOT READY LEDs on the NEM Shelf Processor and OSC plug-in units are lit amber.*

Step 98
Wait for software reset (NEM FAIL/SVC LED is green and NOT READY LED is amber), then click *Logon*.

The NETSMART 500 window closes.

Confirm Software Download

Note: *You must accept the new software load before the validation timer expires. Otherwise, the system software will revert back to the previous load.*

Step 99
Log back on the Remote NE. Refer to Step 3, if necessary.

Step 100
From the menu bar, select *Wizards* > *Software Download*.

The Software Download wizard starts and the *Introduction* screen opens.

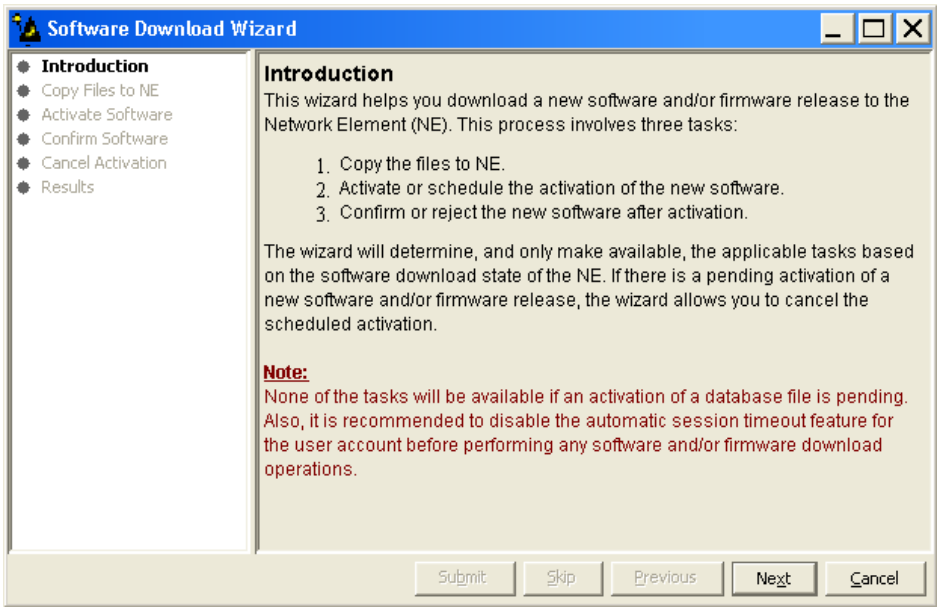


Figure 230: Example Software Download Wizard Introduction Screen

Step 101
Click *Next*.

The *Confirm Software* screen opens.

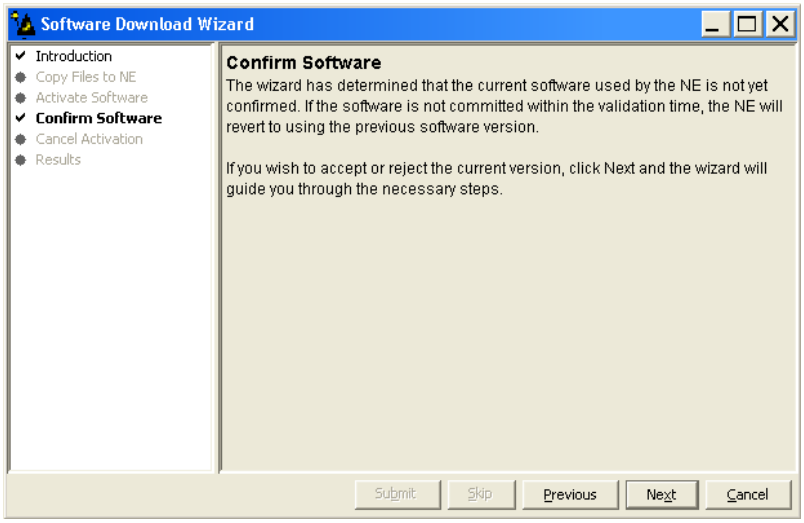


Figure 231: Example Software Download Wizard Confirm Software Screen

Step 102
Click *Next*.

The *Accept/Reject Software* screen opens.

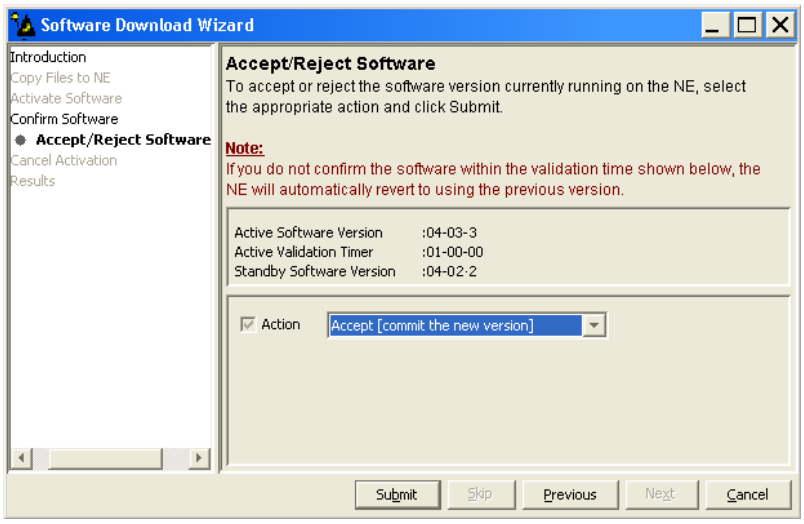


Figure 232: Example Software Download Wizard Accept/Reject Software Screen

Step 103
Verify that the *Accept [commit the new version]* option is selected in the *Action* drop-down list.

Step 104
Click *Submit*.

A progress bar displays while the validation timer is cancelled and the software is accepted.

Once the software is accepted, the *Software Confirmation Result* screen opens.

Note: *The screen may take several minutes to open.*

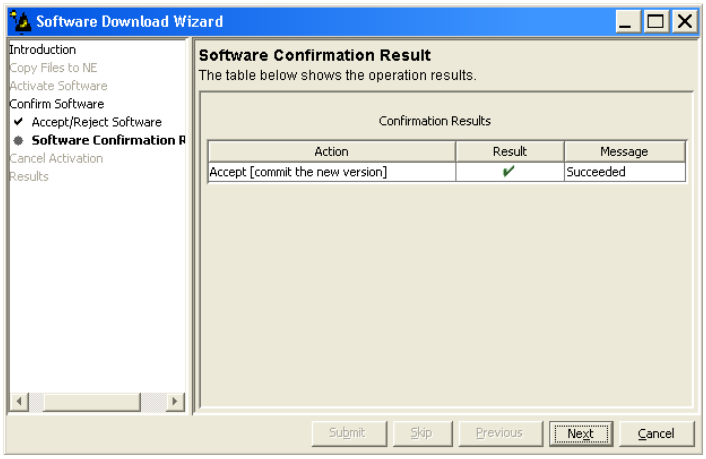


Figure 233: Example Software Download Wizard Software Confirmation Result Screen

Step 105
Click *Next*.

The final *Results* screen opens.

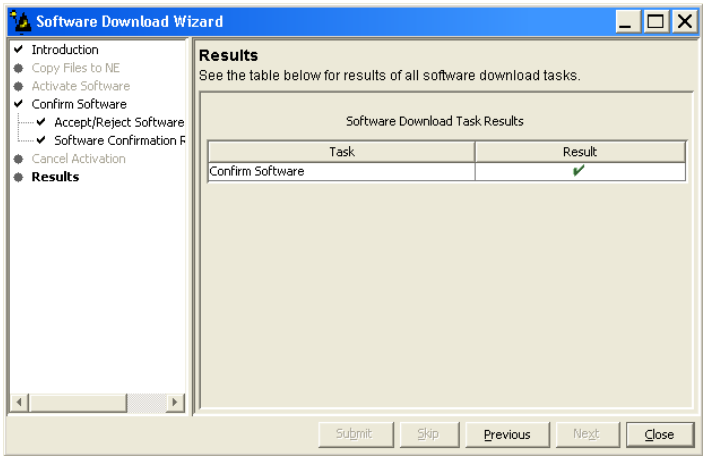


Figure 234: Example Software Download Wizard Results Screen

Step 106
Click *Close*.

The *Results* screen closes and the Software Download wizard closes.

After the system software is activated and the latest firmware file (generic) is downloaded to the system, the system may generate some firmware version mismatch alarms (FVM) against individual plug-in units with incompatible firmware versions.

Step 107
Retrieve alarms and conditions on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 108
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment, for information on clearing FVM alarms. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

Caution: *Installing new firmware on a plug-in unit programs the programmable hardware on the plug-in unit and can impact traffic associated with the plug-in unit. Firmware upgrade and activation on traffic carrying plug-in units can be remotely executed as needed using the INIT-EQPT command and should be scheduled at an appropriate time to avoid service interruption. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

If NO:
Proceed to the next step.

Step 109
Is the system now running the required system software?

Note: *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 before being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x or 8.x.*

If YES:
Proceed to the next step.

If NO:
Repeat the procedures in Upgrading System Software Using NETSMART 500 Software Download Wizard and Upgrade System Software from Another NE Using Software Download Wizard to upgrade to the required system software.

Step 110
Is the system now running Release 8.1 system software?

If YES:
Proceed to the next step.

If NO:
Log off the NE. This procedure is complete.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to confirm.

Step 111
Should the Expansion Pack files be downloaded now?

Attention: *The Expansion Pack files are required for Release 8.1. The Expansion Pack firmware files allow for full support of all FWDL plug-in unit firmware files.*

If YES:
Go to Download Firmware Expansion Pack Files Using TL1Commands or Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard.

If NO:
Log off the NE. This procedure is complete.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to confirm.

✔ This procedure is complete.

3.5 Download Firmware Expansion Pack Files Using TL1Commands

In this section:

This section provides procedures to download Expansion Pack firmware files for a FLASHWAVE 7500 NE with Release 8.1 or later software. Release 8.1 introduced the Firmware Expansion Pack for FLASHWAVE 7500 software. The Expansion Pack allows full support of all FWDL plug-in unit firmware files. The Firmware Expansion Pack also provides future firmware support unrestricted by system processor memory. The Expansion Pack stores the required unit firmware files in the active and standby memory locations on the system processor (MPMA-SHP3/ MPMA-SHP4 and SCMA-SCC4) until they are required, and then the firmware files are downloaded to the appropriate plug-in unit. For more details about Expansion Pack, refer to Maintenance under System Firmware Storage.

Perform the procedures in this section only after successful completion of the system software upgrade to Release 8.1 or later, including native firmware files (for example, A7509011.PGM, B7509011.PGM, and C7509011.PGM).

Caution: *The procedures in this section are only for NEs with Release 8.1 or later software. Refer to Upgrading System Software from Release 4.2 or Later if system software needs to be upgraded to Release 8.1 or later.*

Caution: *After system software has been upgraded to Release 8.1 or later, including native firmware files (for example, A7509011.PGM, B7509011.PGM, and C7509011.PGM), and the Expansion Pack firmware files have been downloaded to the system, the system may generate some firmware version mismatch (FVM) alarms against individual plug-in units with incompatible firmware versions. The firmware version on the unit is not automatically updated during a system software upgrade operation. Upgrading the firmware on the unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit using the TL1 command INIT-EQPT at an appropriate time by following local practices. For more details, refer to Maintenance.*

Software Download Prerequisites

Configurations

To perform software download, connections must exist for file transfer between the node and the file server (repository for Expansion Pack firmware files). The two basic configurations are:

- Configuration 1—The file server connects to the target node through the IP network as shown in the following figure.

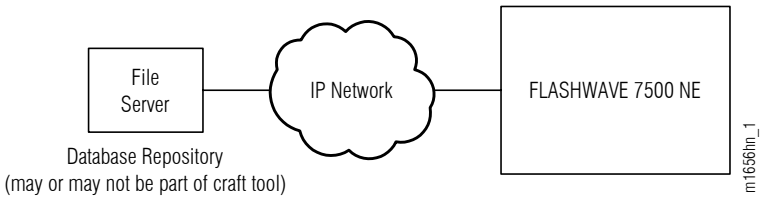


Figure 235: Configuration 1–File Server Connects to Target Node through IP

- Configuration 2– The file server connects to the gateway network element (GNE) through the IP network, and the GNE connects to the target node through SDCC as shown in the following figure.

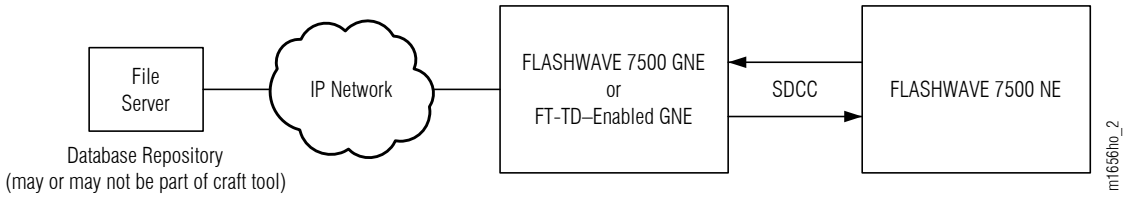


Figure 236: Configuration 2–File Server Connects to GNE through IP, and GNE Connects to Target Node through SDCC

Methods of File Transfer

The FLASHWAVE® 7500 system supports three methods of file transfer. The following table lists the three methods along with the applicable configuration and prerequisites. The procedures in this chapter accommodate all three methods of file transfer.

Table 41: Method of File Transfer Prerequisites

File Transfer Method	Prerequisites	Proceed to
File transfer through IP connection using CPY-FILE	• IP connection exists between file server and target NE.	Download Firmware Expansion Pack Files from File Server to Target NE (Using CPY-FILE)
One-step FT-TD file transfer through GNE using COPY-RFILE	• IP connection exists between file server and GNE. • SDCC connection exists between GNE and target NE. • GNE is FT-TD enabled. • System software on target NE is Release 5.2 or later.	Download Firmware Expansion Pack Files from File Server to Target NE (Using COPY-RFILE)

Table 41: Method of File Transfer Prerequisites (Cont.)

File Transfer Method	Prerequisites	Proceed to
Two-step file transfer through GNE using CPY-FILE	• IP connection exists between file server and GNE. • SDCC connection exists between GNE and target NE.	Download Firmware Expansion Pack Files from File Server to GNE to Target NE (Using CPY-FILE)

All releases of the FLASHWAVE 7500 system support file transfer using the CPY-FILE command. Starting with Release 5.2, the FLASHWAVE 7500 system also supports file transfer using the COPY-RFILE command, which implements File Transfer–Translation Device (FT-TD) protocol.

In Configuration 2 applications (Figure 152), the FT-TD method of file transfer is more efficient because file transfer can be accomplished with a single COPY-RFILE command instead of two CPY-FILE commands. Additionally, if COPY-RFILE is used, the GNE may be any FT-TD–enabled gateway NE, not necessarily a FLASHWAVE 7500 NE.

Prerequisites

Before proceeding with this procedure, do the following:

- Select a method of file transfer (see previous section), and verify that the prerequisites listed for the chosen method of file transfer are satisfied.
- Ensure that the craft tool is connected and able to log on the target NE. (Refer to Craft and OSS.)

  Note: *If the craft tool connection is through the serial port, the file server must be separate from the craft tool.*

- Verify that the user has user privilege code (UPC) Level 4 access and that the automatic time-out option is set to No as described in Craft and OSS.

3.5.1 Download Firmware Expansion Pack Files from File Server to Target NE (Using CPY-FILE)

The following figure shows a flowchart for the subprocedure.

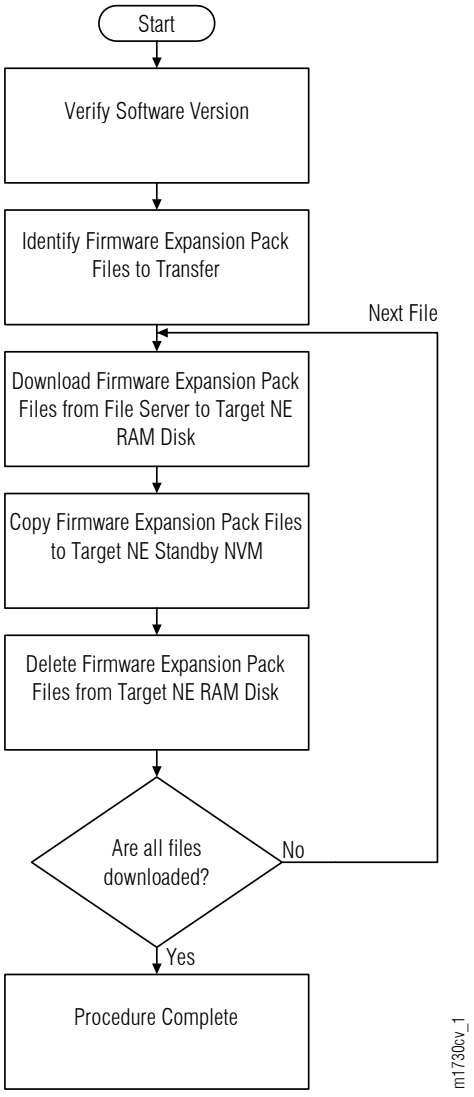


Figure 237: Download Firmware Expansion Pack Files from File Server to Target NE (Using CPY-FILE) (Subprocedure Flowchart)

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a FWDL or SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Download files to target NE as follows:

Note: *Default values are shown in bold.*

Verify NE Software Version

Before downloading Firmware Expansion Pack files, the current system software version must be Release 8.1 or later.

Follow these steps to verify the current software release is Release 8.1 or later:

Step 1
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART® 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start > All Programs > Fujitsu > NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select *NE > Logon*. ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections: For **TERM1** (Serial): TID: FUJITSU User ID: ROOT Password: ROOT/(Route66K) Conn. Mode: Serial Comm. Port: COMx (for example, COM2) Configure: use default[27] For **TERM2** (TCP/IP): TID: FUJITSU User ID: ROOT Password: ROOT/(Route66K) Conn. Mode: TCP/IP IP Address: 192.168.1.1 Port: 2024

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

[27] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

After a successful logon:

- **TL1 user interface**–The FLASHWAVE 7500 system responds with the normal, completed (COMPLD) message.
- **NETSMART 500 user interface**–The NETSMART 500 NE View provides a graphical user interface for provisioning and monitoring the FLASHWAVE 7500 system.

Step 2
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Step 3
Retrieve and verify software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID:AID:CTAG;`
AID:
• ACT, STBY, **ALL**
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	NE ▸ *Systems Operations*
	Click the Attributes tab.

Step 4
Is the current software version Release 8.1 or later?

Note: *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 before being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x, 8.x, or 9.1.*

If YES:
Go to next step.

If NO:
Based on the current software release, follow the procedures in Upgrading System Software from Release 4.1 and/or Upgrading System Software from Release 4.2 or Later to upgrade to Release 8.1 or later.

Identify Firmware Expansion Pack Files to Transfer

Step 5
Identify and record the configuration, program, and Firmware Expansion Pack files to be downloaded. Refer to Software Requirements for the required Firmware Expansion Pack file names for a specific software release. The following table provides an example of the required Firmware Expansion Pack file names.

Example:

Release	Configuration File	Signature File	Firmware File(s)
Release 9.1	Z7509011.CON	Z7509011.SIG	Z7509011.PGM Y7509011.PGM

Step 6
From the set of files identified in the previous step, select a file that has not yet been downloaded.

Attention: *The Z75xxxxx.CON file will be downloaded along with the applicable Z75xxxxx.PGM and Y75xxxxx.PGM files.*

Note: *The Y750xxxx.PGM file is only applicable if upgrading to Release 9.1.x.*

Download Expansion Pack File from File Server to Target NE RAM Disk

Step 7
Copy the file identified in the previous step from the FTP server to the RAM disk of the target NE.

Note: *If this is the first time performing this step, copy the Z75xxxxx.CON file first.*

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction). This is the file, identified in the previous step, that you are currently downloading.

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to the following table.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU:139.145.23.43,Z7509011.CON,RDISK,Z7509011.CON:CTAG:::
OVERWRITE=Y,FTUID=\"swduser\",FTPID=\"moonrock\",FTPATH=\"C:\GENERICS\";
```

Table 42: CPY-FILE Keyword and Domain Input Parameters

Keyword	Domain (Default in Bold)	Description
OVERWRITE[28]	Overwrite files	
	Y	Write over files with the same name at DST
	N	Do not write over files with the same name at DST
COMMENT	\"xxxxx\" **null**	Sets the user-defined comment, where the comment is up to 60 ASCII characters delineated by escape quotes ***Note:*** *The CPY-FILE command is denied if the COMMENT keyword exceeds 60 characters.*
SIGNATURE[29]	8 hex digits **00000000**	Signature code for each file. When more than one file is transferred, signatures are separated with an & character. ***Note:*** *If SIGNATURE is 0 (zero), the file checksum will not be performed.*
FTUID	\"xxxxx\" **null**	UID used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPID	\"xxxxx\" **null**	Password used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes

[28] OVERWRITE=Y must be specified when transferring a file from the FLASHWAVE 7500 NE to another location when using FTP or FTAM.
[29] The SIGNATURE keyword is ignored when transferring a file from the NE to any other location.

Table 42: CPY-FILE Keyword and Domain Input Parameters (Cont.)

Keyword	Domain (Default in Bold)	Description
FTPATH	\"xxxxx\" **null**	Path to the control file on the server; up to 40 ASCII characters delineated by escape quotes

Step 8
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Copy Expansion Pack File to Target NE Standby NVM

Step 9
Copy the file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- CON (configuration file)
- PGM (program file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by *, or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,Z7509011.CON,STBY,:CTAG::CON:
COMMENT=\"RELEASE_8.1\";
```

Step 10
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Delete Expansion Pack File from Target NE RAM Disk

Step 11
Delete the file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
DLT-FILE:FUJITSU:Z7509011.CON:CTAG;
```

Step 12
Have you downloaded all of the identified Expansion Pack files?

Note: *Refer to Software Requirements for the Firmware Expansion Pack file names.*

If YES:
Log off the NE. This procedure is complete.

If NO:
Go to Step 6, and repeat this procedure to download the next Expansion Pack file.

✔ This procedure is complete.

3.5.2 Download Firmware Expansion Pack Files from File Server to Target NE (Using COPY-RFILE)

The following figure shows a flowchart for the subprocedure.

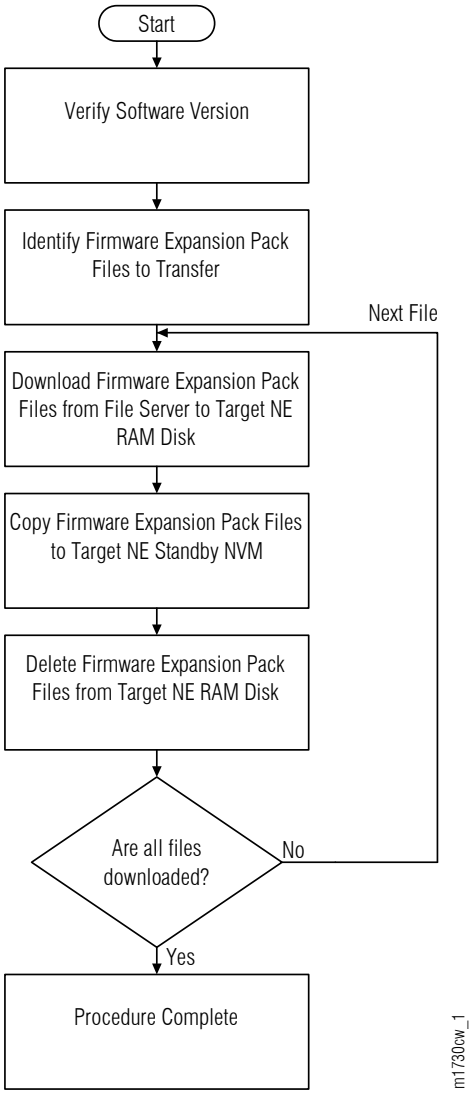


Figure 238: Download Firmware Expansion Pack Files from File Server to Target NE (Using COPY-RFILE) (Subprocedure Flowchart)

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a FWDL or SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Download files to target NE as follows:

Note: *Default values are shown in bold.*

Step 1
Verify that active software load is Release 5.2 or later (GISSUE is 05-02-01 or later).

TL1

```
RTRV-VERSION:TID::CTAG;
```

Example:

```
RTRV-VERSION:FUJITSU::CTAG;
```

Step 2
Is the active GISSUE value 05-02-01 or higher?

If YES:
Proceed to the next step.

If NO:
The target node does not support the COPY-RFILE command. Choose a different method of file transfer.

Verify NE Software Version

Before downloading Firmware Expansion Pack files, the current system software version must be Release 8.1 or later.

Follow these steps to verify the current software release is Release 8.1 or later:

Step 3
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART® 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start > All Programs > Fujitsu > NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select *NE > Logon*. ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

<table>
<tr><th>TL1</th><th>NETSMART® 500</th></tr>
<tr><td>ACT-USER:TID:UID:CTAG::PID;
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;</td><td>For TERM1 (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial
Comm. Port: COMx (for example, COM2)
Configure: use default[30]

For TERM2 (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.
The NETSMART 500 NE View opens.
The Security Message dialog box opens.
Click OK.
Note: Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.</td></tr>
</table>

After a successful logon:

- **TL1 user interface**–The FLASHWAVE 7500 system responds with the normal, completed (COMPLD) message.
- **NETSMART 500 user interface**–The NETSMART 500 NE View provides a graphical user interface for provisioning and monitoring the FLASHWAVE 7500 system.

Step 4
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

[30] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 5
Retrieve and verify software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID:AID:CTAG;`
AID:
• ACT, STBY, **ALL**
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	NE ▸ *Systems Operations*
	Click the Attributes tab.

Step 6
Is the current software version Release 8.1 or later?

Note: *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 before being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x, 8.x, or 9.1.*

If YES:
Go to next step.

If NO:
Based on the current software release, follow the procedures in Upgrading System Software from Release 4.1 and/or Upgrading System Software from Release 4.2 or Later to upgrade to Release 8.1 or later.

Identify Expansion Pack Files to Transfer

Step 7
Identify and record the configuration, program, and Firmware Expansion Pack files to be downloaded. Refer to Software Requirements for the required Firmware Expansion Pack file names for a specific software release. The following table provides an example of the required Firmware Expansion Pack file names.

Example:

Release	Configuration File	Signature File	Firmware File(s)
Release 9.1	Z7509011.CON	Z7509011.SIG	Z7509011.PGM Y7509011.PGM

Step 8
From the set of files identified in the previous step, select a file that has not yet been downloaded.

Attention: *Start with Z75xxxxx.CON file first in the set. The procedure will be performed once for each file to be downloaded.*

Note: *The Y750xxxx.PGM file is only applicable if upgrading to Release 9.1.*

Download Expansion Pack File from File Server to Target NE RAM Disk

Step 9
Copy the file identified in the previous step from the FTP server to the RAM disk of the target NE.

Note: *If this is the first time performing this step, copy the Z75xxxxx.CON file first.*

TL1

```
COPY-RFILE:TID::CTAG::SWDL,SRCURL,DESTURL,OVERWRITE,FTTDURL;
```

TID:

- Target node SID (not GNE)

SRCURL:

- \"xxxxx\" (URL of the source file on remote file server). This is the file, identified in the previous step, that you are currently downloading.

DESTURL:

- \"xxxxx\" (URL of file destination on target node RAM disk)

OVERWRITE:

- YES/**NO**

FTTDURL

- \"xxxxx\" (URL of FT-TD server, GNE)

Example:

```
COPY-RFILE:FUJITSU::CTAG::SWDL,
\"ftp://user1:password1@139.145.23.43/C:\GENERICS\Z7509011.CON\",
\"file:///Z7509011.CON\",OVERWRITE=Y,\"fttd://user1:password1@FUJITSU-GNE\";
```

Step 10
Verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- File name of source file specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Copy Expansion Pack File to Target NE Standby NVM

Step 11
Copy the file from the RAM disk into standby NVM.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- File name of source file specified in previous step

FTYPE:

- CON (configuration file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,Z7509011.CON,STBY,:CTAG::CON:
COMMENT=\"RELEASE_8.1\";
```

Step 12
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- File name of source file specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Delete Expansion Pack File from Target NE RAM Disk

Step 13
Delete the file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- File name of source file specified in previous step
- **ALL** (null)

Example:

```
DLT-FILE:FUJITSU:Z7509011.CON:CTAG;
```

Step 14
Have you downloaded all of the identified Expansion Pack files?

Note: *Refer to Software Requirements for the Firmware Expansion Pack file names.*

If YES:
Log off the NE. This procedure is complete.

If NO:
Go to Step 8, and repeat this procedure to download the next Expansion Pack file.

✔ This procedure is complete.

3.5.3 Download Firmware Expansion Pack Files from File Server to GNE to Target NE (Using CPY-FILE)

The following figure shows a flowchart for the subprocedure.

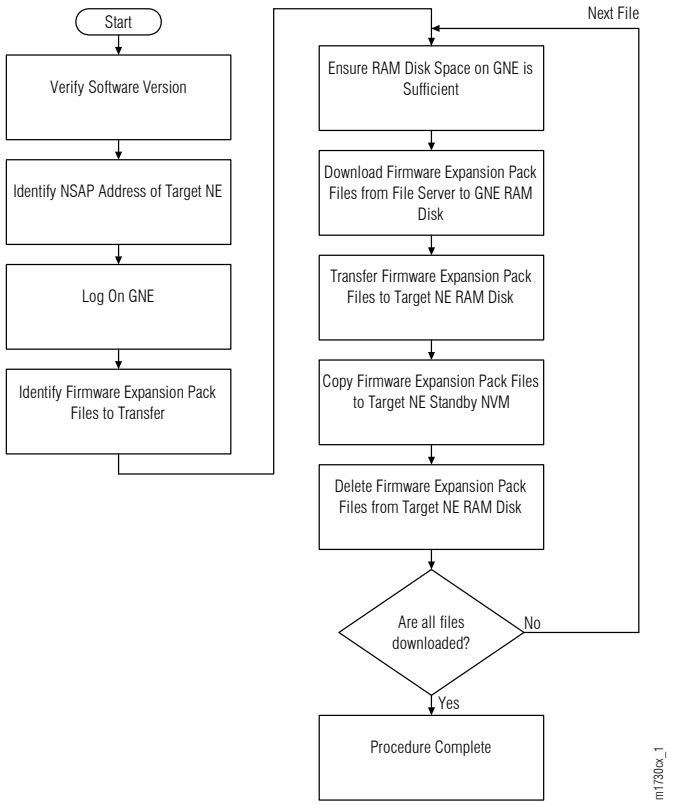


Figure 239: Download Firmware Expansion Pack Files from File Server to GNE to Target NE (Using CPY-FILE) (Subprocedure Flowchart)

Caution: *Installing new firmware on a plug-in unit programs programmable hardware on the plug-in unit and can impact traffic associated with that plug-in unit. Also, when plug-in units are plugged into the system or are reseated, they are programmed with the appropriate firmware file for the plug-in unit.*

The following information should be known:

- IP address of the FTP server
- User name and password for accessing the FTP server
- Path to the directory on the FTP server containing the software files

Caution: *In this procedure, the COMPLD response to the CPY-MEM command does not indicate that the copy is complete, only that the command is being executed. The user must wait for a CPY-MEM-COMPL or CPY-MEM-FAIL autonomous message before sending another software download (SWDL)–related command. Attempting to send these commands before receiving the completion message results in a DENY response (SARB). Before proceeding to the next step, verify receipt of a completed (COMPLD) response to each command. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a FWDL or SWDL is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Download files to target NE as follows:

Note: *Default values are shown in bold.*

Verify NE Software Version

Before downloading Firmware Expansion Pack files, the current system software version must be Release 8.1 or later.

Follow these steps to verify the current software release is Release 8.1 or later:

Step 1
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

<table>
<tr><th>TL1</th><th>NETSMART® 500</th></tr>
<tr><td>Start a terminal or terminal emulator program (for example, HyperTerminal®).

For TERM1 (Serial):
Press CTRL+X.

For TERM2 (TCP/IP):
Establish a Telnet session using IP address 192.168.1.1 and default port 23.

The Welcome screen opens.
Press 3 for TL1.</td><td rowspan="2">To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select NE > Logon.

Note: If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.

The NE Logon dialog box opens.
Make the following selections:

For TERM1 (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial

Comm. Port: COMx (for example, COM2)

Configure: use default[31]

For TERM2 (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024</td></tr>
<tr><td>ACT-USER:TID:UID:CTAG::PID;
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)

Example:
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;</td></tr>
<tr><td colspan="2">Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.</td></tr>
</table>

[31] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

After a successful logon:

- **TL1 user interface**–The FLASHWAVE 7500 system responds with the normal, completed (COMPLD) message.
- **NETSMART 500 user interface**–The NETSMART 500 NE View provides a graphical user interface for provisioning and monitoring the FLASHWAVE 7500 system.

Step 2
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

Step 3
Retrieve and verify software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID:AID:CTAG;`
AID:
• ACT, STBY, **ALL**
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	NE ▸ *Systems Operations*
	Click the Attributes tab.

Step 4
Is the current software version Release 8.1 or later?

Note: *FLASHWAVE 7500 NEs loaded with Release 4.x software must be upgraded to Release 5.1 before being upgraded to Release 5.2, 5.2.2, or 6.x. After upgrading to Release 5.2 or 5.2.2, the FLASHWAVE 7500 NE can be upgraded to Release 6.x or 7.x. After upgrading to Release 6.x, the FLASHWAVE 7500 NE can be upgraded to Release 7.x, 8.x, or 9.1.*

If YES:
Go to next step.

If NO:
Based on the current software release, follow the procedures in Upgrading System Software from Release 4.1 and/or Upgrading System Software from Release 4.2 or Later to upgrade to Release 8.1 or later.

Identify NSAP Address of Target NE

Step 5
Retrieve the AREAADDR and the SYSID of the target NE.

TL1

```
RTRV-NLP:TID::CTAG;
```
TID:
- Target node SID (not GNE)

Example:
```
RTRV-NLP:FUJITSU::CTAG;
```

Response Example:
```
AREAADDR=39840F8000...SYSID=273B84CE...
```

Step 6
Use the AREAADDR and the SYSID retrieved in the previous step to determine the NSAP address of the target NE. Make a record of the NSAP address, which will be used later in Step 9.

Note: *The NSAP address consists of the AREAADDR (26 hex digits), the SYSID (12 hex digits), and the NSEL (always 00, but not displayed).*

If AREAADDR=39840F8000... and SYSID=273B84CE..., then the NSAP address is 39840F8000... 273B84CE...00.

Log On GNE

Step 7
If not already done, log on the GNE. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections: For **TERM1** (Serial): TID: FUJITSU User ID: ROOT Password: ROOT/(Route66K) Conn. Mode: Serial Comm. Port: COMx (for example, COM2) Configure: use default[32] For **TERM2** (TCP/IP): TID: FUJITSU User ID: ROOT Password: ROOT/(Route66K) Conn. Mode: TCP/IP IP Address: 192.168.1.1 Port: 2024

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Identify Expansion Pack Files to Transfer

Step 8

Identify and record the configuration, program, and Firmware Expansion Pack files to be downloaded. Refer to Software Requirements for the required Firmware Expansion Pack file names for a specific software release. The following table provides an example of the required Firmware Expansion Pack file names.

Example:

[32] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Release	Configuration File	Signature File	Firmware File(s)
Release 9.1	Z7509011.CON	Z7509011.SIG	Z7509011.PGM Y7509011.PGM

Step 9
From the set of files identified in the previous step, select a file that has not yet been downloaded.

Attention: *Start with Z75xxxxx.CON file first in the set. The procedure will be performed once for each file to be downloaded.*

Note: *The Y750xxxx.PGM file is only applicable if upgrading to Release 9.1.*

Ensure RAM Disk Space on GNE is Sufficient

Step 10
To ensure that sufficient space exists when the file is copied to the GNE RAM disk, view the current contents of the GNE RAM disk.

TL1

```
RTRV-FILE-RDISK:TID::CTAG;
```

Example:
```
RTRV-FILE-RDISK:FUJITSU-GNE::CTAG;
```

Step 11
If necessary, delete files on the GNE RAM disk to ensure sufficient space.

Note: *Ensure that the files on the GNE RAM disk are no longer needed before deleting them.*

TL1

```
DLT-FILE:TID:FILESPEC:CTAG;
```
FILESPEC:

- Name of file to delete (maximum of 12 alphanumeric characters with no format restrictions) or ALL

Example:
```
DLT-FILE:FUJITSU-GNE:ALL:CTAG;
```

Download Expansion Pack File from File Server to GNE RAM Disk

Step 12
Copy the file from the remote file system to the RAM disk on the GNE.

Note: *If this is the first time performing this step, copy the Z75xxxxx.CON file first.*

TL1

```
CPY-FILE:TID:SRC,SRCFILE,RDISK,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

TID:

- GNE SID

SRC:

- TCP/IP address of the FTP server (xxx.xxx.xxx.xxx)

  Note: *Refer the IP address of the FTP server recorded in* Prepare to Upgrade Using TL1.

SRCFILE:

- Name of file to be copied (maximum of 12 alphanumeric characters with no format restriction). This is the file, identified in Step 5, that you are currently downloading.

DSTFILE:

- Name assigned to the file at the copy destination (NE RAM disk) (DSTFILE file names should match SRCFILE file names.)

KEYWORD=DOMAIN:

- Refer to the following table.

  Note: *Refer to the values for the FTP server user ID, password, and path to the software files recorded in* Prepare to Upgrade Using TL1. *Those values are used here to set keywords FTUID, FTPID, and FTPATH.*

Example:

```
CPY-FILE:FUJITSU-GNE:139.145.23.43,Z7509011.CON,RDISK,Z7509011.CON:CTAG:::
OVERWRITE=Y,FTUID=\"swduser\",FTPID=\"moonrock\",FTPATH=\"C:\GENERICS\";
```

Table 43: CPY-FILE Keyword and Domain Input Parameters

Keyword	Domain (Default in Bold)	Description
OVERWRITE[33]	Overwrite files	
	Y	Write over files with the same name at DST
	N	Do not write over files with the same name at DST
COMMENT	\"xxxxx\" **null**	Sets the user-defined comment, where the comment is up to 60 ASCII characters delineated by escape quotes ***Note:*** *The CPY-FILE command is denied if the COMMENT keyword exceeds 60 characters.*
SIGNATURE[34]	8 hex digits **00000000**	Signature code for each file. When more than one file is transferred, signatures are separated with an & character. ***Note:*** *If SIGNATURE is 0 (zero), the file checksum will not be performed.*
FTUID	\"xxxxx\" **null**	UID used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes

[33] OVERWRITE=Y must be specified when transferring a file from the FLASHWAVE 7500 NE to another location when using FTP or FTAM.
[34] The SIGNATURE keyword is ignored when transferring a file from the NE to any other location.

Table 43: CPY-FILE Keyword and Domain Input Parameters (Cont.)

Keyword	Domain (Default in Bold)	Description
FTPID	\"xxxxx\" **null**	Password used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPATH	\"xxxxx\" **null**	Path to the control file on the server; up to 40 ASCII characters delineated by escape quotes

Transfer Expansion Pack File to Target NE RAM Disk

Step 13
Transfer the file from the GNE RAM disk to the target node RAM disk.

TL1

```
CPY-FILE:TID:RDISK,SRCFILE,NETADDR,DSTFILE:CTAG:::KEYWORD=DOMAIN;
```

TID:

- GNE SID

SRCFILE:

- Name assigned to file at the copy source (GNE RAM disk) (same as DSTFILE in the previous step); maximum of 12 alphanumeric characters with no format restrictions

NETADDR:

- NSAP address of the target node (from Step 2)

DSTFILE:

- Name assigned to file at the copy destination (target node RAM disk); maximum of 12 alphanumeric characters with no format restrictions

KEYWORD=DOMAIN:

- Refer to the following table.

Example:

```
CPY-FILE:FUJITSU-GNE:RDISK,Z7509011.CON,39840F8000...273B84CE...00,
Z7509011.CON:CTAG:::OVERWRITE=Y;
```

Table 44: CPY-FILE Keyword and Domain Input Parameters

Keyword	Domain (Default in Bold)	Description
OVERWRITE[35]	Overwrite files	
	Y	Write over files with the same name at DST
	N	Do not write over files with the same name at DST

[35] OVERWRITE=Y must be specified when transferring a file from the FLASHWAVE 7500 NE to another location when using FTP or FTAM.

Table 44: CPY-FILE Keyword and Domain Input Parameters (Cont.)

Keyword	Domain (Default in Bold)	Description
COMMENT	\"xxxxx\" **null**	Sets the user-defined comment, where the comment is up to 60 ASCII characters delineated by escape quotes ***Note:*** *The CPY-FILE command is denied if the COMMENT keyword exceeds 60 characters.*
SIGNATURE[36]	8 hex digits **00000000**	Signature code for each file. When more than one file is transferred, signatures are separated with an & character. ***Note:*** *If SIGNATURE is 0 (zero), the file checksum will not be performed.*
FTUID	\"xxxxx\" **null**	UID used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPID	\"xxxxx\" **null**	Password used to establish file forwarding protocol; up to 10 ASCII characters delineated by escape quotes
FTPATH	\"xxxxx\" **null**	Path to the control file on the server; up to 40 ASCII characters delineated by escape quotes

Step 14
On the target NE, verify RAM disk information.

TL1

```
RTRV-FILE-RDISK:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-RDISK:FUJITSU::CTAG;
```

Copy Expansion Pack File to Target NE Standby NVM

Step 15
Copy the file from the RAM disk into standby NVM.

[36] The SIGNATURE keyword is ignored when transferring a file from the NE to any other location.

TL1

```
CPY-MEM:TID:RDISK,SRCFILE,STBY,:CTAG::FTYPE:KEYWORD=DOMAIN;
```

SRCFILE:

- As specified in previous step

FTYPE:

- CON (configuration file)

KEYWORD=DOMAIN:

- COMMENT = User-defined comment of up to 60 ASCII characters delineated by \", or **null**

Example:

```
CPY-MEM:FUJITSU:RDISK,Z7509011.CON,STBY,:CTAG::CON:
COMMENT=\"RELEASE_8.1\";
```

Step 16
Verify standby NVM information.

TL1

```
RTRV-FILE-NVM:TID:AID:CTAG::::STBY;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
RTRV-FILE-NVM:FUJITSU::CTAG::::STBY;
```

Delete Expansion Pack File from Target NE RAM Disk

Step 17
Delete the file from the RAM disk.

TL1

```
DLT-FILE:TID:AID:CTAG;
```

AID:

- Value of SRCFILE specified in previous step
- **ALL** (null)

Example:

```
DLT-FILE:FUJITSU:Z7509011.CON:CTAG;
```

Step 18
Have you downloaded all of the identified Expansion Pack files?

Note: *Refer to Software Requirements for the Firmware Expansion Pack file names.*

If YES:
Log off the NE. This procedure is complete.

If NO:
Go to Step 9, and repeat this procedure to download the next Expansion Pack file.

✔ This procedure is complete.

3.6 Download Firmware Expansion Pack Files Using NETSMART 500 Expansion Pack Firmware Download Wizard

In this section:

About NETSMART 500 Expansion Pack Firmware Download Wizard

The NETSMART 500 Expansion Pack Firmware Download wizard assists you in downloading Expansion Pack firmware files for a FLASHWAVE 7500 NE. The NETSMART 500 Expansion Pack Firmware Download wizard is only applicable for Release 8.1 and later. For assistance, call the Fujitsu Technical Assistance Center at 1-800-USE-FTAC (1-800-873-3822).

Note: *Refer to the NETSMART 500 User Guide for complete instructions on starting the NETSMART 500 Expansion Pack Firmware Download wizard.*

The Software Download wizard assists you in:

- Downloading Expansion Pack Firmware to the NE
- Initializing firmware

The wizard determines the applicable tasks based on the software download state and makes available only the applicable tasks.

Note: *These tasks are not available if the NE is pending activation of a new software or database file.*

Caution: *Do not pull out the NEM Shelf Processor or OSC units while a software download (SWDL) is in progress. Pulling out any of these units can cause the download to be interrupted and an alarm (CPY-MEM-FAIL) to occur.*

3.6.1 Log On

Step 1
Ensure that the NEM Shelf Processor and OSC plug-in units are inserted in the NE and that the NE is powered up.

Step 2
Log on the NE.

Note: *To perform this procedure, the user must have privilege code (UPC) Level 4 access and the automatic time-out option (TMOUTA) must be set to False. Refer to* About Release 4.2 or Later System Software Upgrade.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up a direct craft interface connection. For detailed information, refer to* Craft Interface Operations .

NETSMART 500

To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select *NE > Logon*.

Note: *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.*

The NE Logon dialog box opens.
Make the following selections:

For **TERM2** (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 graphical user interface.*

Step 3

Retrieve alarms and conditions on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 4
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions, excluding FVM alarms (refer to Upgrading Firmware on Equipment for information on clearing FVM alarms). After all alarms and conditions are cleared (or accounted for), proceed to the following task.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to the following task.

Continue with next task ►

3.6.2 Download Expansion Pack Files

Step 1
From the menu bar, select *Wizards* > *Expansion Pack Firmware Download*.

Note: *When progressing through the screens in the Expansion Pack Firmware Download wizard, the current screen may momentarily gray before the next screen opens.*

The Expansion Pack Firmware Download wizard opens, showing the Introduction screen.

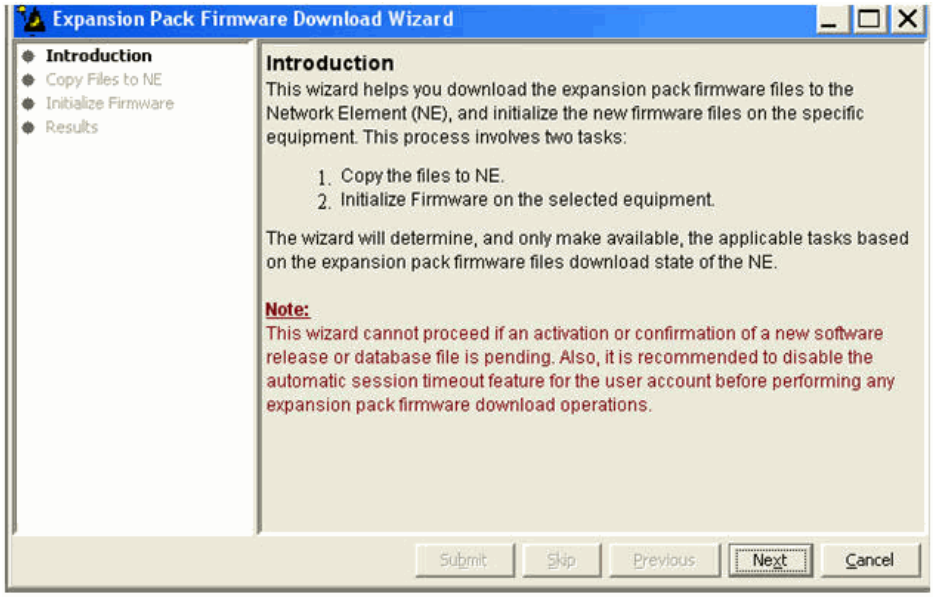


Figure 240: Example Expansion Pack Firmware Download Wizard Introduction Screen

Step 2
Click *Next*.

The *Copy Files to NE* screen opens.

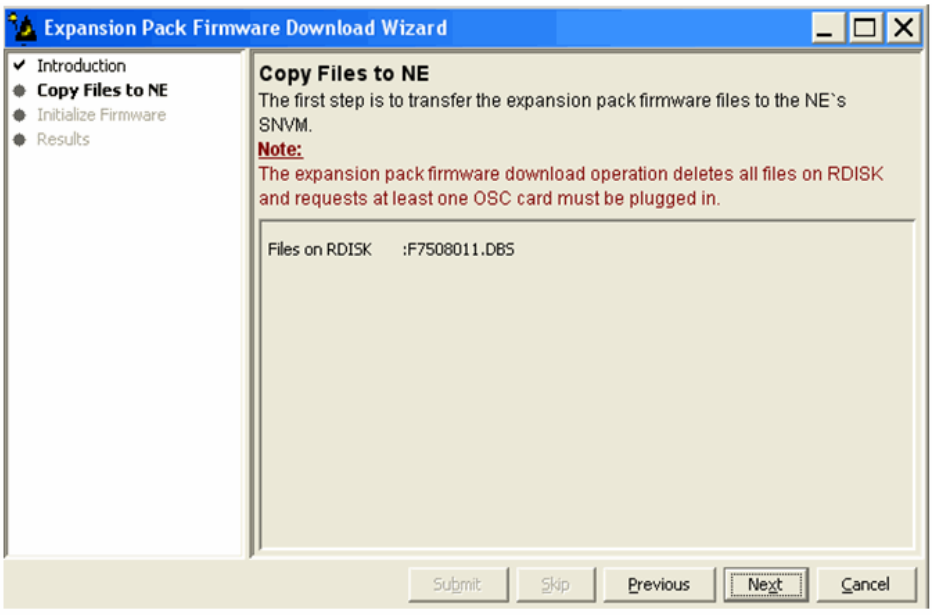


Figure 241: Example Expansion Pack Firmware Download Wizard Copy Files to NE Screen

Step 3
Click *Next*.

The *Copy Files to RDISK and SNVM* screen opens.

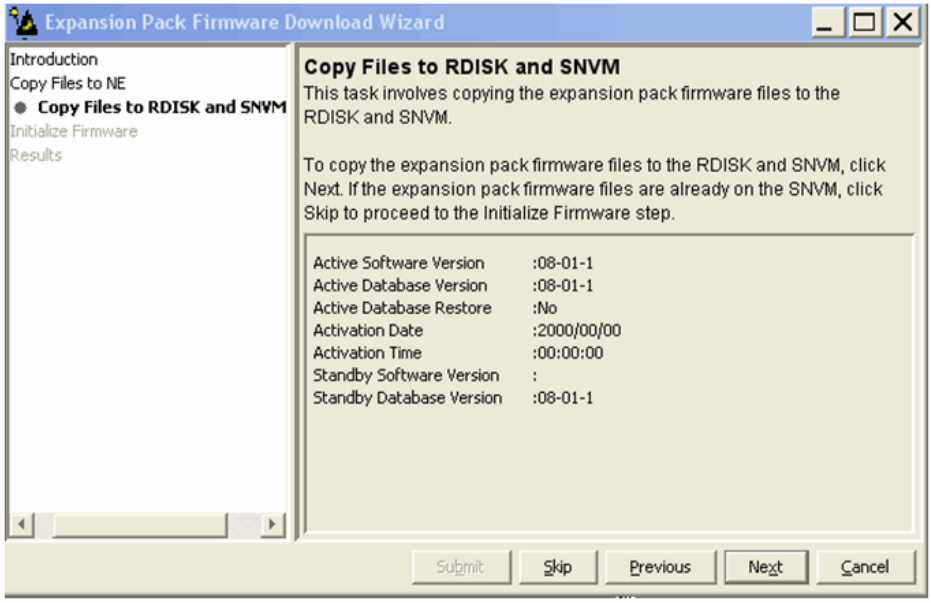


Figure 242: Example Expansion Pack Firmware Download Wizard Copy Files to RDISK and SNVM Screen

Step 4
Click *Next*.

The *Select Host* screen opens.

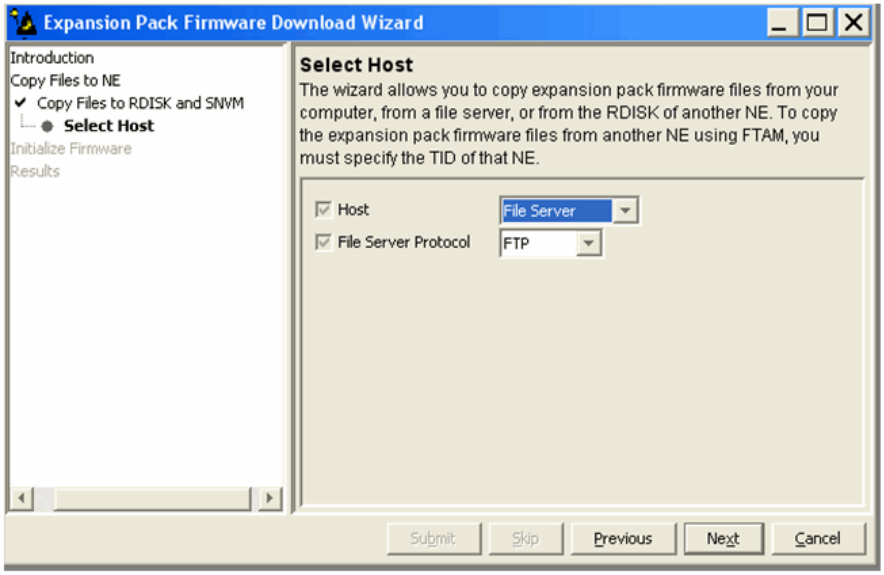


Figure 243: Example Expansion Pack Firmware Download Wizard Select Host Screen

Step 5

Read the instructions on the *Select Host* screen, and then select *File Server* or *Another NE* from the *Host* drop-down list.

Note: *If Another NE is selected, the TID of the other NE must be known.*

One of the following screens is shown.

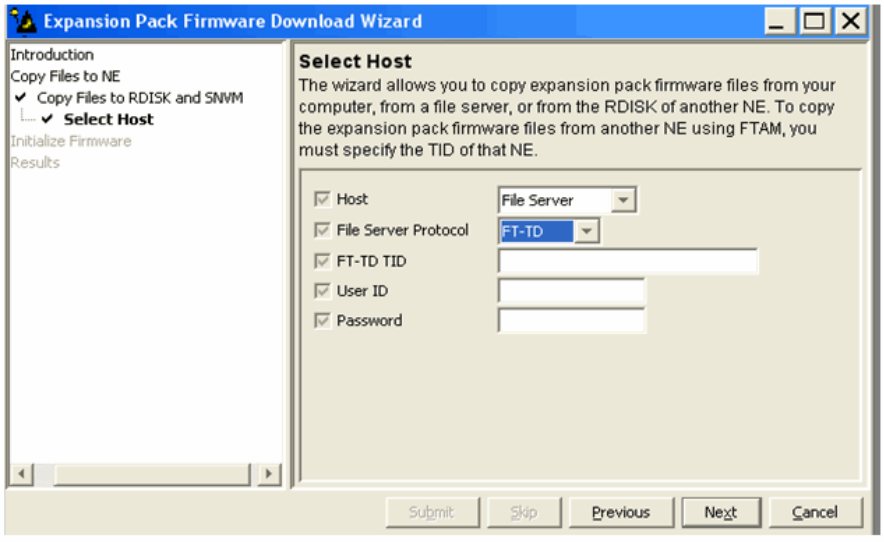


Figure 244: Example Select Host Screen with File Server Selected

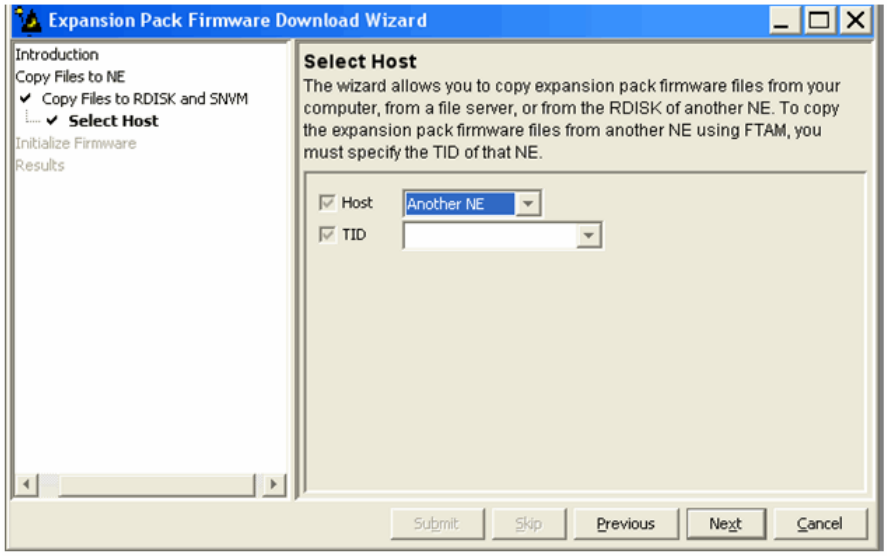


Figure 245: Example Select Host Screen with Another NE Selected

Step 6

Enter the applicable information on the *Select Host* screen selected, and then click *Next*.

The *Select FTP Server* screen opens.

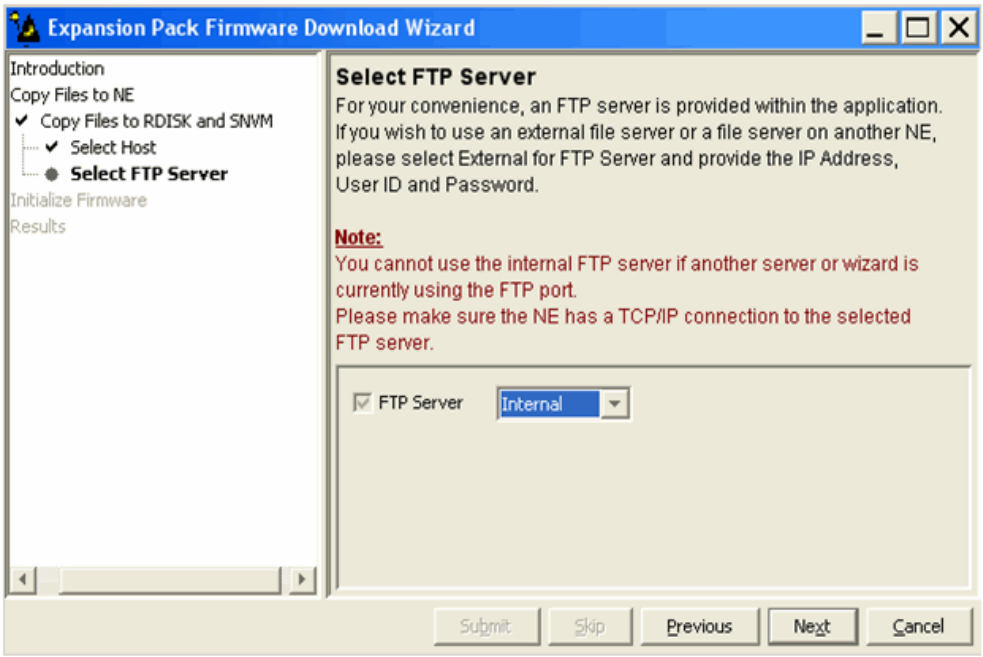


Figure 246: Example Expansion Pack Firmware Download Wizard Select FTP Server Screen

Step 7
Are the software files located on an internal FTP server or an external FTP server?

If YES:
If internal FTP server: Continue with the next step.

If NO:
If external FTP server: Skip the next step.

Step 8
From the *FTP Server* drop-down list, select *Internal*, and skip the next step.

Step 9
From the *FTP Server* drop-down list, select *External*.

The *Select FTP Server* screen displays additional fields.

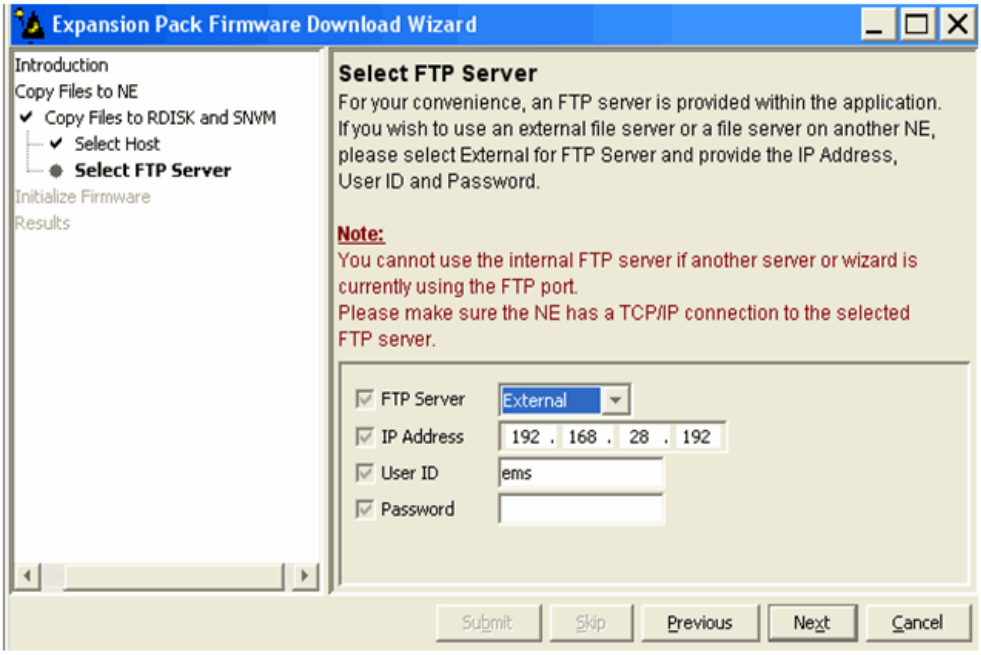


Figure 247: Example Expansion Pack Firmware Download Wizard Select FTP Server Screen–External FTP Server

a) Enter the *IP Address* of the external FTP server.

b) Enter a valid *User ID* for accessing the FTP server.

c) Enter a valid *Password* for accessing the FTP server.

Step 10
Click *Next*.

The *Select Files* screen opens.

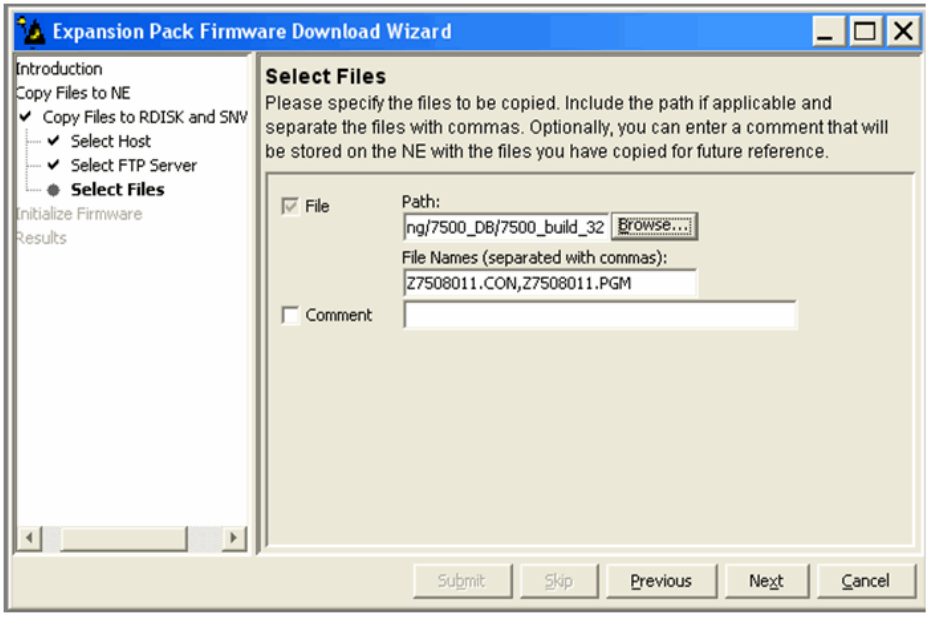


Figure 248: Example Expansion Pack Firmware Download Wizard Select Files Screen

Step 11
In the *File: Path* text box, enter the location of the software file, or click *Browse* to search for the file.

When browsing, at least one file must be selected from the Browse dialog box to update the path. Multiple files can be selected by using the CTRL key.

Note: *If files have been located previously through the Software Download wizard from the same PC, the text box defaults to that location.*

Step 12
In the *File: File Names (separated with commas)* text box, enter the required file names:

Example:

- *Z7509011.CON*
- *Z7509011.PGM*

- *Y7509011.PGM*
- *Z7509011.SIG*

Note: *The Y750xxxx.PGM file is only applicable if upgrading to Release 9.1.*

Step 13
In the *Comment* text box, enter comments, if required.

Note: *Fujitsu recommends the user's name or initials and the date of upgrade.*

Step 14
Click *Next*.

Note: *The software download may take up to 15 minutes. The Select Files screen grays while the system downloads the file.*

The *Enter Signatures* screen opens.

Note: *If an external FTP server was selected or the files are being copied from another NE, the signature fields will be populated with zeros (00000000) by default. In this case, the user can either manually enter the signatures or leave the zeros to bypass the checksum.*

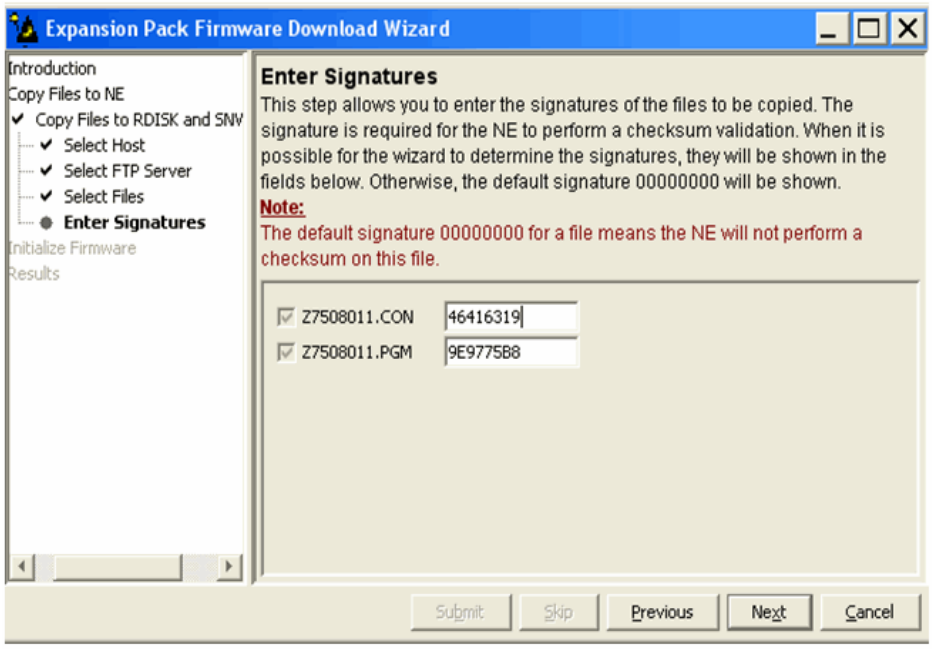


Figure 249: Example Expansion Pack Firmware Download Wizard Enter Signatures Screen

Step 15
Click *Next*.

The *Copy to RDISK and SNVM* screen opens.

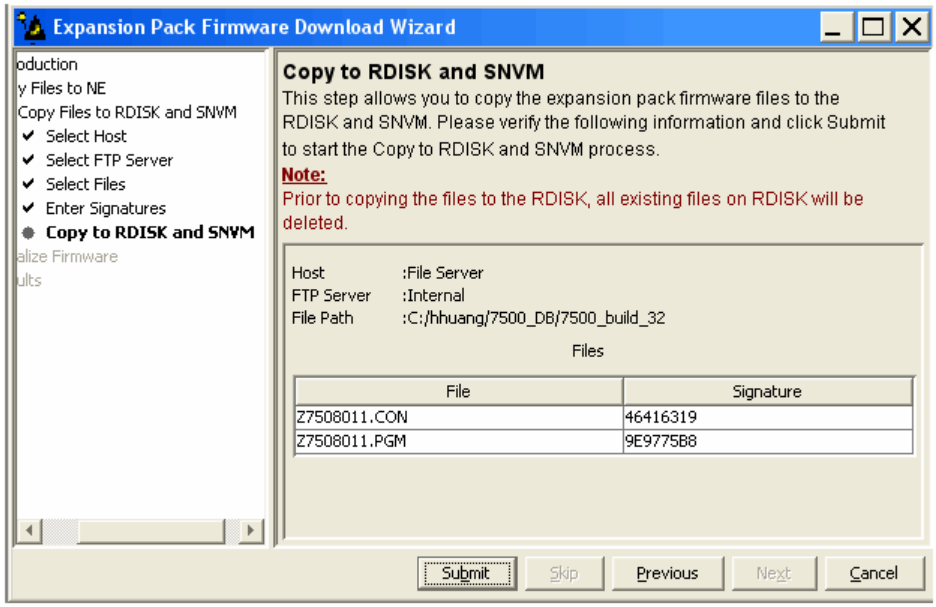


Figure 250: Example Expansion Pack Firmware Download Wizard Copy to RDISK and SNVM Screen

Step 16
Click *Submit*.

A Performing Copy File dialog box opens, displaying the progress of the copying for each file.

Note: *The files may take up to 15 minutes to copy. During the operation, the NOT READY LED on the NEM is yellow.*

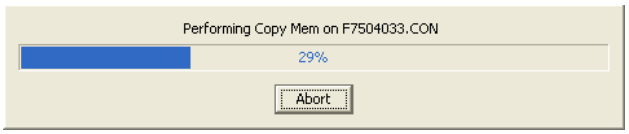


Figure 251: Example of a Typical Performing Copy File Window

A successful completion message box momentarily appears, and then the *Copy to RDISK and SNVM Results* screen opens.

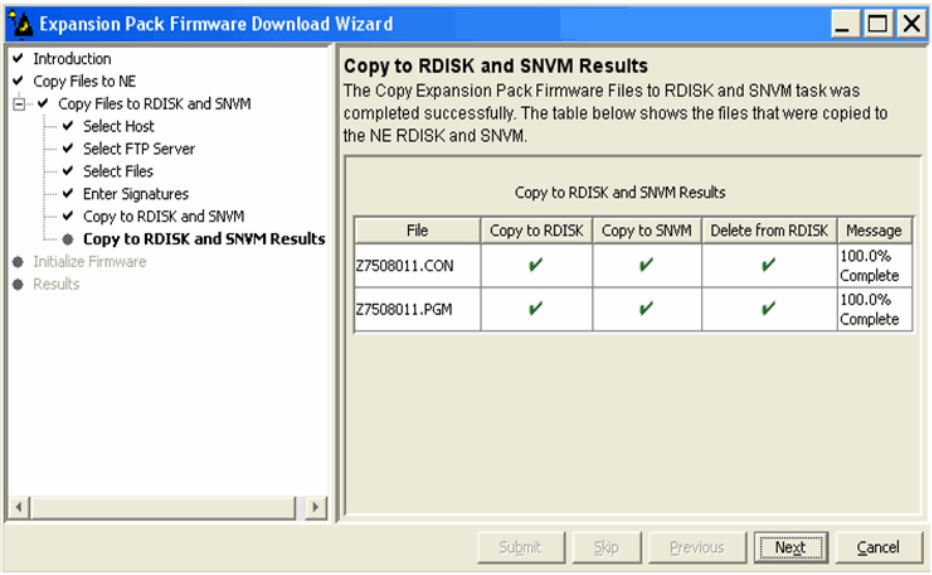


Figure 252: Example Expansion Pack Firmware Download Wizard Copy to RDISK and SNVM Results Screen

Step 17
Proceed to Initialize Expansion Pack Firmware Files.

Continue with next task ►

3.6.3 Initialize Expansion Pack Firmware Files

Step 1
Click *Next*.

The *Initialize Firmware* screen opens.

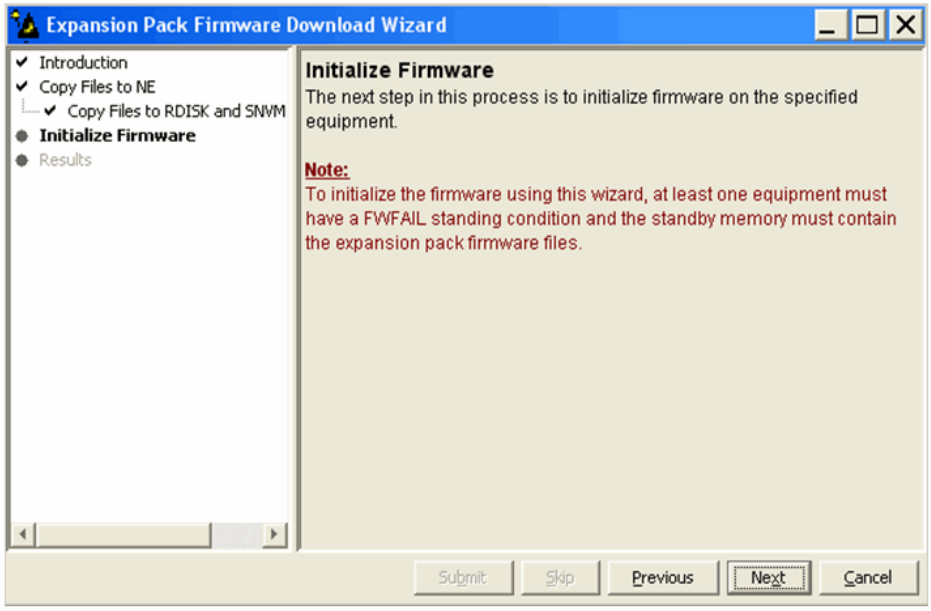


Figure 253: Example Expansion Pack Firmware Download Wizard Initialize Firmware Screen

Step 2
Click *Next*.

The *Initialize Firmware Parameters* screen opens.

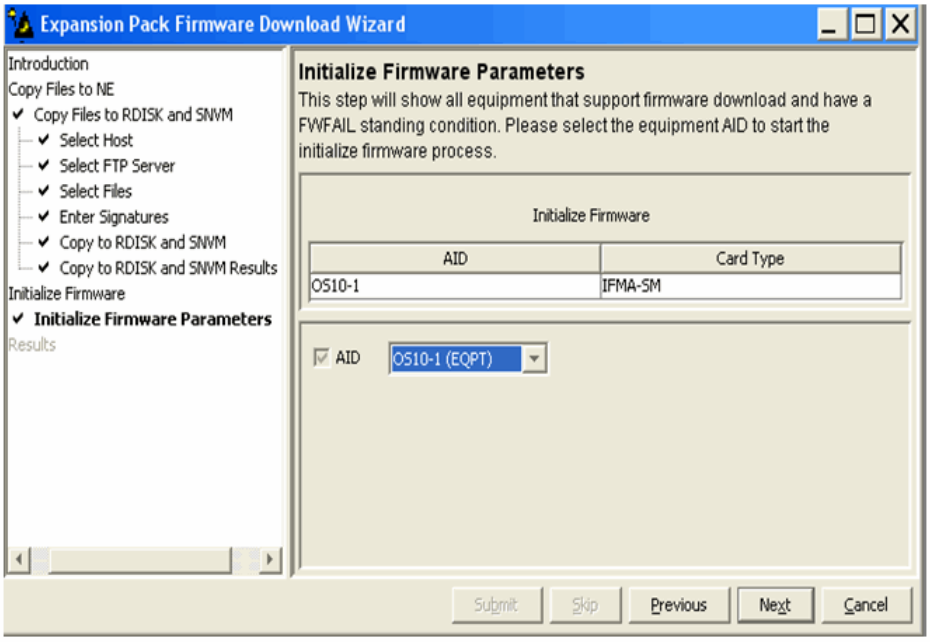


Figure 254: Example Expansion Pack Firmware Download Wizard Initialize Firmware Parameters Screen

Step 3
Click *Next*.

The *Initialize Firmware Confirmation* screen opens.

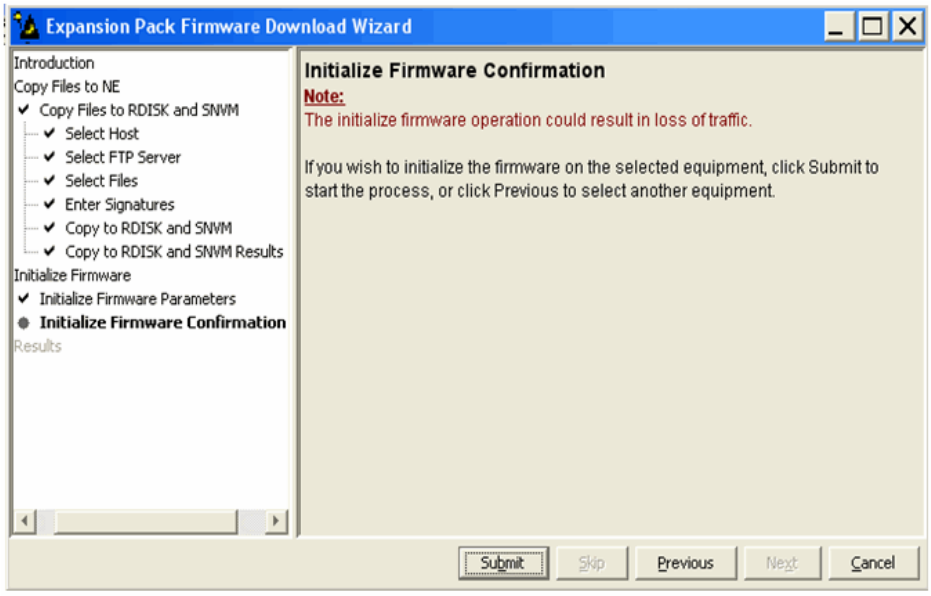


Figure 255: Example Expansion Pack Firmware Download Wizard Initialize Firmware Confirmation Screen

Step 4
Click *Submit*.

The *Initialize Firmware Result* screen opens.

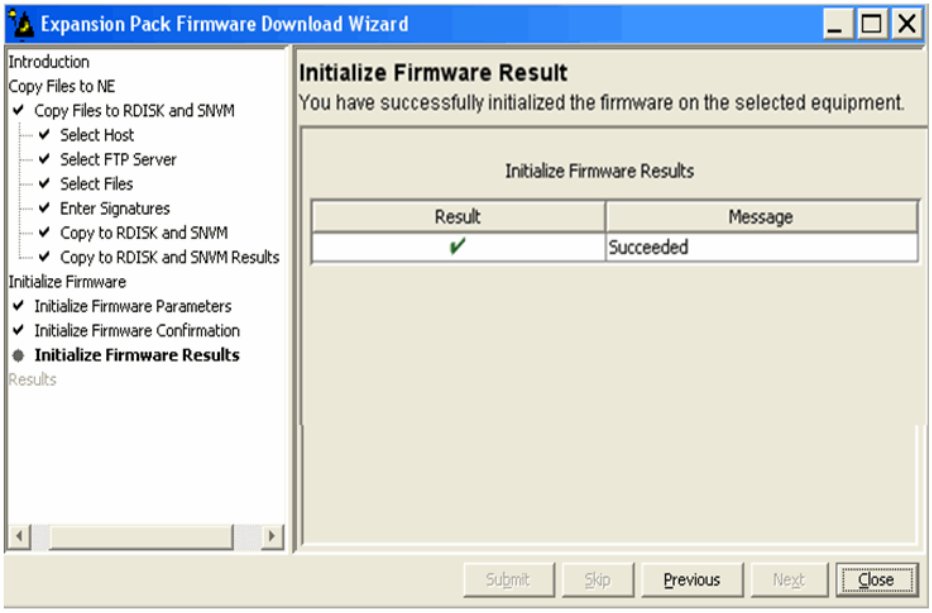


Figure 256: Example Expansion Pack Firmware Download Wizard Initialize Firmware Result Screen

Step 5
Click *Next*.

The *Results* screen opens.

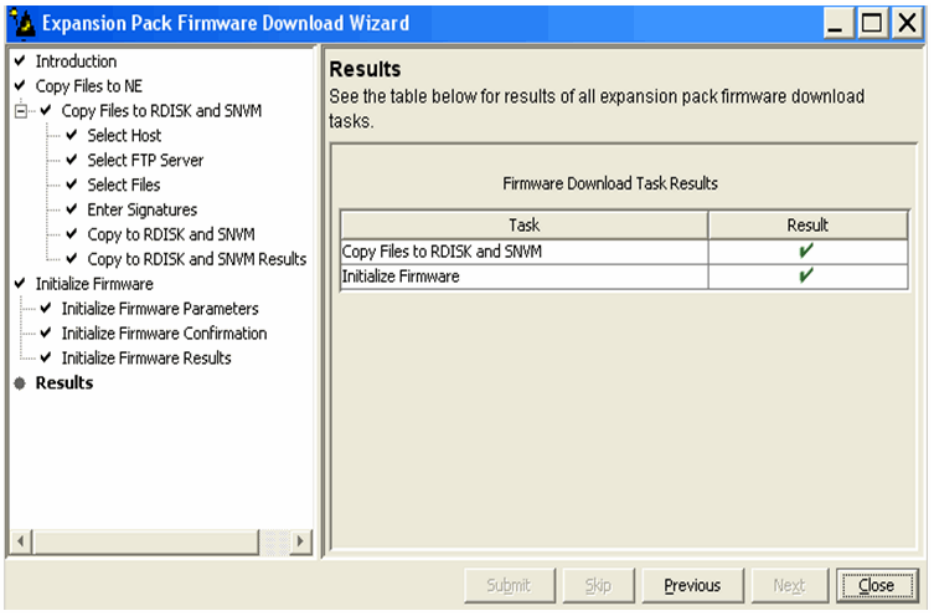


Figure 257: Example Expansion Pack Firmware Download Wizard Results Screen

Step 6
Click *Close*.

The Expansion Pack Firmware Download wizard closes. You may continue working in the NETSMART 500 environment and stay logged on the NE.

3.7
Upgrading Firmware on Equipment

After the system software is upgraded, a firmware version mismatch (FVM) alarm may be generated against individual plug-in units with firmware versions that are not compatible with the new system software. The firmware version on plug-in units is not automatically updated during a system software upgrade operation.

If a plug-in unit reports an FVM alarm after a system software upgrade, the firmware on the plug-in unit is incompatible with the new system software and must be upgraded.

Caution: *Upgrading the firmware on a firmware upgradeable unit may impact traffic currently carried on that unit. Users should manually upgrade the firmware on the unit at an appropriate time by following local practices.*

The following table lists the firmware downloadable plug-in units.

Attention: *This table shows the most recent issue of the plug-in units shipped from the factory at the time of the current release. The issue number (for example, -I03) indicates the firmware version of the plug-in unit as it left the factory. If a plug-in unit has an earlier issue number, it can still be used in the current-release system, but it may need a firmware upgrade to support current-release features fully.*

Table 45: Firmware Downloadable Units

Unit Name	Part Number	Minimum Release 9.1 Software/ FirmwareVersion	Minimum Compatible Firmware Version for Release 9.1 ILA Configuration	Minimum Compatible Firmware Version for Release 9.1 Non-ILA Configuration
APMA-ASC1	FC9682ASC1	01-01-3	n/a	01-01-1
APMA-DRC1	FC9682DRC1	01-01-D	n/a	01-01-1
APMA-MHU1	FC9682MHU1	01-01-2	n/a	01-01-1
APMA-MHU2	FC9682MHU2	01-01-2	01-01-1	n/a
APMA-L2C1	FC9682L2C1-I07	04-01-1	02-01-1	01-01-1
APMA-M2C1	FC9682M2C1-I04	04-01-1	02-01-1	01-01-1
APMA-M2U1	FC9682M2U1	05-01-1	01-01-1	01-01-1
APMA-ULC1	FC9682ULC1	04-01-1	02-01-1	01-01-1
APMA-ULU1	FC9682ULU1	06-01-1	01-01-1	01-01-1

Table 45: Firmware Downloadable Units (Cont.)

Unit Name	Part Number	Minimum Release 9.1 Software/ FirmwareVersion	Minimum Compatible Firmware Version for Release 9.1 ILA Configuration	Minimum Compatible Firmware Version for Release 9.1 Non-ILA Configuration
IFMA-8TC1	FC96828TC1-I02	05-01-1	n/a	01-01-1
IFMA-8TC2	FC96828TC2	04-01-1	n/a	01-01-1
IFMA-BXC1	FC9692BXC1	05-01-4	n/a	01-01-1
IFMA-SMC1	FC9692SMC1	02-01-5	n/a	01-01-1
IFMA-GUC1	FC9682GUC1-I07	02-01-2	n/a	01-01-1
IFMA-LGB1	FC9682LGB1	01-01-1	n/a	01-01-1
IFMA-QMC1	FC9682QMC1	03-01-2	n/a	01-01-1
IFMA-QMC2	FC9682QMC2	01-03-1	n/a	01-01-1
IFMA-QRC1	FC9682QRC1	01-03-2	n/a	01-01-1
IFMA-QRC2	FC9682QRC2	01-02-2	n/a	01-01-1
IFMA-QUC1	FC9682QUC1	03-01-4	n/a	01-01-1
IFMA-QUC2	FC9682QUC2	02-01-1	n/a	01-01-1
IFMA-RGC1	FC9682RGC1	03-01-1	n/a	01-01-1
IFMA-RGC3	FC9682RGC3	03-01-1	n/a	01-01-1
IFMA-U1C1	FC9682U1C1	06-01-1	n/a	01-01-1
IFMA-U1C2	FC9682U1C2	04-01-1	n/a	01-01-1
IFMA-U2C1	FC9682U2C1	06-01-1	n/a	01-01-1
IFMA-U2C2	FC9682U2C2	04-01-1	n/a	01-01-1
IFMA-U3C1	FC9682U3C1	06-01-1	n/a	01-01-1
IFMA-U3C2	FC9682U3C2	04-01-1	n/a	01-01-1
IFMA-U4C1	FC9682U4C1	06-01-1	n/a	01-01-1
IFMA-U5C2	FC9682U5C2	02-01-3	n/a	01-01-1
MCMA-RCS1	FC9682RCS1	03-01-4	n/a	01-01-1
MDMA-RMC1	FC9682RMC1-I02	01-01-1	n/a	01-01-1

Table 45: Firmware Downloadable Units (Cont.)

Unit Name	Part Number	Minimum Release 9.1 Software/ FirmwareVersion	Minimum Compatible Firmware Version for Release 9.1 ILA Configuration	Minimum Compatible Firmware Version for Release 9.1 Non-ILA Configuration
MDXP-MDC3	FC9503MDC3	01-01-1	n/a	01-01-1
SCMA-SCC4	FC9682SCC4-I02	06-03-1	03-01-1	01-01-1
SFMA-CDC1	FC9682CDC1-I02	01-01-1	n/a	01-01-1
SFMA-CMC1	FC9682CMC1-I03	02-01-3	n/a	01-01-1
SFMA-RDC1	FC9682RDC1	01-02-1	n/a	01-01-1
TCMA-ST31	FC9682ST31-I03	01-01-2	n/a	01-01-1

Caution: *On rare occasions, either at system turn-up or during OSC plug-in unit replacement, the system software may stick in a SYNC state. As a result, CPY-MEM, INIT-EQPT, and INIT-SYS commands may fail, returning the SARB or SROF error code. To clear the problem, reseat the OSC unit. After the LEDs change from amber to green, execute an INIT-SYS command with LEVEL=WARM. If the command fails again, reseat the other OSC plug-in unit.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters.* ***HINT****: Specific information is available by clicking the hyperlinked TL1 command name (for example, ENT-EQPT) in the TL1 column.*

Step 1
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	
	Comm. Port: COMx (for example, COM2)
	
	Configure: use default[37]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 2
Retrieve alarms and conditions on the NE.

[37] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Are any FVM alarms present?

If YES:
Continue with the next step.

Note: *If any alarms other than FVM, FWFAIL, or FLT are present, clear the alarms before continuing. Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
This procedure is complete.

Step 4
Initialize the alarmed plug-in unit to download and activate program files to the firmware.

TL1	NETSMART 500

`INIT-EQPT:TID:AID:CTAG:::FORCE=Y, OVERWRITE=Y;`
AID:
• Refer to Access Identifiers, for all equipment AIDs.
 	
Example:
`INIT-EQPT:FUJITSU:OS1-1&OS1-19: CTAG:::FORCE=Y,OVERWRITE=Y;`
	Click the Equipment tab in the tree view.
	
	Select the plug-in unit, expanding the tree as necessary.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Operations Dialog*
	
	Select the Initialize tab.
	Select the Firmware tab.
	
	Verify that *Yes* is selected for *FORCE*.
	Select *Yes* for *OVERWRITE*.
	Click Initialize.
	
	A confirmation dialog box opens.
	Click Yes.
	Close the dialog box.

Note: *The firmware can take several minutes to upgrade. The transient condition FWACT will be reported during the upgrade.*

Step 5
Verify the firmware is upgraded on the specified plug-in unit.

TL1	NETSMART 500

`RTRV-FWINFO:TID:AID:CTAG;`
AID:
• As used in previous step.
Example:
`RTRV-FWINFO:FUJITSU:OS1-1&OS1-19:CTAG;`
	NE ▸ *TL1 Command Builder*
	TL1 Command Builder dialog box opens.
	Select the RTRV-FWINFO command from the *Command Name* drop-down list.
	Enter the AID of the unit in the *AID* field.
	Click *Send*.
	Close the TL1 Command Builder dialog box.

Step 6
Retrieve alarms and conditions on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 7
Are any active alarms or conditions being reported on the NE?

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 8.

If NO:
Log off the NE, this procedure is complete.

Step 8
Log off the NE.

This procedure is complete.

4
Upgrading to the Enhanced NEM

In this chapter:

This chapter provides upgrade procedures for upgrading the FLASHWAVE® 7500 system to the Enhanced NE Management (NEM) Processor plug-in unit (MPMA-SHP4). The upgrade procedures include:

- Upgrading the FLASHWAVE® 7500 system to Release 6.1 or later software
- Replacing the MPMA-SHP3 plug-in unit with the MPMA-SHP4 plug-in unit

4.1 Verifying the System Software

Before upgrading to the Enhanced NEM Processor plug-in unit (MPMA-SHP4), the current system software version must be Release 6.1 or later.

Additionally, if the current software is Release 4.1, the system must first be upgraded following the procedures given in Upgrading System Software from Release 4.1 before upgrading to Release 6.1 or later. Releases 4.2 and later must be upgraded to Release 6.1 or later following the procedures given in Upgrading System Software from Release 4.2 or Later.

Follow these steps to verify the current software release and upgrade to Release 6.1 or later, if necessary:

Step 1
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART® 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start > All Programs > Fujitsu > NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select *NE > Logon*. ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

<table>
<tr><th>TL1</th><th>NETSMART® 500</th></tr>
<tr><td>ACT-USER:TID:UID:CTAG::PID;
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;</td><td>For TERM1 (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial
Comm. Port: COMx (for example, COM2)
Configure: use default[38]

For TERM2 (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.
The NETSMART 500 NE View opens.
The Security Message dialog box opens.
Click OK.
Note: Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.</td></tr>
</table>

After a successful logon:

- **TL1 user interface**–The FLASHWAVE 7500 system responds with the normal, completed (COMPLD) message.
- **NETSMART 500 user interface**–The NETSMART 500 NE View provides a graphical user interface for provisioning and monitoring the FLASHWAVE 7500 system.

Step 2
Are any active alarms or conditions being reported on the NE?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to the next step.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to the next step.

[38] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Retrieve and verify software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID:AID:CTAG;`
AID:
• ACT, STBY, **ALL**
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	NE ▸ *Systems Operations*
	Click the Attributes tab.

Step 4
Is the current software version Release 6.1 or later?

If YES:
Go to Upgrading the Processor Unit.

If NO:
Based on the current software release, follow the procedures in Upgrading System Software from Release 4.1 and/or Upgrading System Software from Release 4.2 or Later to upgrade to Release 6.1 or later. Then proceed to Upgrading the Processor Unit.

4.2 Upgrading the Processor Unit

This procedure lists the general steps required for upgrading the MPMA-SHP3 NE Management (NEM) shelf processor plug-in unit to the Enhanced NEM shelf processor unit (MPMA-SHP4). This procedure assumes that you have already completed the procedure in Verifying the System Software .

Caution: *If an MPMA-SHP3 or SCMA-SCC4 plug-in unit needs to be removed, ensure that all proper prerequisites for plug-in unit removal, including safety precautions, have been completed and that the NOT READY LED on the plug-in unit is off (not lit) before removing the plug-in unit.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Step 1
Log on the NE.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to Setting Up Craft Interface (TL1 Session through TERM1) through Setting Up Craft Interface (NETSMART 500 Session through TERM2).*

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

<table>
<tr><th>TL1</th><th colspan="2">NETSMART 500</th></tr>
<tr><td rowspan="2">ACT-USER:TID:UID:CTAG::PID;
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;</td><td>For TERM1 (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial
Comm. Port: COMx (for example, COM2)
Configure: use default[39]</td><td>For TERM2 (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024</td></tr>
<tr><td colspan="2">Click Logon.
The NETSMART 500 NE View opens.
The Security Message dialog box opens.
Click OK.
Note: Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.</td></tr>
</table>

After a successful logon:

- **TL1 user interface**—The FLASHWAVE 7500 system responds with the normal, completed (COMPLD) message.
- **NETSMART 500 user interface**—The NETSMART 500 NE View provides a graphical user interface for provisioning and monitoring the FLASHWAVE 7500 system.

Step 2

Retrieve all active alarms and conditions currently being reported on the NE.

[39] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 3
Are any active alarms or conditions currently being reported on the NE?

If YES:
Clear all active alarms and conditions before continuing this procedure. Refer to Responding to Alarms and Conditions, if necessary. After alarms are cleared, proceed to the next step.

If NO:
Go to the next step.

Step 4
Inspect the Enhanced NEM Processor plug-in unit (MPMA-SHP4) to be installed for possible physical damage or debris.

Step 5
Does the MPMA-SHP4 plug-in unit appear to be free from defects?

If YES:
Go to the next step.

If NO:
Set the plug-in unit aside for repair paperwork processing (refer to Repairing and Returning Defective Equipment), obtain another MPMA-SHP4 plug-in unit, and then go to the previous step.

Step 6
Record the serial number and issue number of the MPMA-SHP4 plug-in unit.

Step 7
Locate the plug-in unit to be replaced. See the following figure.

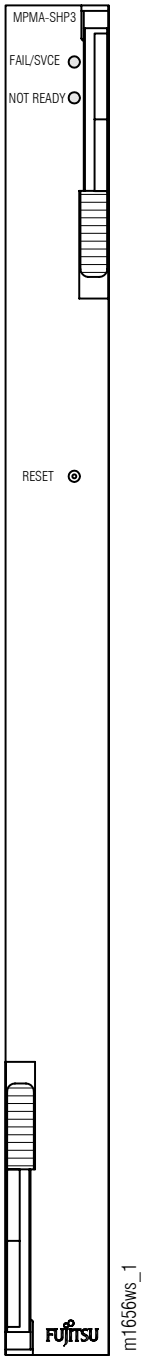


Figure 258: MPMA-SHP3 NE Management Shelf Processor Plug-In Unit Front Panel

Step 8
Remove the plug-in unit being replaced.

Step 9
Install the replacement MPMA-SHP4 plug-in unit into the working shelf slot (MPMA-1). Refer to the following table and the previous figure for proper LED responses during MPMA-SHP4 plug-in unit replacement.

Note: *The NOT READY LED on the MPMA-SHP4 shelf processor plug-in unit lights yellow two times, indicating that the software download (SWDL) is in progress. Refer to the following table for proper LED responses. A software download may require approximately 30 minutes to complete.*

Table 46: NE Management Shelf Processor (MPMA-SHP4) LED Responses

Stage	MPMA-SHPx LED	Response
Immediately after plug-in unit is installed	NOT READY	Lit yellow
After completion of software download (SWDL)	NOT READY	Not lit
	FAIL/SVCE[40]	Lit green

Step 10
Wait up to 30 minutes to allow the FAIL/SVCE LED to light.

Step 11
Is the FAIL/SVCE LED on the MPMA-SHP4 shelf processor plug-in unit lit red?

If YES:
The MPMA-SHP4 plug-in unit may be defective. Continue with the next step.

If NO:
Go to Step 14.

Step 12
Remove the plug-in unit, and set the plug-in unit aside for repair paperwork processing. (Refer to Repairing and Returning Defective Equipment, for additional information.)

Step 13
Obtain another spare MPMA-SHP4 plug-in unit, return to Step 4 to repeat this procedure on that spare plug-in unit, and then continue with the next step.

[40] A flashing red FAIL/SVCE LED indicates a plug-in unit mismount or mismatch. Refer to Correcting a Mismounted Plug-In Unit or SFP/XFP Module.

Step 14
Is the FAIL/SVCE LED on the MPMA-SHP4 shelf processor plug-in unit lit green?

If YES:
Go to Step 18.

Note: *After the initialization of a tributary shelf MPMA-SHP4 shelf processor unit completes (FAIL/SVCE LED turns green) and the CTNEQPTSHELF alarm clears a T-LBCN (Laser Bias Current Normalized), TCA may immediately be reported against one or more of the tributary IFMA units. This behavior is normal and not traffic affecting. This TCA is not persistent and will not be reported again unless a valid LBCN condition exists.*

If NO:
Go to the next step.

Step 15
Using a small, sharp-tipped object such as a ballpoint pen, press the RESET button (CPU reset) on the plug-in unit.

Note: *The NOT READY LEDs on the MPMA-SHP4 and SCMA-SCC4 plug-in units light yellow two times, indicating that the software download is in progress.*

Step 16
Wait up to 30 minutes to allow the FAIL/SVCE LED to light.

Step 17
Is the FAIL/SVCE LED on the MPMA-SHP4 plug-in unit lit green?

If YES:
Go to the next step.

If NO:
Call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.

Step 18
Retrieve all active alarms and conditions currently being reported on the NE.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 19
Are any active alarms or conditions currently being reported on the NE?

If YES:
Clear all active alarms and conditions that are not related to the plug-in unit being replaced before continuing this procedure. Refer to Responding to Alarms and Conditions, if necessary. After alarms are cleared, proceed to the next step.

If NO:
Go to the next step.

Step 20
Set the date and time for the NE.

Note: *This step is required because the clock on the new CPU will likely not contain accurate date and time values.*

TL1	NETSMART 500

`SET-DAT:TID::CTAG::DATE,TIME;`
DATE:
• yymmdd
• null (leaves system date unchanged)
TIME:
• hhmmss
• null (leaves system time unchanged)
Example:
`SET-DAT:FUJITSU::CTAG::000424,1015;`
	NE ▸ *System Operations*
	Click the Time tab.
	In the Command Parameters area:
	• Enter date (yyyy/mm/dd) in the Date field.
	• Enter time (hh:mm:ss) in the Time field.
	Click Modify.
	Close the Operations dialog box.

Step 21
Log off the NE.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to confirm.

Step 22
Is the craft interface cable to be removed at this time?

If YES:
Continue with the next step.

If NO:
This procedure is complete.

Step 23
Carefully disconnect the craft interface cable connector from the TERM1 or TERM2 connector on the front of the shelf.

Warning: *Do not pull out the connector by pulling on the interface cable. Pulling on the cable may damage the connector or cable.*

The TERM1 and TERM2 connectors on the front of the shelf are used as follows:

- TERM1– D-sub, 9-pin connector (serial communication interface)
- TERM2– RJ-45 connector (LAN or TCP/IP communication interface)

Step 24
Carefully remove the craft interface cable connector from the TERM1 or TERM2 connector on the front of the shelf by grasping the connector shell and slowly removing it from the connector.

Step 25
If desired, shut down the terminal or PC.

Step 26
If desired, carefully disconnect and remove the interface cable from the terminal or PC port.

This procedure is complete.

5
Adding or Deleting a Node in a Network

In this chapter:

The procedure in Add/Delete Node can be used to either add or delete a node in a FLASHWAVE® 7500 ring network. The procedure is applicable to Core, Small, or ETSI Configuration networks.

5.1
About Adding a Node

The procedure in Add/Delete Node is written for the case shown in the following figure) in which a new node, Node B, is inserted between existing nodes, Node A and Node C, in a 3-node ring network.

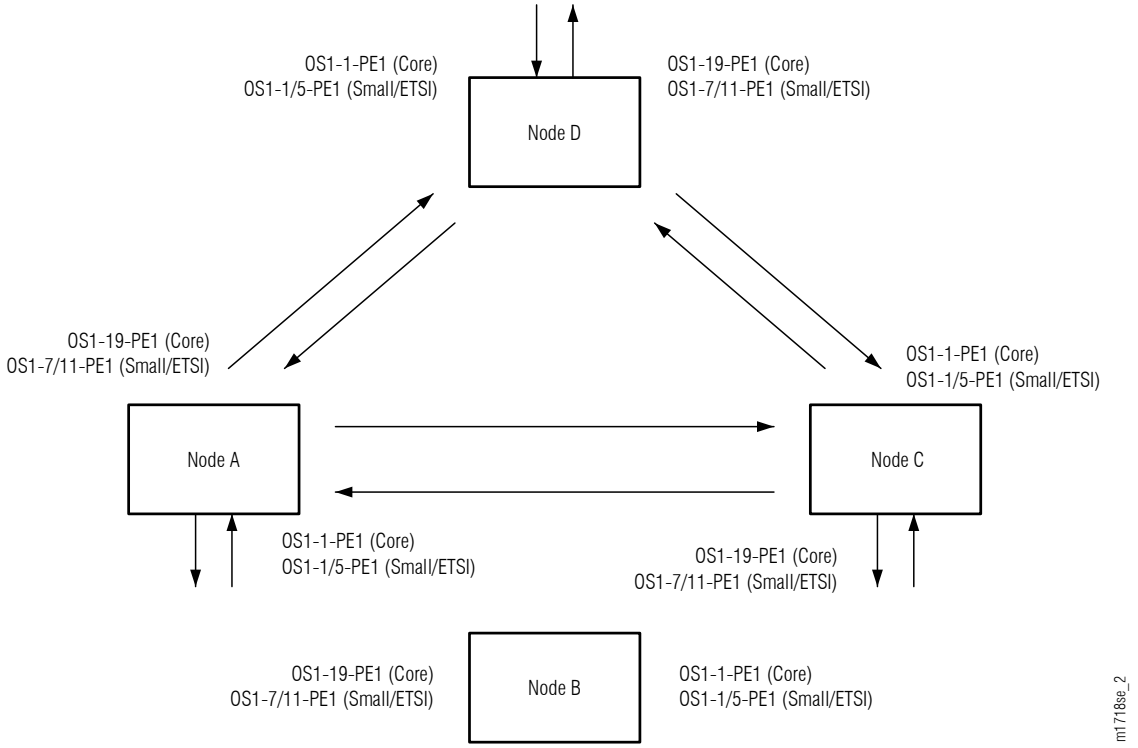


Figure 259: Ring Network Configuration before Node B Is Added

The following figure shows the ring network after Node B has been added.

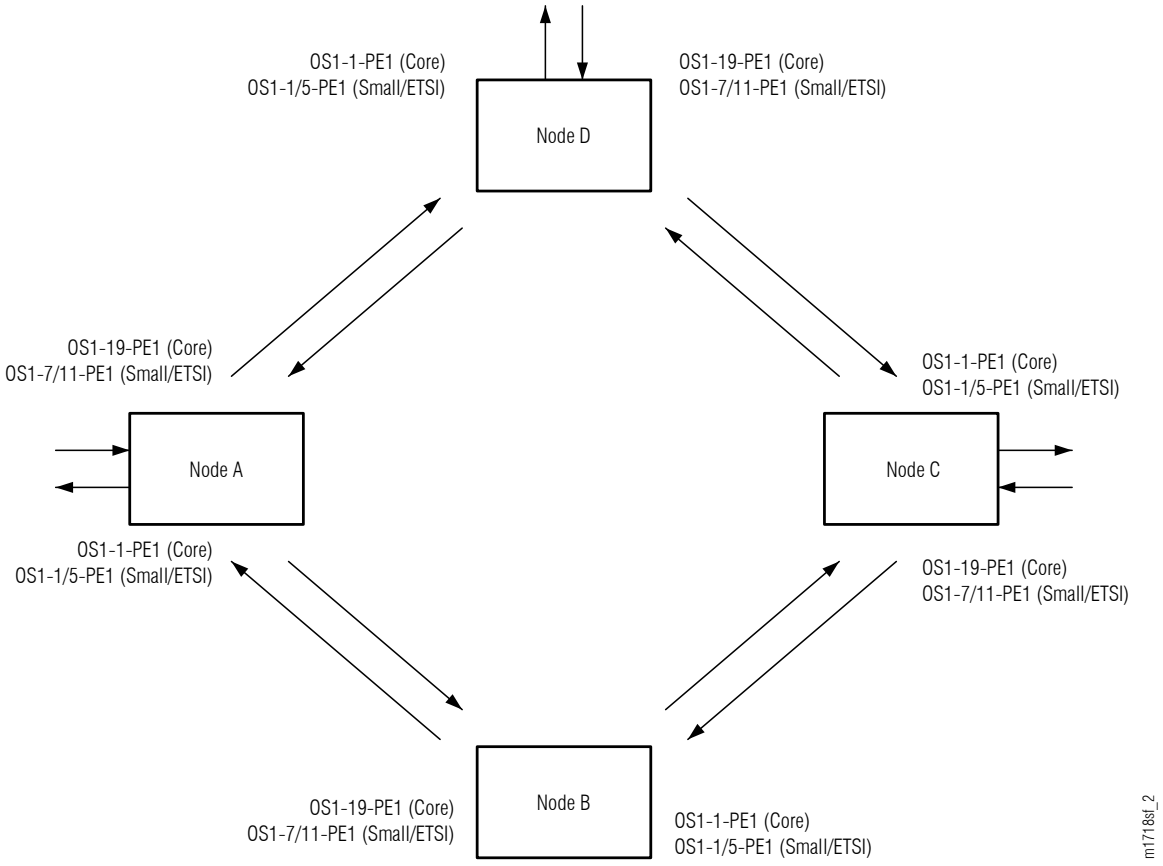


Figure 260: Ring Network Configuration after Node B Is Added

The procedure can also be used for ring networks with more than three nodes. In multiple-node ring networks, all nodes that are not adjacent to the insertion span should be treated as Node D is treated.

5.2
About Deleting a Node

The procedure in Add/Delete Node is written for a 4-node ring network, as shown in the following figure, in which Node B, located between Nodes A and C, is to be removed.

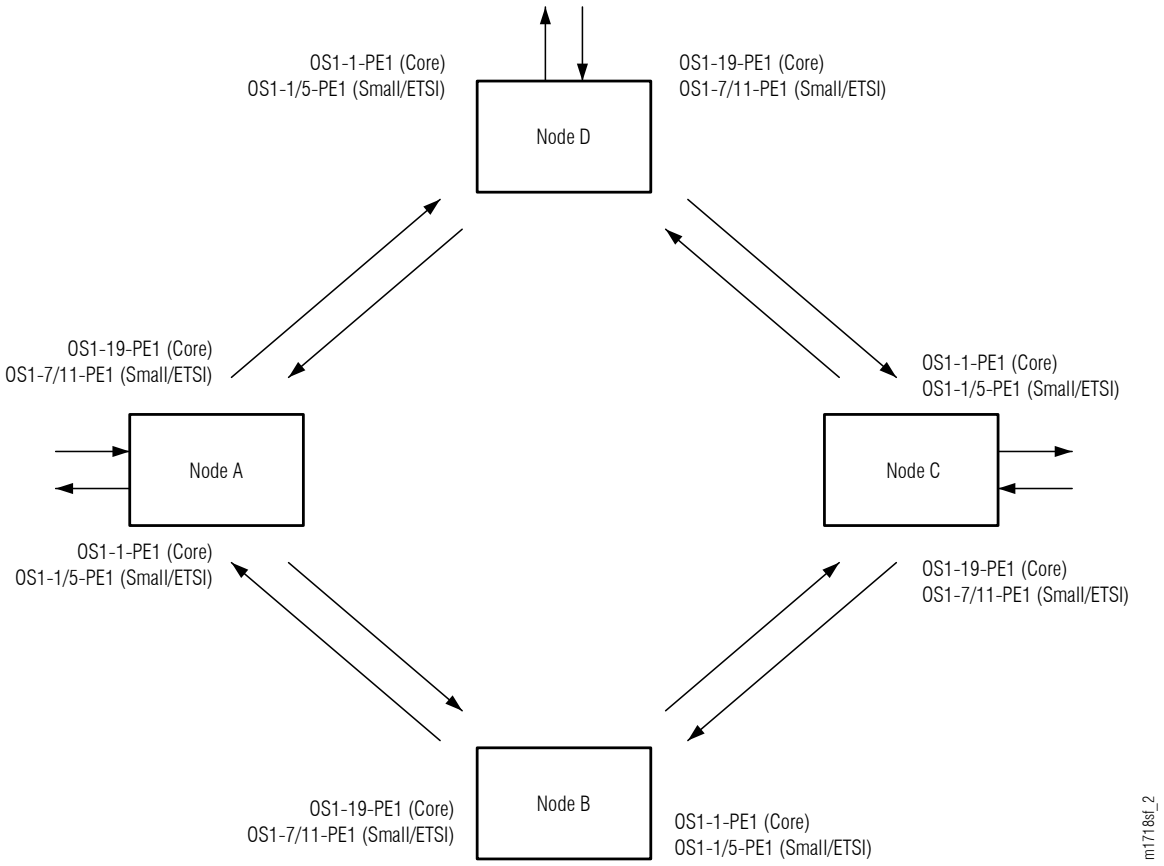


Figure 261: Ring Network Before Node B Is Removed

The following figure shows the ring network after Node B is removed.

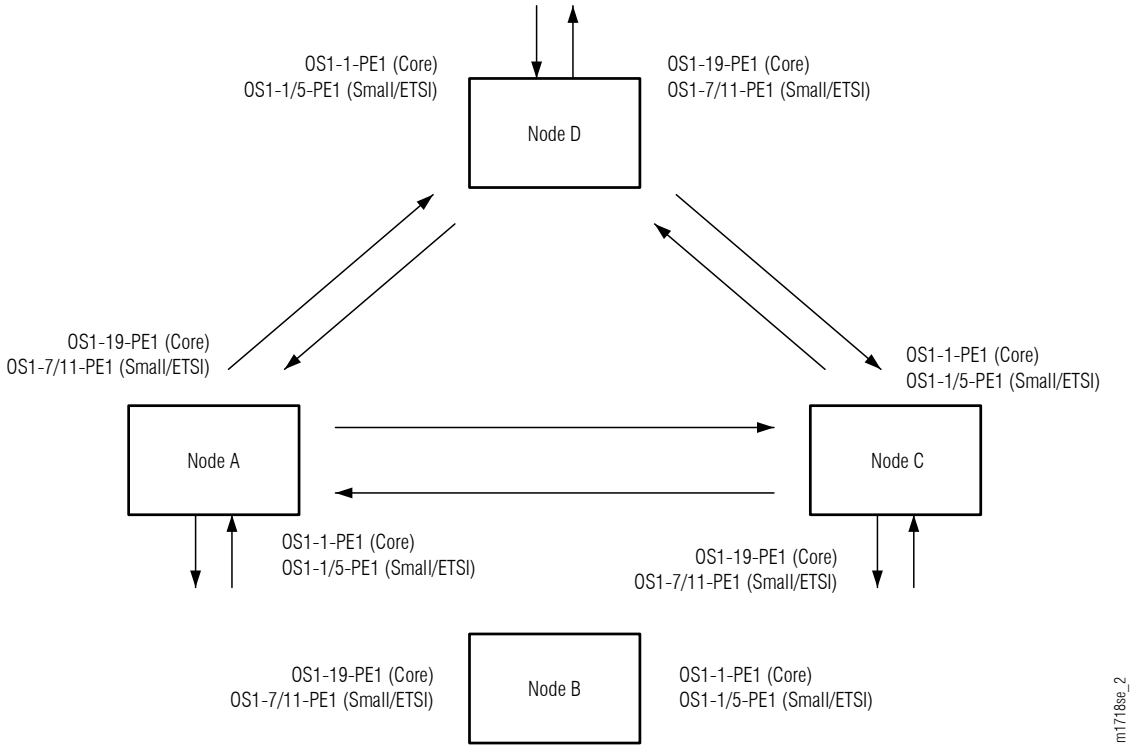


Figure 262: Ring Network After Node B Is Removed

This procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to the node being removed should be treated as Node D is treated.

5.3
References

Throughout this chapter, some procedures refer to other documents for more detailed instructions. Be sure to review and follow the referenced procedures within these documents when applicable:

- Introduction to Equipment Installation
- Introduction to System Turn-Up Core Configuration or Introduction to System Turn-Up Small and ETSI Configuration
- Introduction to System Operations General
- Introduction to TL1 Commands
- Introduction to Maintenance and Trouble Clearing
- *NETSMART 500 User Guide*

5.4 Add/Delete Node

In this section:

A flowchart of the overall process is shown in the following figure.

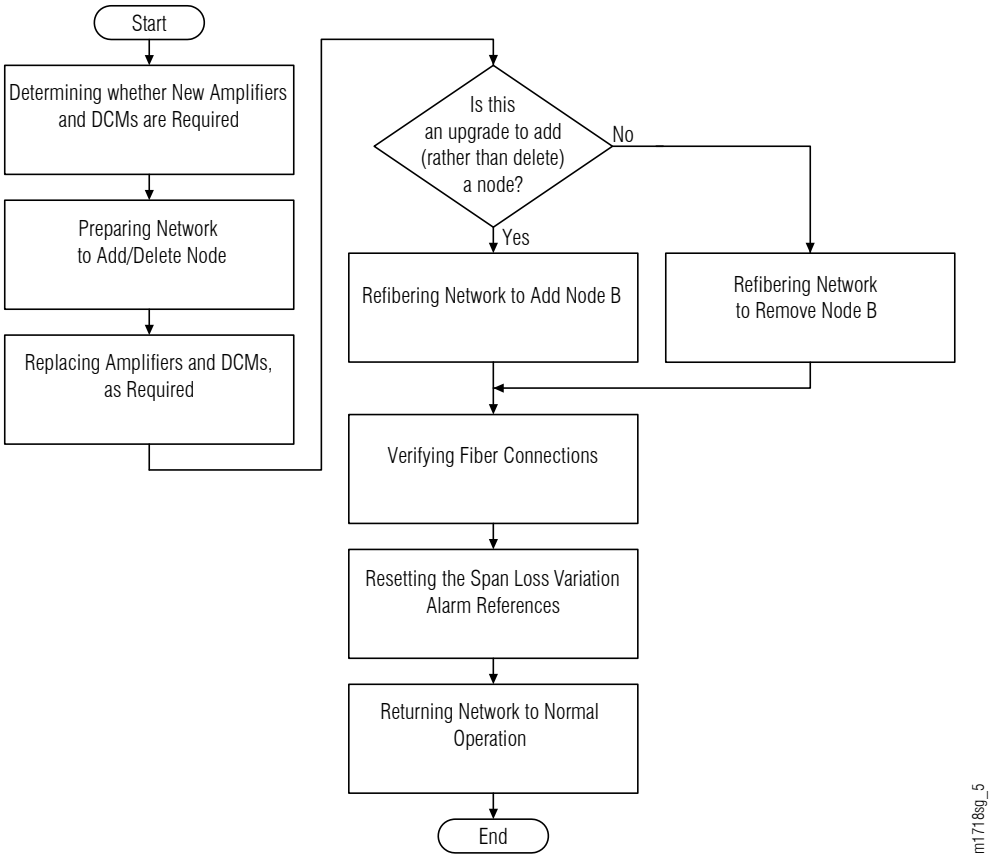


Figure 263: Adding/Deleting Node (Procedure Flowchart)

5.4.1 Determining Whether New Amplifiers and DCMs Are Required

Compile Amplifier and DCM Information

Step 1
Obtain the new amplifier and DCM specifications from the network design.

Step 2
Obtain the current amplifier and DCM information from existing node records.

Note: *If a node adjacent to a node being added to or deleted from a ring network is an ILA node (refer to Applications), the node on the other side of the ILA node may also require a new amplifier and DCM. Consult your network design team on how to proceed.*

Step 3
Enter the information in the appropriate table:

- The following table for Core Configuration

Table 47: Amplifier and DCM Information (Core Configuration)

Node	Direction	Equipment	Status	Unit Name[41]
A	OSn-1-PE1	Amplifier (Optical Shelf Slot 1)	Current	APMA -_ _ _ _
			New	APMA - _ _ _ _
		DCM	Current	
			New	
C	OSn-19-PE1	Amplifier (Optical Shelf Slot 19)	Current	APMA -_ _ _ _
			New	APMA -_ _ _ _
		DCM	Current	
			New	

- The following table for Small/ETSI Configuration

Table 48: Amplifier and DCM Information (ETSI Configuration)

Node	Direction	Equipment	Slot	Status	Equipment Type[42]
A	OSn-1-PE1	Amplifier	1 (Optical shelf)	Current	APMA - _ _ _ _
				Required	APMA - _ _ _ _

[41] If none, enter dash (–) or *None*. If no DCM is required, an optical jumper must be installed.
[42] If none, enter dash (–) or *None*. If no DCM is required, an optical jumper must be installed.

Table 48: Amplifier and DCM Information (ETSI Configuration) (Cont.)

Node	Direction	Equipment	Slot	Status	Equipment Type[42]
		Raman Amplifier/Mux Demux Unit[43][44]	5 (Optical shelf)	Current	
				Required	
		DCM	1 (DCM shelf)	Current	
				Required	
C	OSn-11-PE1	Amplifier	11 (Optical shelf)	Current	APMA - _ _ _ _
				Required	APMA -_ _ _ _
		Raman Amplifier/Mux Demux Unit[45]	7 (Optical shelf)	Current	
				Required	
		DCM	2 (DCM shelf)	Current	
				Required	

Step 4
Is the upgrade for a Small/ETSI Configuration system?

If YES:
Proceed to Step 5.

If NO:
Proceed to Step 6.

Determine Whether Raman Amplification Changes Are Required

Step 5
Refer to the information that was gathered in the preceding table. Does the upgrade require a change in either of the following plug in units?

- Node A, Optical shelf slot 5
- Node C, Optical shelf slot 7

If YES:
This upgrade procedure does not support changes in Raman amplification. Call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.

If NO:
Proceed to Step 6.

[43] Slot 5 supports either the Raman Amplifier (APMA-DRC1) or the multiplexer/demultiplexer unit (MDMA-RMC1).
[44] If Raman Amplifier (APMA-DRC1) is used in slot 5 of Optical shelf OS1/OS2, the multiplexer/demultiplexer unit (MDMA-RMC1) is displaced to slot 5 of Tributary shelf OS10/OS20.
[42] **If none, enter dash (–) or *None*. If no DCM is required, an optical jumper must be installed.**

Determine Whether New Amplifiers and DCMs Are Required

Step 6
Do the current and new unit names for the same amplifier(s) differ in Step 3?

Note: *For detailed information on amplifier equipment types, refer to* Amplifier Units.

If YES:
Proceed to Step 7.

If NO:
Proceed to Step 8.

Step 7
Obtain the new amplifier(s).

Note: *The amplifiers are required for the procedures in* Replacing Amplifiers and DCMs, as Required.

Step 8
Do the current and new unit names for the same DCM(s) differ in Step 3?

Note: *For detailed information on DCMs, refer to* Dispersion Compensation Modules.

If YES:
Proceed to Step 9.

If NO:
Proceed to Step 10.

Step 9
Obtain the new DCM(s) or optical jumpers.

Note: *The DCMs (or optical jumpers) are required in the procedures in* Replacing Amplifiers and DCMs, as Required.

Step 10
Proceed to Preparing Network to Add/Delete Node.

✔ This procedure is complete.

[42] **If none, enter dash (–) or *None*. If no DCM is required, an optical jumper must be installed.**
[45] If Raman Amplifier (APMA-DRC1) is used in slot 7 of Optical shelf OS1/OS2, the multiplexer/demultiplexer unit (MDMA-RMC1) is displaced to slot 7 of Tributary shelf OS10/OS20.

5.4.2
Preparing Network to Add/Delete Node

This procedure assumes the following conditions:

- Information is available (for example, from local records) for each optical channel dedicated protection ring (OCh-DPRING)–protected drop cross-connect on Node D that identifies which node in the ring network is the source of the channel signal dropped at Node D.

  Note: *This information is needed to complete* Step 45.

- If you are deleting Node B, no service is currently added or dropped at Node B.

- If you are adding Node B, Node B is turned up but not yet connected to the network.

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART® 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

To prepare to add or delete a node, perform the following steps:

Clear Alarms and Conditions

Step 1
If not already done, log on Nodes A, B (if applicable), C, and D. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values, apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	
	Comm. Port: COMx (for example, COM2)
	
	Configure: use default[46]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 2
At each node in the system, retrieve alarms and conditions.

[46] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), then proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Step 4
Is this an upgrade to add (rather than delete) Node B?

If YES:
Proceed to Step 5.

If NO:
Proceed to Step 7.

Turn Up Node B

Applicable to the Add Node Upgrade Only

Step 5
Turn up the Node B system, but do not connect network fiber-optic cables, and do not enter any cross-connects at this time.

Note: *Refer to System Turn-Up (Core Configuration), or System Turn-Up (Small/ETSI Configuration), but omit steps for connecting network cables to the NE.*

Step 6
Proceed to Step 9.

Verify Node B Cross-Connects Are Pass-Through
Applicable to the Delete Node Upgrade Only

Step 7
Retrieve all cross-connects at Node B.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select the cross-connect entity.
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are pass-through.
	
	Close the Properties dialog box.

Step 8
Does Node B have any add/drop cross-connects?

If YES:
Remove or reroute all services added or dropped at Node B, and repeat Step 7.

If NO:
Proceed to Step 9.

Verify Traffic Protection

Step 9
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services on the span being broken should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the span being upgraded. After the upgrade the traffic can be switched back.*

Step 10
Determine whether the drop path cross-connects at Nodes A, C, and D are OCh-DPRING–protected.

Note: *The cross-connect indicates a path switch default by keyword PSWDEF. The existence of this keyword indicates that the connection is OCh-DPRING–protected. The keyword is absent from cross-connects that are not OCh-DPRING–protected.*

Step 11
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 15.

If NO:
Some of the drop paths are unprotected. Proceed to Step 12.

Step 12
Do the unprotected drop paths go through the span between Node A and Node C?

If YES:
Proceed to Step 13.

If NO:
Proceed to Step 15.

Step 13
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B addition/deletion completes. Proceed to Step 14.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then proceed to Step 14.

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Provision OLC Adds and Drops.

Step 14
Is this an upgrade to add (rather than delete) Node B?

If YES:
Proceed to Step 15.

If NO:
Proceed to Step 19.

Provision Pass-Through Cross-Connects for Node B

Applicable to the Add Node Upgrade Only

Note: *These steps ensure that Node B passes the traffic that is currently passing between Node A and Node C appropriately when it is inserted into the ring network.*

Step 15
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 16
From the retrieved cross-connects from Node A, identify and record the WCH channel numbers of all cross-connects that direct traffic to /from Node C.

Inspect the toAID and fromAID for each retrieved cross-connect. If either AID is listed in the following table, record the channel number and the circuit identifier (CKTID) if applicable.

Table 49: AIDs for Node A Cross-Connects to/from Node C

Configuration		WCH Facility AIDs[47]	
Core Configuration		OSn-1-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c	
	with Raman Amplifier in slot 5	OSn-5-PE1-c	

Step 17
At Node B, for each WCH channel identified in Step 16, provision pass-through cross-connects in both directions.

TL1	NETSMART 500

`ENT-CRS-WCH:TID:fromAID,toAID:CTAG :::KEYWORD=DOMAIN;`
fromAID, toAID:
• Refer to the following table.
KEYWORD=DOMAIN:
• CKTID = Character string of up to 45 alphanumeric characters, including hyphens (-), delineated by escape quotes (\")
• **Null**
Example:
`(for channel 34)`
`ENT-CRS-WCH:FUJITSU-NODEB: OS1-1-PE1-34,OS1-19-PE1-34:CTAG; ENT-CRS-WCH:FUJITSU-NODEB: OS1-19-PE1-34,OS1-1-PE1-34:CTAG;`
	NE ▸ Graphical Cross-Connects
	The Cross-Connects window opens.
	From the View Rate drop-down list, select XC_WCH.
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment or facility associated with the fromAID.
	From a different drop-down list, select the equipment or facility associated with the toAID.
	Click on the fromAID to begin drawing a line that represents the connection.
	Click on the toAID to terminate the line.
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	Entity ▸ Operations Dialog
	Click Create.
	The dashed line becomes solid.
	Close the Operations dialog box.
	Do not close the Cross-Connects window.

[47] **If the toAID or fromAID of a WCH cross-connect at Node A is one of these values, then the cross-connect directs traffic to/from Node C.**

Table 50: Pass-Through WCH Cross-Connect AIDs

Configuration	fromAID	toAID
Core WSS	OSn-s-PE1-c (WCH facility) • n = 1…4, 25, 26 (shelf) • s = 1, 19 (slot) • c = 1…40 (channel)	OSn-s-PE1-c (WCH facility) • n = 1…4, 25, 26 (shelf) • s = 1, 19 (slot) • c = 1…40 (channel)
Core 2D-ROADM	OS1-s-PE1-c (WCH facility) • s = 1, 19 (slot) • c = 1…40 (channel)	OS1-s-PE1-c (WCH facility) • s = 1, 19 (slot) • c = 1…40 (channel)
Small/ETSI WSS	OSn-s-PE1-c (WCH facility) • n = 1, 2 (shelf) • s = 1, 5, 7, 11 (slot) • c = 1…40 (channel)	OSn-s-PE1-c (WCH facility) • n = 1, 2 (shelf) • s = 1, 5, 7, 11 (slot) • c = 1…40 (channel)
	Note: *WCH facility AIDs for each network degree depend on whether the Raman Amplifier (APMA-DRC1) is used. Slots 5 and 7 of the Optical shelf support the Raman Amplifier. If slot 5 is provisioned with the Raman Amplifier, the WCH facility AIDs are OSn-**5**-PE1-1…40, rather than OSn-**1**-PE1-1…40. If slot 7 is provisioned with the Raman Amplifier, the WCH facility AIDs are OSn-**7**-PE1-1…40, rather than OSn-**11**-PE1-1…40.*	
Small/ETSI 2D-ROADM	OS1-s-PE1-c (WCH facility) • s = 1, 11 (slot) • c = 1…40 (channel)	OS1-s-PE1-c (WCH facility) • s = 1, 11 (slot) • c = 1…40 (channel)
Small 32-Ch	OS1-s-PE1-c (WCH facility) • s = 1, 11 (slot) • c = 5…36 (channel)	OS1-s-PE1-c (WCH facility) • s = 1, 11 (slot) • c = 5…36 (channel)

Step 18
At Node B, verify that pass-through cross-connects have been provisioned in both directions for each WCH channel identified in Step 16.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that the provisioning parameters are correct.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node A)

Step 19
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 20
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 21
Are any dropped channels currently taking traffic from Node B/C (refer to the following table)?

Table 51: Decision Table (Node A)

Configuration	Retrieved Cross-Connect Values		Is Current Traffic Dropped from Node B/C?
	PSWDEF[48]	SST	
Core Configuration	OSn-1-PE1-c	DEF	Yes
		SWITCH	No
	OSn-19-PE1-c	DEF	No

[48] **c = 1...40 (channel number)**

Table 51: Decision Table (Node A) (Cont.)

Configuration	Retrieved Cross-Connect Values		Is Current Traffic Dropped from Node B/C?
	PSWDEF[48]	SST	
		SWITCH	Yes
Small/ETSI Configuration	OSn-1-PE1-c OSn-5-PE1-c	DEF	Yes
		SWITCH	No
	OSn-11-PE1-c OSn-7-PE1-c	DEF	No
		SWITCH	Yes

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable; then proceed to Step 22.

If NO:
Proceed to Step 26.

Step 22
At Node A, for each channel identified in Step 21, initiate a manual protection switch away from Node B/C.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

[48] **c = 1...40 (channel number)**

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• The AID of the WCH facility to switch away from. Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 52: WCH Facility AIDs to Switch Away From (Node A)

Configuration		AID	
Core Configuration		OSn-1-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c	
	with Raman Amplifier in slot 5	OSn-5-PE1-c	

Step 23
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from Node B/C (refer to Table 51).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 24
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 25
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 26.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 26.

Perform Forced Protection Switches (Node A)

Step 26
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from Node B/C.

Note: *This step should not impact traffic because all traffic should already be directed away from Node B/C.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• The AID of the WCH facility to switch away from. Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 53: WCH Facility AIDs to Switch Away From (Node A)

Configuration		AID	
Core Configuration		OSn-1-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c	
	with Raman Amplifier in slot 5	OSn-5-PE1-c	

Step 27
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 28
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 29
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 30.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 30.

Step 30
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from Node B/C.

Note: *Use the same criteria used in Step 21.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Step 31
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 32
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 33
Are any dropped channels currently taking traffic from Node A/B (refer to the following table)?

Table 54: Decision Table (Node C)

Configuration		Retrieved Cross-Connect Values		Is Current Traffic Dropped from Node A/B?
		PSWDEF[49]	SST	
Core Configuration		OSn-1-PE1-c	DEF	No
			SWITCH	Yes
		OSn-19-PE1-c	DEF	Yes
			SWITCH	No
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c	DEF	No

[49] **c = 1...40 (channel number)**

Table 54: Decision Table (Node C) (Cont.)

Configuration		Retrieved Cross-Connect Values		Is Current Traffic Dropped from Node A/B?
		PSWDEF[49]	SST	
	with Raman Amplifier in slot 5	OSn-5-PE1-c	SWITCH	Yes
	without Raman Amplifier in slot 7	OSn-11-PE1-c	DEF	Yes
	with Raman Amplifier in slot 7	OSn-7-PE1-c	SWITCH	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable; then proceed to Step 34.

If NO:
Proceed to Step 38.

Step 34
At Node C, for each channel identified in Step 33, initiate a manual protection switch away from Node A/B.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

[49] c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• The AID of the WCH facility to switch away from. Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 55: WCH Facility AIDs to Switch Away From (Node C)

Configuration		AID	
Core Configuration		OSn-19-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 7	OSn-11-PE1-c	
	with Raman Amplifier in slot 7	OSn-7-PE1-c	

Step 35
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from Node A/B (refer to Table 54).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 36
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 37
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 38.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 38.

Perform Forced Protection Switches (Node C)

Step 38
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from Node A/B.

Note: *This step should not impact traffic because all traffic should already be directed away from Node A/B.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• The AID of the WCH facility to switch away from. Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 56: WCH Facility AIDs to Switch Away From (Node C)

Configuration		AID	
Core Configuration		OSn-19-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 7	OSn-11-PE1-c	
	with Raman Amplifier in slot 7	OSn-7-PE1-c	

Step 39
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 40
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 41
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 42.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 42.

Step 42
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from Node A/B.

Note: *Use the same criteria used in Step 33.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Step 43
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 44
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 45
For each drop cross-connect identified in Step 44, identify which network direction (WDM-1 or WDM-2; refer to the following table) is the ***break direction***. The break direction is the network direction that will lose signal if Network Segment AC is opened to add or remove Node B.

Table 57: Network Directions

Configuration	WDM-1	WDM-2
Core Configuration	OSn-1-PE1	OSn-19-PE1
Small/ETSI Configuration	OSn-1-PE1 (Raman not used) OSn-5-PE1 (Raman used)	OSn-11-PE1 (Raman not used) OSn-7-PE1 (Raman used)

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Travelling around the ring network from Node D in the WDM-1 direction, do you arrive at Network Segment AC before you arrive at the source node?

Step 46
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 58: Decision Table (Node D)

Configuration		Retrieved Cross-Connect Values		Break Direction[50]	Is Current Traffic Dropped from the Break Direction?
		PSWDEF[51]	SST		
Core Configuration		OSn-1-PE1-c	DEF	OSn-1-PE1	Yes
				OSn-19-PE1	No
			SWITCH	OSn-1-PE1	No
				OSn-19-PE1	Yes
		OSn-19-PE1c	DEF	OSn-1-PE1	No
				OSn-19-PE1	Yes
			SWITCH	OSn-1-PE1	Yes
				OSn-19-PE1	No
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c	DEF	OSn-1/5-PE1	Yes
				OSn-7/11-PE1	No
	with Raman Amplifier in slot 5	OSn-5-PE1-c	SWITCH	OSn-1/5-PE1	No
				OSn-7/11-PE1	Yes
	without Raman Amplifier in slot 7	OSn-11-PE1-c	DEF	OSn-1/5-PE1	No
				OSn-7/11-PE1	Yes
	with Raman Amplifier in slot 7	OSn-7-PE1-c	SWITCH	OSn-1/5-PE1	Yes
				OSn-7/11-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable, and then proceed to Step 47.

If NO:
Proceed to Step 47.

[50] Refer to Step 45.
[51] c = 1...40 (channel number)

Step 47
At Node D, for each channel identified in Step 46, initiate a manual protection switch away from the break direction.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• The AID of the WCH facility to switch away from. Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 59: WCH Facility AIDs to Switch Away From (Node D)

Configuration		WCH Facility AIDs[52]			
		If WDM-1 is the Break Direction		If WDM-2 is the Break Direction	
Core Configuration		OSn-1-PE1-c	c = 1...40 (channel number)	OSn-19-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c		n/a	
	with Raman Amplifier in slot 5	OSn-5-PE1-c		n/a	
	without Raman Amplifier in slot 7	n/a		OSn-11-PE1-c	
	with Raman Amplifier in slot 7	n/a		OSn-7-PE1-c	

Step 48
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 58).

[52] **Refer to Step 45 for an explanation of break direction.**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 49
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 50
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 51.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 51.

Perform Forced Protection Switches (Node D)

Step 51
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction identified in Step 46.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• The AID of the WCH facility to switch away from. Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 60: WCH Facility AIDs to Switch Away From (Node D)

Configuration		WCH Facility AIDs[53]			
		If WDM-1 is the Break Direction		If WDM-2 is the Break Direction	
Core Configuration		OSn-1-PE1-c	c = 1...40 (channel number)	OSn-19-PE1-c	c = 1...40 (channel number)
Small/ETSI Configuration	without Raman Amplifier in slot 5	OSn-1-PE1-c		n/a	
	with Raman Amplifier in slot 5	OSn-5-PE1-c		n/a	
	without Raman Amplifier in slot 7	n/a		OSn-11-PE1-c	
	with Raman Amplifier in slot 7	n/a		OSn-7-PE1-c	

Step 52
Retrieve conditions at Node D to verify that the forced protection switches occurred.

[53] **Refer to Step 45 for an explanation of break direction.**

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 53
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 54
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 55.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 55.

Step 55
At Node D, retrieve all cross-connects and verify that no dropped channels are currently taking traffic from the break direction.

Note: *Use the same criteria used in Step 46.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 56
If more than one nonadjacent node (similar to Node D) exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 57
Proceed to Replacing Amplifiers and DCMs, as Required.

✔ This procedure is complete.

5.4.3 Replacing Amplifiers and DCMs, as Required

Warning: *The APMA-M2U1 amplifier unit with built-in variable optical attenuation (VOA) only supports DCAX dispersion compensation module (DCM) unit types. The APMA-ULU1 dual-stage amplifier with built-in VOA supports both DCMX and DCAX DCM unit types. If the APMA-ULU1 dual-stage amplifier is used in association with a RAMAN amplifier (APMA-DRC1), only the DCAX DCM unit type is supported.*

Warning: *When replacing a Release 4 amplifier with a Release 5 amplifier, do not uninstall the network-side DCMX DCM (and associated attenuators) unless it is being replaced with a DCAX DCM.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

To replace amplifiers and DCMs, as required, perform the following steps:

Note: *Perform this procedure for both Node A and Node C, starting at either node.*

Note: *This procedure does not support amplifier replacement for network degrees that include Raman Amplification. Refer to* Step 5 *in* Determining Whether New Amplifiers and DCMs Are Required.

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Note: *Default values are shown in bold.*

Determine Which Amplifiers and DCMs to Replace

Step 1
Does the amplifier need to be replaced based on the information from Determining Whether New Amplifiers and DCMs Are Required?

If YES:
Proceed to Step 4.

If NO:
Proceed to Step 2.

Step 2
Does the DCM (or jumper) connected to the amplifier need to be replaced based on the information from Determining Whether New Amplifiers and DCMs Are Required?

If YES:
Proceed to Step 27.

If NO:
Proceed to Step 3.

Step 3
Was this procedure performed at both Nodes A and C?

If YES:
Proceed to Refibering Network to Add Node B.

If NO:
Repeat procedure for second node starting with Step 1.

Place Amplifier and Dependent Entities Out of Service

Step 4
If not already done, log on the node (Step 1 in Preparing Network to Add/Delete Node). If already logged on, proceed to the next step.

Step 5
Place the OSC facility associated with the amplifier in the Out of Service (OOS) state.

TL1	NETSMART 500

`ED-OSC:TID:AID:CTAG::::OOS;`
AID:
• Refer to the following table.
Example:
`ED-OSC:FUJITSU:OS1-9-PE1:CTAG::::`
`OOS;`
	Click the Facility tab in the tree view.
	Select OSC component.
	Entity ▸ *Operations Dialog*
	Select the State tab.
	Select OOS.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 61: Applicable OSC Facility AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-9-PE1
	Node C	OSn-11-PE1
Small/ETSI Configuration	Node A	OSn-13-PE1
	Node C	OSn-15-PE1

Step 6
Verify that the OSC facility is removed from service.

TL1	NETSMART 500

`RTRV-OSC:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-OSC:FUJITSU:OS1-9-PE1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the facility is OOS.
	Close the Operations dialog box.

Step 7
Place the WDM associated with the amplifier in the Out of Service (OOS) state.

TL1	NETSMART 500

`ED-WDM:TID:AID:CTAG::::OOS;`
AID:
• Refer to the following table.
Example:
`ED-WDM:FUJITSU:OS1-1-PE1:CTAG::::`
`OOS;`
	Click the Facilities tab in the tree view.
	Expand the appropriate shelf component.
	Select WDM.
	Entity ▸ *Operations Dialog*
	Select the State tab.
	Select OOS.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 62: Applicable WDM Facility AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-1-PE1
	Node C	OSn-19-PE1
Small/ETSI[54] Configuration	Node A	OSn-1-PE1
	Node C	OSn-11-PE1

Step 8
Verify that the WDM is removed from service.

TL1	NETSMART 500

`RTRV-WDM:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-WDM:FUJITSU:OS1-1-PE1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the facility is OOS.
	Close the Operations dialog box.

[54] This table does not include WDM facility AIDs for network degrees supported by Raman amplification because this procedure does not support amplifier replacement for network degrees that include Raman Amplification. Refer to Step 5 in Determining Whether New Amplifiers and DCMs Are Required.

Step 9
Place the amplifier equipment entity in the Out of Service (OOS) state.

TL1	NETSMART 500

`ED-EQPT:TID:AID:CTAG::::OOS;`
AID:
• Refer to the following table.
Example:
`ED-EQPT:FUJITSU:OS1-1:CTAG::::OOS;`
	In the tree view, click the Equipment tab.
	Expand the appropriate shelf.
	Select the appropriate slot.
	OR
	In the graphical view, select the appropriate slot.
	Entity ▸ *Operations Dialog*
	On the State tab, select the New Prov. state option *Out of Service (ED:OOS)*.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 63: Applicable Amplifier Unit Equipment AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-1
	Node C	OSn-19
Small/ETSI Configuration	Node A	OSn-1
	Node C	OSn-11

Step 10
Verify that the amplifier equipment entity is out of service.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-EQPT:FUJITSU:OS1-1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the equipment is OOS.
	Close the Operations dialog box.

Remove Amplifier

Step 11
Inspect the fiber connections to the amplifier plug-in unit, and verify that each fiber is clearly marked or labeled to identify the connector to which the fiber is connected. Refer to the following table for amplifier locations.

Table 64: Applicable Amplifier Unit

Configuration	Node	Shelf	Slot
Core Configuration	Node A	OSn	1
	Node C	OSn	19
Small/ETSI Configuration	Node A	OSn	1
	Node C	OSn	11

Step 12
Is each fiber clearly marked to identify its corresponding connector?

Note: *Fiber marking or labeling depends on local practice.*

If YES:
Continue to Step 13.

If NO:
Mark or label fibers according to local practice; then, repeat this step.

Step 13
Disconnect fibers, and remove the amplifier.

Provision Amplifier and Place Amplifier and Dependent Entities In Service

Note: *To edit the amplifier equipment type, the amplifier must be in a RMVD, UNEQ, or MEA standing condition.*

Note: *An MEA alarmed condition will not be raised for the following amplifier equipment replacement because these amplifiers are compatible:*

- *Provisioned TYPE = APMA-S2C1 and Actual TYPE = APMA-M2C1 Issue 2*
- *Provisioned TYPE = APMA-M2C2 and Actual TYPE = APMA-L2C1 Issue 3*
- *Provisioned TYPE = APMA-M2C1 Issue 2 and Actual TYPE = APMA-M2U1*

- *Provisioned TYPE = APMA-ULC1 and Actual TYPE = APMA-ULU1*
- *Provisioned TYPE = APMA-L2C1 Issue 3 and Actual TYPE = APMA-ULU1*

Step 14
Edit amplifier equipment entity to the appropriate type.

TL1	NETSMART 500

`ED-EQPT:TID:AID:CTAG::TYPE;`
AID:
• Refer to the following table.
TYPE:
• APMA-L2C1
• APMA-M2C1
• APMA-ULC1
• APMA-M2U1
• APMA-ULU1
Example:
`ED-EQPT:FUJITSU:OS1-1:CTAG::`
`APMA-M2C1;`
	In the tree view, click the Equipment tab.
	Expand the appropriate shelf.
	Select the appropriate slot.
	OR
	In the graphical view, select the appropriate slot.
	Entity ▸ *Operations Dialog*
	Select the Upgrade tab.
	Select Amplifier Type.
	Click Modify.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 65: Applicable Amplifier Unit Equipment AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-1
	Node C	OSn-19
Small/ETSI Configuration	Node A	OSn-1
	Node C	OSn-11

Step 15
Verify that the amplifier equipment entity is provisioned correctly.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-EQPT:FUJITSU:OS1-1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the equipment provisioning parameters are correct.
	Close the Operations dialog box.

Step 16
Install the amplifier in its appropriate slot by doing the following:

a) Verify that the amplifier type displayed on the front panel of the amplifier plug-in unit matches the amplifier TYPE entered in Step 14.

b) Inspect the plug-in unit for possible damage or debris.

c) Slide the unit into the appropriate shelf slot.

Step 17
Edit the amplifier equipment entity and place it in the In Service (IS) state.

TL1	NETSMART 500

`ED-EQPT:TID:AID:CTAG::::IS;`
AID:
• Refer to the following table.
Example:
`ED-EQPT:FUJITSU:OS1-1:CTAG::::IS;`
	In the tree view, click the Equipment tab.
	Expand the appropriate shelf.
	Select the appropriate slot.
	OR
	In the graphical view, select the appropriate slot.
	Entity ▸ *Operations Dialog*
	Select the State tab.
	Select ENT:IS.
	Click Modify.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 66: Applicable Amplifier Unit Equipment AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-1
	Node C	OSn-19
Small/ETSI Configuration	Node A	OSn-1
	Node C	OSn-11

Step 18
Verify that the amplifier equipment entity is In Service and provisioned correctly.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-EQPT:FUJITSU:OS1-1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the equipment is IS and the provisioning parameters are correct.
	Close the Operations dialog box.

Step 19
Place the WDM facility in the In Service (IS) state.

TL1	NETSMART 500

`ED-WDM:TID:AID:CTAG::::IS;`
AID:
• Refer to the following table.
Example:
`ED-WDM:FUJITSU:OS1-1-PE1:CTAG::::`
`IS;`
	Click the Facilities tab in the tree view.
	Expand the appropriate shelf component.
	Select WDM.
	Entity ▸ *Operations Dialog*
	Select the State tab.
	Select IS.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 67: Applicable WDM Facility AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-1-PE1
	Node C	OSn-19-PE1
Small/ETSI[55] Configuration	Node A	OSn-1-PE1
	Node C	OSn-11-PE1

Step 20
Verify that the WDM is In Service and provisioned correctly.

[55] This table does not include WDM facility AIDs for network degrees supported by Raman amplification because this procedure does not support amplifier replacement for network degrees that include Raman Amplification. Refer to Step 5 in Determining Whether New Amplifiers and DCMs Are Required.

TL1	NETSMART 500

`RTRV-WDM:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-WDM:FUJITSU:OS1-1-PE1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the facility is IS.
	Close the Operations dialog box.

Step 21
Place the OSC facility associated with the amplifier in the In Service (IS) state.

TL1	NETSMART 500

`ED-OSC:TID:AID:CTAG::::IS;`
AID:
• Refer to the following table.
Example:
`ED-OSC:FUJITSU:OS1-9-PE1:CTAG::::`
`IS;`
	Click the Facility tab in the tree view.
	Select OSC component.
	Entity ▸ *Operations Dialog*
	Select the State tab.
	Select IS.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Table 68: Applicable OSC Facility AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-9-PE1
	Node C	OSn-11-PE1
Small/ETSI Configuration	Node A	OSn-13-PE1
	Node C	OSn-15-PE1

Step 22
Verify that the OSC facility is In Service and provisioned correctly.

TL1	NETSMART 500

`RTRV-OSC:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-OSC:FUJITSU:OS1-9-PE1:CTAG;`
	In the Current Values area of the Operations dialog box, verify that the facility is IS.
	Close the Operations dialog box.

Reconnect Amplifier Fibers

Step 23
Identify the fiber-optic cables that were disconnected in Step 13.

Step 24
Clean the optical connectors on the optical fibers. Refer to Fiber Cable Handling.

Step 25
Carefully connect the fiber-optic cables to the proper connectors on the amplifier plug-in unit.

Step 26
Does the DCM connected to the amplifier need to be replaced based on the information from Determining Whether New Amplifiers and DCMs Are Required?

If YES:
Proceed to Step 27.

If NO:
Proceed to Step 3.

Replace DCM

Step 27
Inspect the fiber connections to the DCM. Verify that each fiber is clearly marked or labeled to identify the connector to which the fiber is connected.

Warning: *The APMA-M2U1 amplifier unit with built-in variable optical attenuation (VOA) only supports DCAX dispersion compensation module (DCM) unit types. The APMA-ULU1 dual-stage amplifier with built-in VOA supports both DCMX and DCAX DCM unit types. If the APMA-ULU1 dual-stage amplifier is used in association with a RAMAN amplifier (APMA-DRC1), only the DCAX DCM unit type is supported.*

Warning: *When replacing a Release 4 amplifier with a Release 5 amplifier, do not uninstall the network-side DCMX DCM (and associated attenuators) unless it is being replaced with a DCAX DCM.*

Step 28
Is each fiber clearly marked to identify its corresponding connector?

Note: *Fiber marking or labeling depends on local practice.*

If YES:
Continue to next step.

If NO:
Mark or label fibers according to local practice; then, repeat this step.

Step 29
Disconnect the fibers, and remove the DCM.

Step 30
Insert the new DCM.

Step 31
Clean the optical connectors on the optical fibers. Refer to Fiber Cable Handling.

Step 32
Carefully connect the fiber-optic cables to the proper connectors on the DCM.

Step 33
Update inventory information for the DCM modules, as required.

TL1	NETSMART 500

`ED-DCM:TID:AID:CTAG:::`
`KEYWORD=DOMAIN;`
AID:
• Refer to Table 69.
KEYWORD=DOMAIN:
• Refer to Table 70.
Example:
`ED-DCM:FUJITSU:OS1-1:CTAG:::`
`DCM1VENDID=FC9682F220-01,`
`DCM1SERIALNO=1234567,`
`DCM3DOM=07-07,`
`DCM3CLEI=ABCD123456,`
`DCM3USI=ABCDEFGH12345678MNOPQRST;`
	In the tree view, select the Equipment tab.
	Expand the appropriate Optical shelf.
	Select amplifier unit.
	Entity ▸ *Operations Dialog*
	The Operations dialog box opens.
	Click the DCM tab.
	In the Command Parameters area, enter the DCM inventory information, per your local practice.
	Click Modify.
	Do not close the Operations dialog box.

Table 69: Applicable Amplifier Unit Equipment AIDs

Configuration	Node	AID
Core Configuration	Node A	OSn-1
	Node C	OSn-19
Small/ETSI Configuration	Node A	OSn-1
	Node C	OSn-11

Table 70: ED-DCM Keyword and Domain Input Parameters

Keyword	Domain	Description
DCMxVENDID (x=1...3)	FCnnnnnnnn-mm	DCM vendor ID, where FCnnnnnnnn is the 10-character FC code and mm is the 2-character hardware revision number (13-character string) ***Example:*** `FC9682F220-01`
DCMxSERIALNO(x=1...3)	nnnnnnn	DCM equipment unit serial number (up to a 7-character string)
DCMxDOM (x=1...3)	yy.mm	DCM date of manufacture, where yy = last two digits of the year and mm = 01...12 (5-character string)
DCMxCLEI (x=1...3)	nnnnnnnnnn	COMMON LANGUAGE® Equipment Identifier (CLEI™) (10-character string) ***Note:*** *The CLEI must be a 10-character string.* ***Note:*** *The CLEI attribute is associated with the shelf and provides inventory information about the plug-in unit.*
DCMxUSI(x=1...3)	nnnnnnnnnnnnnnnnnnnnnnnnn	DCM unique serial identifier (USI) (25-character string)

Step 34
Verify the DCM inventory information.

TL1	NETSMART 500

`RTRV-DCM:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-DCM:FUJITSU:OS1-1:CTAG;`
	Verify that the values shown in the Current Values area of the Operations dialog are correct.
	Close the Operations dialog box.

Step 35
Does the amplifier or DCM at the other node (Node A or C) need to be replaced?

If YES:
Repeat Steps 27 through 35 for the other node.

If NO:
Proceed to Step 36.

Step 36
Is this an upgrade to add (rather than delete) Node B?

If YES:
Proceed to Refibering Network to Add Node B.

If NO:
Proceed to Refibering Network to Remove Node B.

✔ This procedure is complete.

5.4.4
Refibering Network to Add Node B

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Reconnect the network fiber-optic cables to add Node B as follows:

Disconnect Node A and Node C

Step 1
Disconnect the two optical fibers connecting Node A to Node C. Refer to the following table.

Table 71: Network Fiber Connections between Nodes A and C

Configuration		Node A			Node C		
		Shelf	Slot	Connector	Shelf	Slot	Connector
Core Configuration		OSn	1	OPT IN	OSn	19	OPT OUT
		OSn	1	OPT OUT	OSn	19	OPT IN
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn	11	OPT OUT
		OSn	1	OPT OUT	OSn	11	OPT IN
	with Raman amplification	OSn	5	OPT IN	OSn	7	OPT OUT
		OSn	5	OPT OUT	OSn	7	OPT IN

Connect Node A and Node B

Step 2
Identify and clean both ends of the two network fiber-optic cables associated with the span between Nodes A and B.

Note: *This procedure assumes that both fiber-optic cables include all attenuators required by the network engineering design specification.*

Step 3
Connect the cable ends to the appropriate amplifiers and connectors. Refer to the following table.

Table 72: Network Fiber Connections between Nodes A and B

Configuration		Node A			Node B		
		Shelf	Slot	Connector	Shelf	Slot	Connector
Core Configuration		OSn	1	OPT IN	OSn	19	OPT OUT
		OSn	1	OPT OUT	OSn	19	OPT IN
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn	11	OPT OUT
		OSn	1	OPT OUT	OSn	11	OPT IN
	with Raman amplification	OSn	5	OPT IN	OSn	7	OPT OUT
		OSn	5	OPT OUT	OSn	7	OPT IN

The NOT READY indicators on the amplifiers light and then go out after approximately 5 minutes. After the NOT READY indicators go out, the FAIL/SVCE indicators light green on the amplifiers.

Step 4
After the NOT READY indicators go out and the FAIL/SVCE indicators light green, proceed to the next step.

Connect Node B and Node C

Step 5
Identify and clean both ends of the two network fiber-optic cables associated with the span between Nodes B and C.

Note: *This procedure assumes that both fiber-optic cables include all attenuators required by the network engineering design specification.*

Step 6
Connect the cable ends to the appropriate amplifiers and connectors. Refer to the following table.

Table 73: Network Fiber Connections between Nodes B and C

Configuration		Node B			Node C		
		Shelf	Slot	Connector	Shelf	Slot	Connector
Core Configuration		OSn	1	OPT IN	OSn	19	OPT OUT
		OSn	1	OPT OUT	OSn	19	OPT IN
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn	11	OPT OUT
		OSn	1	OPT OUT	OSn	11	OPT IN
	with Raman amplification	OSn	5	OPT IN	OSn	7	OPT OUT
		OSn	5	OPT OUT	OSn	7	OPT IN

The NOT READY indicators on the amplifiers light and then go out after approximately 5 minutes. After the NOT READY indicators go out, the FAIL/SVCE indicators light green on the amplifiers.

Step 7
After the NOT READY indicators go out and the FAIL/SVCE indicators light green, proceed to Verifying Fiber Connections.

✔ This procedure is complete.

5.4.5
Refibering Network to Remove Node B

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Reconnect the network fiber-optic cables to remove Node B as follows:

Disconnect Node A and Node B

Step 1
Disconnect the two optical fibers connecting Node A to Node B. Refer to the following table.

Table 74: Network Fiber Connections between Nodes A and B

Configuration		Node A			Node B		
		Shelf	Slot	Connector	Shelf	Slot	Connector
Core Configuration		OSn	1	OPT IN	OSn	19	OPT OUT
		OSn	1	OPT OUT	OSn	19	OPT IN
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn	11	OPT OUT
		OSn	1	OPT OUT	OSn	11	OPT IN
	with Raman amplification	OSn	5	OPT IN	OSn	7	OPT OUT
		OSn	5	OPT OUT	OSn	7	OPT IN

Disconnect Node B and Node C

Step 2
Disconnect the two optical fibers connecting Node B to Node C. Refer to the following table.

Table 75: Network Fiber Connections between Nodes B and C

Configuration		Node B			Node C		
		Shelf	Slot	Connector	Shelf	Slot	Connector
Core Configuration		OSn	1	OPT IN	OSn	19	OPT OUT
		OSn	1	OPT OUT	OSn	19	OPT IN
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn	11	OPT OUT
		OSn	1	OPT OUT	OSn	11	OPT IN
	with Raman amplification	OSn	5	OPT IN	OSn	7	OPT OUT
		OSn	5	OPT OUT	OSn	7	OPT IN

Connect Node A and Node C

Step 3
Identify and clean both ends of the two network fiber-optic cables associated with the span between Nodes A and C.

Note: *This procedure assumes that both fiber-optic cables include all attenuators required by the network engineering design specification.*

Step 4
Connect the cable ends to the appropriate amplifiers and connectors. Refer to the following table.

Table 76: Network Fiber Connections between Nodes A and C

Configuration		Node A			Node C		
		Shelf	Slot	Connector	Shelf	Slot	Connector
Core Configuration		OSn	1	OPT IN	OSn	19	OPT OUT
		OSn	1	OPT OUT	OSn	19	OPT IN
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn	11	OPT OUT
		OSn	1	OPT OUT	OSn	11	OPT IN
	with Raman amplification	OSn	5	OPT IN	OSn	7	OPT OUT
		OSn	5	OPT OUT	OSn	7	OPT IN

The NOT READY indicators on the amplifiers light and then go out after approximately 5 minutes. After the NOT READY indicators go out, the FAIL/SVCE indicators light green on the amplifiers.

Step 5
After the NOT READY indicators go out and the FAIL/SVCE indicators light green, proceed to Verifying Fiber Connections.

✔ This procedure is complete.

5.4.6
Verifying Fiber Connections

Verifying that every optical transmitter is connected to the correct optical receiver at the downstream node is important. Connection errors may not show up immediately as alarm indicators and can lead to protection switching failures.

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in Optical Specifications.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence so that network path switching has been enabled. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Step 1
If not already done, log on the node (Step 1 in Preparing Network to Add/Delete Node). If already logged on, proceed to the next step.

Step 2
At each modified node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Step 4
Choose one of the modified nodes to begin the verification process.

Note: *The following verification steps are applied at each modified node in turn. The node under verification is called the* ***current node****.*

Step 5
For only the amplifiers involved in the add/delete, do the following:

a) Identify the downstream node to which the amplifier plug-in unit is supposed to transmit. Also identify the shelf and slot in the downstream node to which the amplifier is supposed to transmit. The following table lists the possible shelf and slot locations.

Note: *The following table also lists the associated OSC facility AID for use in Step 5c.*

Table 77: Downstream Receive Connections and OSC Facilities

Configuration	Network Receive Connection on Downstream Node			OSC Facility AID
	Shelf	Slot	Connector	
Core Configuration	OSn	1	OPT IN	OSn-9-PE1

Table 77: Downstream Receive Connections and OSC Facilities (Cont.)

Configuration		Network Receive Connection on Downstream Node			OSC Facility AID
		Shelf	Slot	Connector	
			19	OPT IN	OSn-11-PE1
Small/ETSI Configuration	without Raman amplification	OSn	1	OPT IN	OSn-13-PE1
			11	OPT IN	OSn-15-PE1
	with Raman amplification	OSn	5	OPT IN	OSn-13-PE1
			7	OPT IN	OSn-15-PE1

b) While monitoring alarms for the downstream node, temporarily disconnect the fiber-optic cable from the amplifier plug-in unit connector OPT OUT on the current node.

c) Verify that an OSC LOS alarm (or WDM LOS alarm if a ROADM node) is raised for the appropriate OSC facility at the downstream node. Refer to the following table.

Note: *If a different node or facility produces an alarm instead, troubleshoot and correct the fiber connection error, and then repeat the verification process.*

d) Reconnect the fiber that was disconnected in Step 5b.

e) Verify that the downstream receiver OSC LOS alarm clears within a few seconds.

Step 6
Have all the amplifiers in the modified nodes been verified?

If YES:
Proceed to Resetting the Span Loss Variation Alarm References.

If NO:
Repeat Step 5 for each amplifier in every modified node.

Step 7
Proceed to Resetting the Span Loss Variation Alarm References.

5.4.7 Resetting the Span Loss Variation Alarm References

When a node has been added or deleted from the system, the system reference value (SYSREF) for the span loss variation (SLV) alarm associated with each amplifier on the network must be reset. The reset procedure for the Core Configuration is given in detail in Reset the Span Loss Variation Alarm References. The reset procedure for the Small/ETSI Configuration is given in detail in Reset the Span Loss Variation Alarm References.

Follow the applicable procedure for the system:

- Core Configuration Reset
- Small/ETSI Configuration Reset

Core Configuration Reset

Follow this procedure to set the value of SYSREF to the current span loss variation value for the Core configuration:

Step 1
Using the procedure in Reset the Span Loss Variation Alarm References, reset the span loss variation value for each amplifier.

Step 2
Proceed to Returning Network to Normal Operation.

Small/ETSI Configuration Reset

Follow this procedure to set the value of SYSREF to the current span loss variation value for the Small/ETSI configuration:

Step 1
Using the procedure in Reset the Span Loss Variation Alarm References, reset the span loss variation value for each amplifier.

Step 2
Proceed to Returning Network to Normal Operation.

5.4.8 Returning Network to Normal Operation

This procedure returns the ring network to normal operation (see Figure 260).

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

To release protection switches and verify that the network is free of alarms and conditions, perform the following steps:

Note: *Perform Steps 2 through 11 for each node in the ring network.*

Release Protection Switches

Note: *An audit of all the unprotected wavelengths and services on the span should be done. If these services/ connections are used by an external device providing protection, that device should be instructed to protection switch away from the span being upgraded. After the upgrade the traffic can be switched back.*

Step 1
If not already done, log on Nodes A, B, C, and D (Step 1 in Preparing Network to Add/Delete Node). If already logged on, proceed to the next step.

Step 2
Retrieve conditions to identify the forced protection switches.

Note: *If the amplifier procedure is performed, the forced switch will automatically clear when the WDM is deleted.*

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Release each forced protection switch.

TL1	NETSMART 500

`RLS-PROTNSW-WCH:TID:AID:CTAG;`
AID:
• The AID of either WCH facility in the protection group. Refer to the following table.
Example:
`RLS-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-1:CTAG;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Release tab.
	Click Release.

Table 78: WCH Facility AIDs

Configuration	WCH Facility AID
Core Configuration	OSn-s-PE1-c • s = 1, 19 (slot) • c = 1…40 (channel)
Small/ETSI	OSn-s-PE1-c • n = 1, 2 (shelf) • s = 1, 5, 7, 11 (slot) • c = 1…40 (channel)
	Note: *WCH facility AIDs for each network degree depend on whether the Raman Amplifier (APMA-DRC1) is used. Slots 5 and 7 of the Optical shelf support the Raman Amplifier. If slot 5 is provisioned with the Raman Amplifier, the WCH facility AIDs are OSn-**5**-PE1-1…40 rather than OSn-**1**-PE1-1…40. If slot 7 is provisioned with the Raman Amplifier, the WCH facility AIDs are OSn-**7**-PE1-1…40 rather than OSn-**11**-PE1-1…40.*

Step 4
Retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 5
Identify all OCh-DPRING–protected drop cross-connects that have parameter SST=`SWITCH`.

Note: *The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 6
Do local procedures require switch back to the preferred path?

If YES:
Proceed to Step 7.

If NO:
Proceed to Step 11.

Step 7
For each channel identified in Step 5, initiate a manual protection switch.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• Refer to the following table.
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Table 79: WCH Facility AIDs

Configuration	WCH Facility AID
Core Configuration	OSn-s-PE1-c • s = 1, 19 (slot) • c = 1…40 (channel)
Small/ETSI Configuration	OSn-s-PE1-c • n = 1, 2 (shelf) • s = 1, 5, 7, 11 (slot) • c = 1…40 (channel)

Table 79: WCH Facility AIDs (Cont.)

Configuration	WCH Facility AID
	Note: *WCH facility AIDs for each network degree depend on whether the Raman Amplifier (APMA-DRC1) is used. Slots 5 and 7 of the Optical shelf support the Raman Amplifier. If slot 5 is provisioned with the Raman Amplifier, the WCH facility AIDs are OSn-**5**-PE1-1...40 rather than OSn-**1**-PE1-1...40. If slot 7 is provisioned with the Raman Amplifier, the WCH facility AIDs are OSn-**7**-PE1-1...40 rather than OSn-**11**-PE1-1...40.*

Step 8
At Node A, retrieve all cross-connects, and confirm that all OCh-DPRING–protected drop cross-connects are switched to the preferred path (SST=DEF).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
   TID DATE TIME
M CTAG COMPLD
   "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 9
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 10
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 11.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 11.

Step 11
Repeat Steps 2 through 10 for each node in the ring network.

Verify Ring Network Is Free of Alarms and Conditions

Step 12
Clear the outstanding "Telink reconfiguration" condition at each end of the original span by changing the value of TELINK to 0:

TL1	NETSMART 500

`ED-TELINK:TID:AID:CTAG:::DOMTYPE=, LINKCOST=,FBRTYPE=,FBRLEN=,FBRLOSS=, LCOEFF=,FBRPMD=,PMDCOEFF=,PADR=, MEASSPANDISP=,MEASSPANDISPSLOPE=, MEASLAMBDA=,UNCERTAINTY=,PRVRNODEID=, PRVRTELID=,NBRDISC=,RECNF=,BULKLOSS=, RPRMRGN=,RPRMRGNDB=:STATE;`
 	
Example:
`ED-TELINK::OS1-1-PE1:C:::RECNF=0;`
	NE ▸ *Facilities* ▸ *TELINK* ▸ *Attributes* ▸ *Modify*

Note: *After a node is added or deleted, the CP topology information will only automatically update after 18 hours. Performing the procedure described in Step 12 refreshes the information immediately.*

Step 13
After clearing the "Telink reconfiguration" condition, return the value of the RECNF (reconfiguration time) to its default value (N):

TL1	NETSMART 500
ED-TELINK:TID:AID:CTAG:::DOMTYPE=, LINKCOST=,FBRTYPE=,FBRLEN=,FBRLOSS=, LCOEFF=,FBRPMD=,PMDCOEFF=,PADR=, MEASSPANDISP=,MEASSPANDISPSLOPE=, MEASLAMBDA=,UNCERTAINTY=,PRVRNODEID=, PRVRTELID=,NBRDISC=,RECNF=,BULKLOSS=, RPRMRGN=,RPRMRGNDB=:STATE; ***Example:*** ED-TELINK::OS1-1-PE1:C:::RECNF=N;	*NE* ▸ *Facilities* ▸ *TELINK* ▸ *Attributes* ▸ *Modify*

Step 14
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500
RTRV-COND-ALL:TID::CTAG; ***Example:*** RTRV-COND-ALL:FUJITSU::CTAG;	*NE* ▸ *Alarms* *View* ▸ *Filter* Verify that all Fault Types and Severity Levels are selected as reporting. Click Close. Close Active Alarms window.

Step 15
Are any other active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Verifying Fiber Connections.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Go to Step 16.

Step 16
Log off the nodes.

TL1	NETSMART 500
CANC-USER:TID:UID:CTAG; ***Example:*** CANC-USER:FUJITSU:ROOT:CTAG;	*File* ▸ *Exit* Click Yes to continue.

This procedure is complete.

✔ This procedure is complete.

6
Adding or Deleting a Tributary Shelf

In this chapter:

This chapter describes procedures for adding and deleting Tributary shelves in FLASHWAVE® 7500 systems. This chapter is applicable to Core, Small, and ETSI Configuration NEs.

6.1 Add Tributary Shelf

Use the following procedure to add Tributary shelves to a Core, Small, or ETSI Configuration system.

Step 1
Install the Tributary shelf using the procedures referenced in the following table.

Table 80: Adding a Tributary Shelf

Task	Practice and Section		
	Core Configuration	Small Configuration	ETSI Configuration
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle	Installing the Optical/ Tributary Shelf	Installing the Optical/ Tributary Shelf
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables	Installing Power, Ground, and Alarm Cables	Installing Power and Ground Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)	Installing LAN Cable (Optical/Tributary Shelf)	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units	
Create Tributary shelf entity, and install shelf processors.	Create Subtending Shelves and Install Shelf Processors	Create Subtending Shelves and Install Shelf Processors	
Provision synchronization and/or Tributary shelf OSC units, if required.[56]	Provision Synchronization and/or Tributary Shelf OSC Units	Provision Tributary Shelf Equipment	

Step 2
Are additional Tributary shelves being added to the node?

If YES:
Repeat this procedure.

If NO:
This procedure is complete.

[56] Refer to procedure for applicability.

6.2
Delete Tributary Shelf

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Danger: *Never handle exposed fiber with bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Warning: *When handling FLASHWAVE 7500 plug-in units, wear an ESD wrist strap with a minimum resistance of 1000 kilohms to prevent possible damage to the units. Before using the strap, check it for opens, shorts, and minimum resistance value. If the strap does not pass these checks, do not use it.*

Caution: *Verify that you have received a completed (COMPLD) response to each command before going to the next step. If unable to complete a command after several tries, call Fujitsu at 1-800-USE-FTAC (1-800-873-3822) for technical assistance.*

Step 1
If not already done, log on the node. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

<table>
<tr><th>TL1</th><th>NETSMART® 500</th></tr>
<tr><td>Start a terminal or terminal emulator program (for example, HyperTerminal®).

For TERM1 (Serial):
Press CTRL+X.

For TERM2 (TCP/IP):
Establish a Telnet session using IP address 192.168.1.1 and default port 23.

The Welcome screen opens.
Press 3 for TL1.</td><td rowspan="2">To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar:

Start > All Programs > Fujitsu > NETSMART 500

The NETSMART 500 Dashboard opens.

Click the Logon icon, or select NE > Logon.

Note: If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.

The NE Logon dialog box opens.
Make the following selections:

For TERM1 (Serial):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: Serial

Comm. Port: COMx (for example, COM2)

Configure: use default[57]

For TERM2 (TCP/IP):
TID: FUJITSU
User ID: ROOT
Password: ROOT/(Route66K)
Conn. Mode: TCP/IP
IP Address: 192.168.1.1
Port: 2024

Click Logon.

The NETSMART 500 NE View opens.

The Security Message dialog box opens.
Click OK.

Note: Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.</td></tr>
<tr><td>ACT-USER:TID:UID:CTAG::PID;
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)

Example:
ACT-USER:FUJITSU:ROOT:CTAG::ROOT;</td></tr>
</table>

Step 2
Remove all service from the Tributary shelf.

Note: *Refer to the procedures in* Service Deletion.

Step 3
Remove the fan units from service.

[57] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500

`ED-EQPT:TID:AID:CTAG::::OOS;`
AID:
• OSn-FAN-1…4 (Core Configuration)
  • n = 10…13, 20…23, 30…33, 40…43, 100, 101, 110, 111, 120, 130, 200, 210, 211, 220, 230, 300, 301, 311, 320, 330, 400, 401, 410, 411, 420, 430
• OSn-FAN-1…3 (Small/ETSI Configuration)
  • n = 10…13, 20…23, 30…33, 40…43, 100, 101, 110, 111, 120, 130, 200, 210, 211, 220, 230, 300, 301, 311, 320, 330, 400, 401, 410, 411, 420, 430
Example:
`ED-EQPT:FUJITSU:OS12-FAN-1&&OS12-FAN-4:CTAG::::OOS;`
	In the tree view, click the Equipment tab.
	Expand the appropriate shelf.
	Select the equipment entity.
	Note: *Select more than one component using CTRL +click (multiple) or SHIFT+click (range).*
	Entity ▸ *Operations Dialog*
	Click the State tab.
	Select the New Prov. state option *Out of Service (ED:OOS)*.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Step 4
Verify that the fan units have been removed from service.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-EQPT:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the equipment is OOS.
	Close the Operations dialog box.

Step 5
Remove the NE Management (NEM) Shelf Processor (MPMA-SHPx) unit from service.

TL1	NETSMART 500

`ED-EQPT:TID:AID:CTAG::::OOS;`
AID:
• OSn-MPMA-1
• • n = 10…13, 20…23, 30…33, 40…43, 100, 101, 110, 111, 120, 130, 200, 210, 211, 220, 230, 300, 301, 311, 320, 330, 400, 401, 410, 411, 420, 430 (Core Configuration)
• n = 10…13, 20…23, 30…33, 40…43, 100, 101, 110, 111, 120, 130, 200, 210, 211, 220, 230, 300, 301, 311, 320, 330, 400, 401, 410, 411, 420, 430 (Small/ETSI Configuration)
Example:
`ED-EQPT:FUJITSU:OS12-MPMA-1:CTAG::::OOS;`
	In the tree view, click the Equipment tab.
	Expand the appropriate shelf.
	Select the equipment entity.
	Entity ▸ *Operations Dialog*
	Click the State tab.
	Select the New Prov. state option *Out of Service (ED:OOS)*.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Step 6

Verify that the NEM Shelf Processor unit(s) have been removed from service.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-EQPT:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the equipment is OOS.
	Close the Operations dialog box.

Step 7

Remove the Tributary shelf from service.

TL1	NETSMART 500

`ED-EQPT:TID:AID:CTAG::::OOS;`
AID:
• OSn
• • n = 10…13, 20…23, 30…33, 40…43, 100, 101, 110, 111, 120, 130, 200, 210, 211, 220, 230, 300, 301, 311, 320, 330, 400, 401, 410, 411, 420, 430 (Core Configuration)
• n = 10…13, 20…23, 30…33, 40…43, 100, 101, 110, 111, 120, 130, 200, 210, 211, 220, 230, 300, 301, 311, 320, 330, 400, 401, 410, 411, 420, 430 (Small/ETSI Configuration)
Example:
`ED-EQPT:FUJITSU:OS12:CTAG::::OOS;`
	In the tree view, click the Equipment tab.
	Select the appropriate shelf.
	Entity ▸ *Operations Dialog*
	The Operations dialog box opens.
	Click the State tab.
	Select the New Prov. state option *Out of Service (ED:OOS)*.
	Click Modify.
	A confirmation dialog box opens.
	Click Yes.
	The Operations dialog box updates.
	Do not close the Operations dialog box.

Step 8
Delete the Tributary shelf equipment entity.

TL1	NETSMART 500

`DLT-EQPT:TID:AID:CTAG;`
AID:
• As identified in previous step
Example:
`DLT-EQPT:FUJITSU:OS12:CTAG;`
	In the Operations dialog box, click the Delete tab.
	Click Delete.
	Note: *If the prerequisite conditions for equipment removal have not been met (look for an "x" in the Passed column), make the appropriate changes, and repeat this step.*
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 9
Verify that the Tributary shelf equipment entity has been deleted.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• As identified in Step 7
• **ALL** (null)
Example:
`RTRV-EQPT:FUJITSU:OS12:CTAG;`
	In the tree view, verify that the Tributary shelf is not present.

Step 10
Log off the node.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

Step 11
Disconnect and remove the LAN cable connecting LAN1 on the back of the Tributary shelf from LANn on the back of the Main Optical shelf, Auxiliary Optical shelf, or other Tributary shelf.

For Core Configuration NEs, refer to the following figure and the following table.

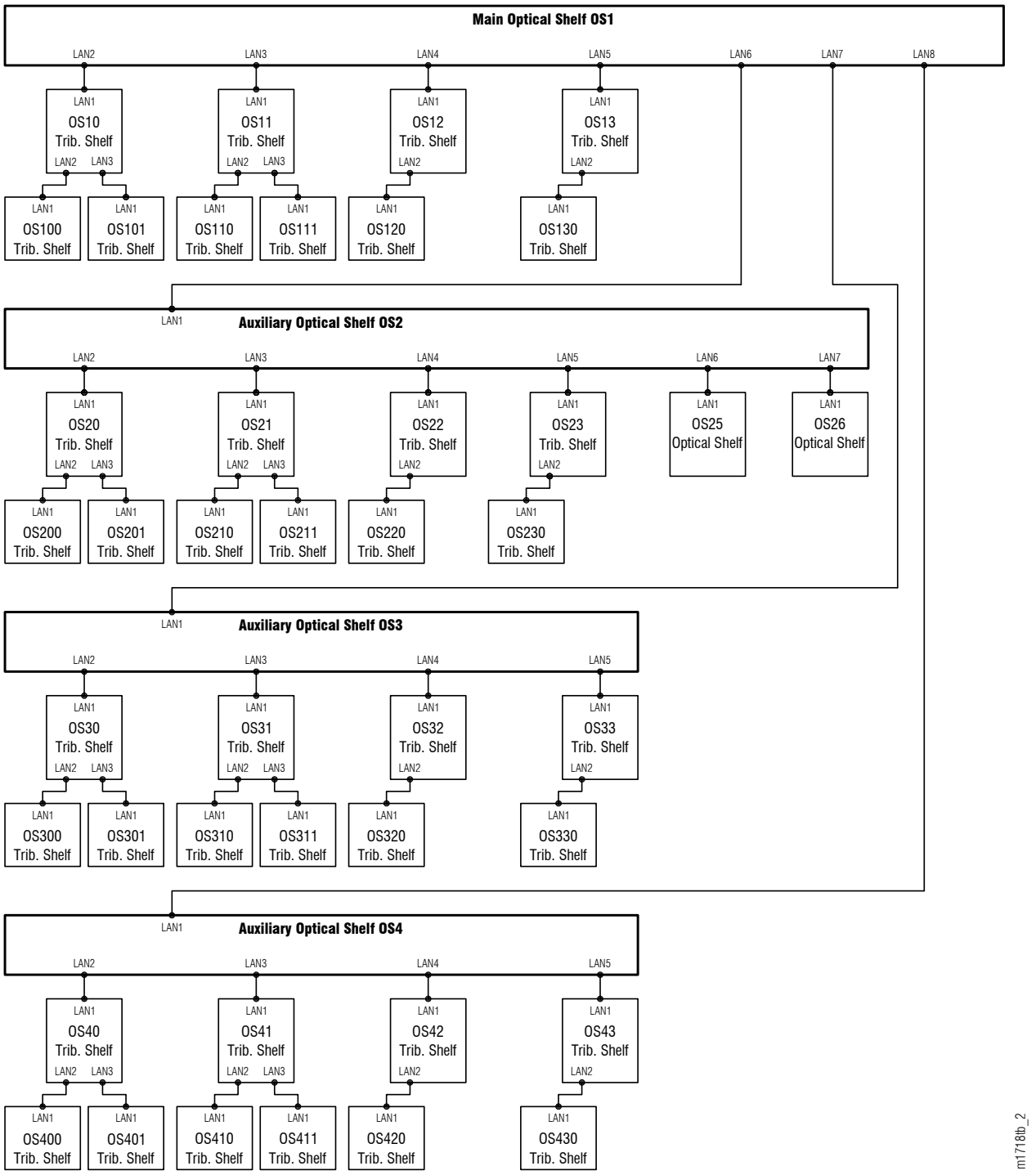


Figure 264: Shelf Hierarchy (FLASHWAVE 7500 Core Configuration)

Table 81: LAN Intershelf Connections(FLASHWAVE 7500 Core Configuration)

From			To		
Shelf	Connector	Label	Shelf	Connector	Label
OS1 (Main Optical)	CN19	LAN2	OS10 (Tributary)	CN18	LAN1
	CN20	LAN3	OS11 (Tributary)	CN18	LAN1
	CN21	LAN4	OS12 (Tributary)	CN18	LAN1
	CN22	LAN5	OS13 (Tributary)	CN18	LAN1
	CN23	LAN6	OS2 (Auxiliary Optical)	CN18	LAN1
	CN6	LAN7	OS3 (Auxiliary Optical)	CN18	LAN1
	CN7	LAN8	OS4 (Auxiliary Optical)	CN18	LAN1
OS10 (Tributary)	CN19	LAN2	OS100 (Tributary)	CN18	LAN1
	CN20	LAN3	OS101 (Tributary)	CN18	LAN1
OS11 (Tributary)	CN19	LAN2	OS110 (Tributary)	CN18	LAN1
	CN20	LAN3	OS111 (Tributary)	CN18	LAN1
OS12 (Tributary)	CN19	LAN2	OS120 (Tributary)	CN18	LAN1
OS13 (Tributary)	CN19	LAN2	OS130 (Tributary)	CN18	LAN1
OS2 (Auxiliary Optical)	CN19	LAN2	OS20 (Tributary)	CN18	LAN1
	CN20	LAN3	OS21 (Tributary)	CN18	LAN1
	CN21	LAN4	OS22 (Tributary)	CN18	LAN1
	CN22	LAN5	OS23 (Tributary)	CN18	LAN1
	CN23	LAN6	OS25 (Auxiliary Optical)	CN18	LAN1
	CN6	LAN7	OS26 (Auxiliary Optical)	CN18	LAN1
OS20 (Tributary)	CN19	LAN2	OS200 (Tributary)	CN18	LAN1
	CN20	LAN3	OS201 (Tributary)	CN18	LAN1
OS21 (Tributary)	CN19	LAN2	OS210 (Tributary)	CN18	LAN1
	CN20	LAN3	OS211 (Tributary)	CN18	LAN1
OS22 (Tributary)	CN19	LAN2	OS220 (Tributary)	CN18	LAN1
OS23 (Tributary)	CN19	LAN2	OS230 (Tributary)	CN18	LAN1
OS3 (Auxiliary Optical)	CN19	LAN2	OS30 (Tributary)	CN18	LAN1
	CN20	LAN3	OS31 (Tributary)	CN18	LAN1
	CN21	LAN4	OS32 (Tributary)	CN18	LAN1
	CN22	LAN5	OS33 (Tributary)	CN18	LAN1

Table 81: LAN Intershelf Connections(FLASHWAVE 7500 Core Configuration) (Cont.)

From			To		
Shelf	Connector	Label	Shelf	Connector	Label
OS30 (Tributary)	CN19	LAN2	OS300 (Tributary)	CN18	LAN1
	CN20	LAN3	OS301 (Tributary)	CN18	LAN1
OS31 (Tributary)	CN19	LAN2	OS310 (Tributary)	CN18	LAN1
	CN20	LAN3	OS311 (Tributary)	CN18	LAN1
OS32 (Tributary)	CN19	LAN2	OS320 (Tributary)	CN18	LAN1
OS33 (Tributary)	CN19	LAN2	OS330 (Tributary)	CN18	LAN1
OS4 (Auxiliary Optical)	CN19	LAN2	OS40 (Tributary)	CN18	LAN1
	CN20	LAN3	OS41 (Tributary)	CN18	LAN1
	CN21	LAN4	OS42 (Tributary)	CN18	LAN1
	CN22	LAN5	OS43 (Tributary)	CN18	LAN1
OS40 (Tributary)	CN19	LAN2	OS400 (Tributary)	CN18	LAN1
	CN20	LAN3	OS401 (Tributary)	CN18	LAN1
OS41 (Tributary)	CN19	LAN2	OS410 (Tributary)	CN18	LAN1
	CN20	LAN3	OS411 (Tributary)	CN18	LAN1
OS42 (Tributary)	CN19	LAN2	OS420 (Tributary)	CN18	LAN1
OS43 (Tributary)	CN19	LAN2	OS430 (Tributary)	CN18	LAN1

For Small and ETSI Configuration NEs, refer to the following figure and the following table.

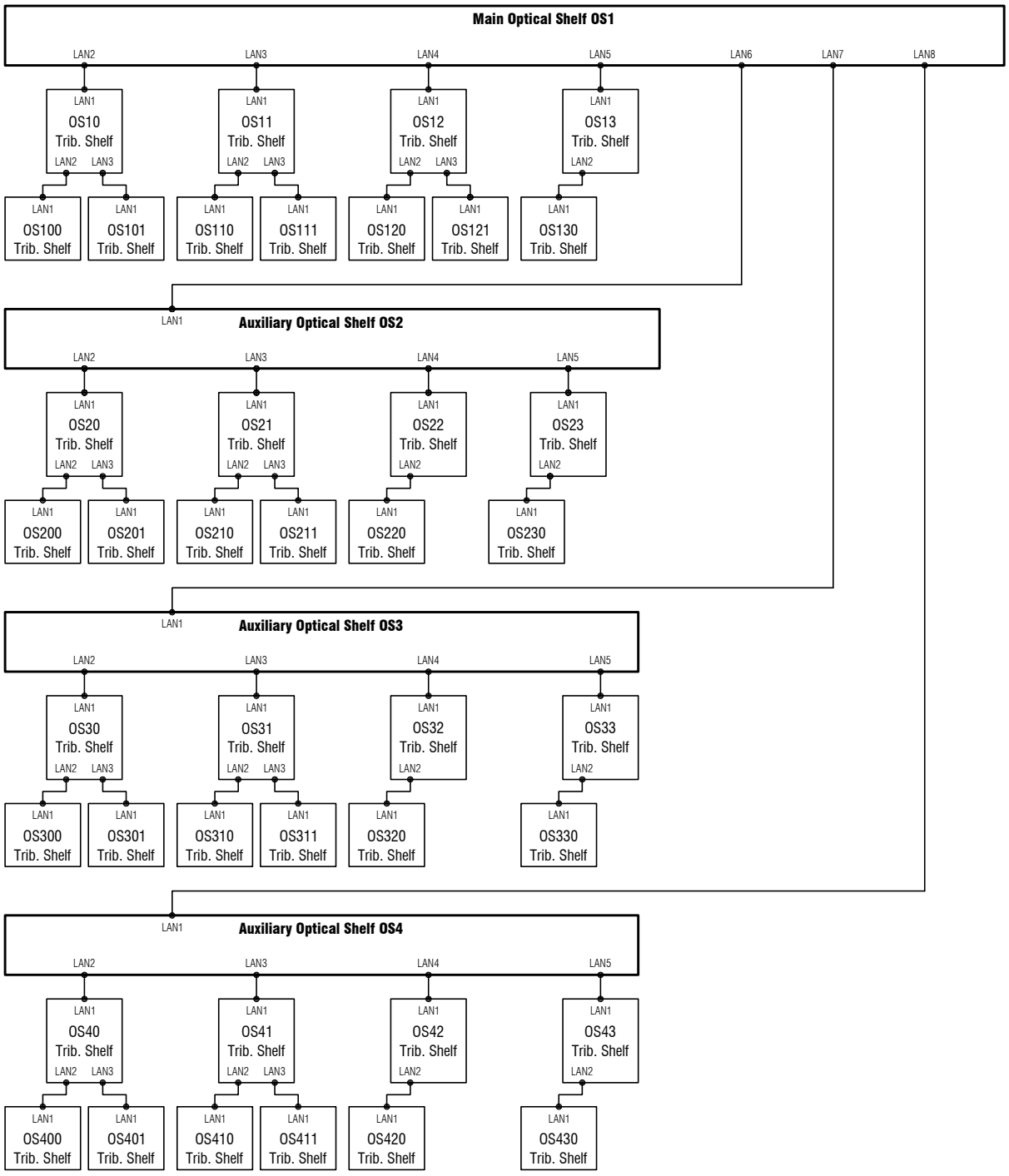


Figure 265: Shelf Hierarchy (FLASHWAVE 7500 Small/ETSI Configuration)

Table 82: LAN Connections (Small/ETSI Configuration)

From			To		
Shelf	Connector	Label	Shelf	Connector	Label
OS1 (Main Optical)	CN2	LAN2	OS10 (Tributary)	CN1	LAN1
	CN3	LAN3	OS11 (Tributary)	CN1	LAN1
	CN4	LAN4	OS12 (Tributary)	CN1	LAN1
	CN5	LAN5	OS13 (Tributary)	CN1	LAN1
	CN6	LAN6	OS2 (Auxiliary Optical)	CN1	LAN1
OS10 (Tributary)	CN2	LAN2	OS100 (Tributary)	CN1	LAN1
	CN3	LAN3	OS101 (Tributary)	CN1	LAN1
OS11 (Tributary)	CN2	LAN2	OS110 (Tributary)	CN1	LAN1
	CN3	LAN3	OS111 (Tributary)	CN1	LAN1
OS12 (Tributary)	CN2	LAN2	OS120 (Tributary)	CN1	LAN1
	CN3	LAN3	OS121 (Tributary)	CN1	LAN1
OS13 (Tributary)	CN2	LAN2	OS130 (Tributary)	CN1	LAN1
OS2 (Auxiliary Optical)	CN2	LAN2	OS20 (Tributary)	CN1	LAN1
	CN3	LAN3	OS21 (Tributary)	CN1	LAN1
	CN4	LAN4	OS22 (Tributary)	CN1	LAN1
	CN5	LAN5	OS23 (Tributary)	CN1	LAN1
OS20 (Tributary)	CN2	LAN2	OS200 (Tributary)	CN1	LAN1
	CN3	LAN3	OS201 (Tributary)	CN1	LAN1
OS21 (Tributary)	CN2	LAN2	OS210 (Tributary)	CN1	LAN1
	CN3	LAN3	OS211 (Tributary)	CN1	LAN1
OS22 (Tributary)	CN2	LAN2	OS220 (Tributary)	CN1	LAN1
OS23 (Tributary)	CN2	LAN2	OS230 (Tributary)	CN1	LAN1
OS3 (Auxiliary Optical)	CN2	LAN2	OS30 (Tributary)	CN1	LAN1
	CN3	LAN3	OS31 (Tributary)	CN1	LAN1
	CN4	LAN4	OS32 (Tributary)	CN1	LAN1
	CN5	LAN5	OS33 (Tributary)	CN1	LAN1
OS30 (Tributary)	CN2	LAN2	OS300 (Tributary)	CN1	LAN1
	CN3	LAN3	OS301 (Tributary)	CN1	LAN1
OS31 (Tributary)	CN2	LAN2	OS310 (Tributary)	CN1	LAN1

Table 82: LAN Connections (Small/ETSI Configuration) (Cont.)

From			To		
Shelf	Connector	Label	Shelf	Connector	Label
	CN3	LAN3	OS311 (Tributary)	CN1	LAN1
OS32 (Tributary)	CN2	LAN2	OS320 (Tributary)	CN1	LAN1
OS33 (Tributary)	CN2	LAN2	OS330 (Tributary)	CN1	LAN1
OS4 (Auxiliary Optical)	CN2	LAN2	OS40 (Tributary)	CN1	LAN1
	CN3	LAN3	OS41 (Tributary)	CN1	LAN1
	CN4	LAN4	OS42 (Tributary)	CN1	LAN1
	CN5	LAN5	OS43 (Tributary)	CN1	LAN1
OS40 (Tributary)	CN2	LAN2	OS400 (Tributary)	CN1	LAN1
	CN3	LAN3	OS401 (Tributary)	CN1	LAN1
OS41 (Tributary)	CN2	LAN2	OS410 (Tributary)	CN1	LAN1
	CN3	LAN3	OS411 (Tributary)	CN1	LAN1
OS42 (Tributary)	CN2	LAN2	OS420 (Tributary)	CN1	LAN1
OS43 (Tributary)	CN2	LAN2	OS430 (Tributary)	CN1	LAN1

Step 12
Remove the NEM Shelf Processor plug-in unit(s).

Step 13
Remove the fan plug-in units.

Step 14
Remove power from the Tributary shelf by setting the appropriate circuit breaker at the distribution panel to the OFF position.

Step 15
If necessary, follow local practice to disconnect power, ground, and alarm cables and completely remove the shelf.

Note: *Shelf removal can be modeled on the shelf installation process (Introduction to Equipment Installation) done in reverse.*

This procedure is complete.

7

Converting Linear Network, Core Configuration

In this chapter:

7.1 Converting a Linear Network to a Ring Network

This chapter describes the procedure for converting a linear network to a ring network. A span is inserted between Nodes A and C of a linear network to form a 3-node ring network as shown in the following figure.

Note: *This procedure can also be used to form a ring network with more than three nodes. In multiple-node ring networks, all nodes that are not adjacent to the insertion span should be treated as Node D is treated.*

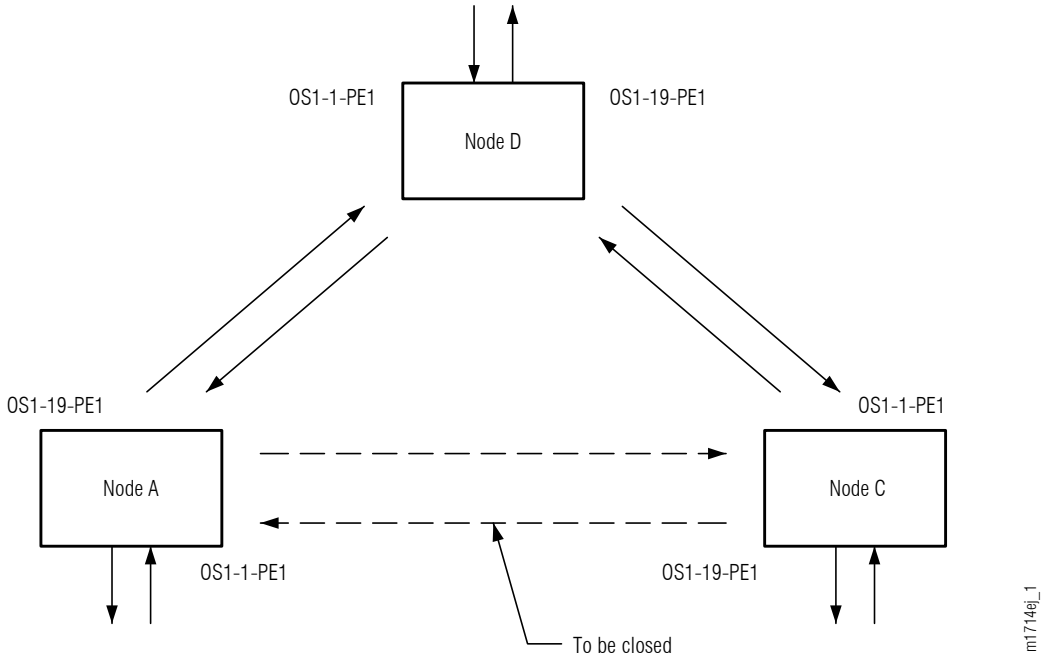


Figure 266: Insertion Span Forming a Ring Network

The following flowchart illustrates the sequences for converting a linear network into a ring network.

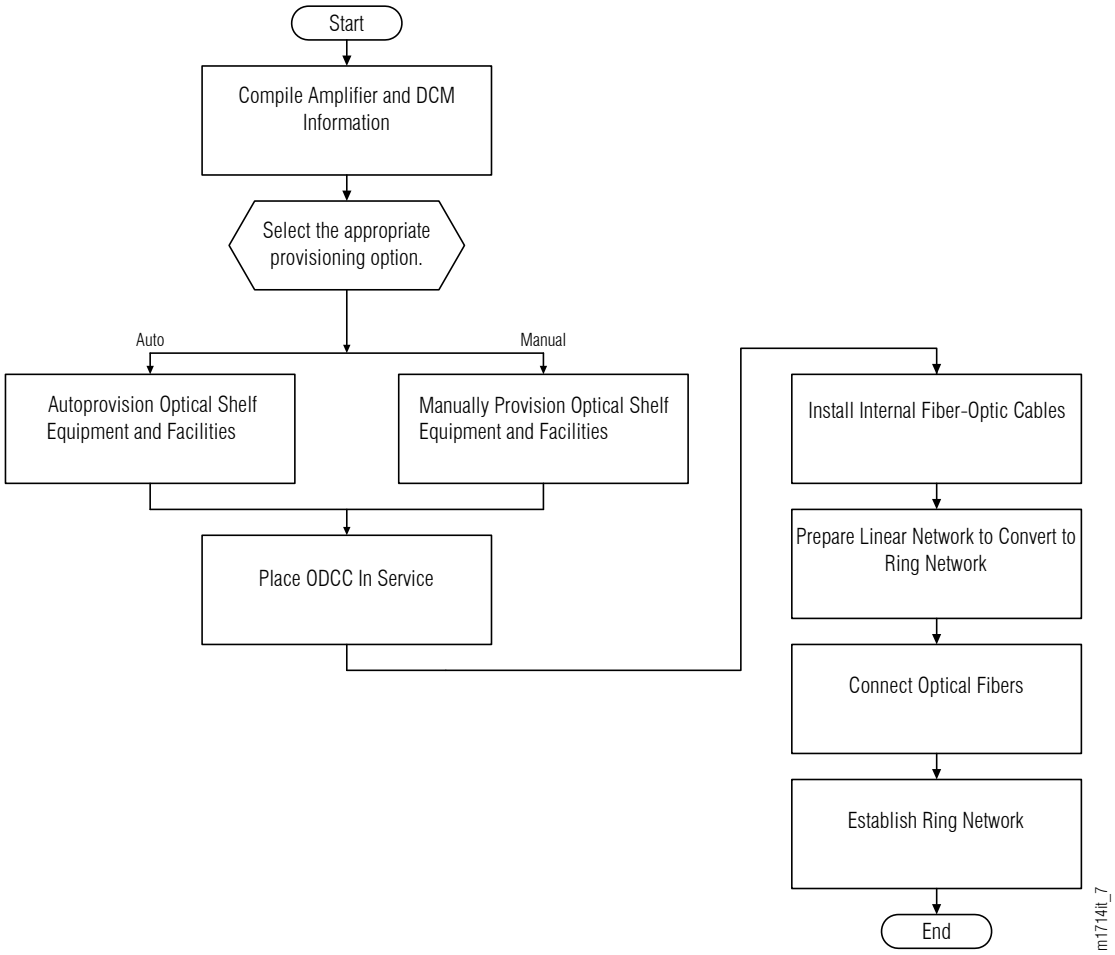


Figure 267: Convert Linear Network to Ring Network (Procedure Flowchart) (FLASHWAVE® 7500 Core Configuration)

7.2
References

Throughout this chapter, some procedures refer to other documents for more detailed instructions. Be sure to review and follow the referenced procedures within these documents when applicable:

- Introduction to Equipment Installation
- Introduction to System Turn-Up Core Configuration
- Introduction to System Operations General
- Introduction to TL1 Commands
- Introduction to Maintenance and Trouble Clearing
- *NETSMART 500 User Guide*

7.3 Compile Amplifier and DCM Information

Use this procedure to compile Amplifier and DCM information before proceeding to the procedures to convert a linear network to a ring network. For assistance, call the Fujitsu Technical Assistance Center at 1-800-USE-FTAC (1-800-873-3822).

Step 1
Obtain the equipment specifications from the network design.

Step 2
Enter information in the following table:

Equipment	Location	Unit Name	Quantity
Amplifier	Node A	APMA - _ _ _ _	1
	Node C	APMA - _ _ _ _	1
DCM[58]	Node A		
	Node C		
Mux/Demux unit	Node A	MDMA-RMC1	2
	Node C		
OSC Processing unit	Node A	SCMA-SCC4	2
	Node C		
WSS Core Switch unit	Node A	SFMA-CMC1	2
	Node C		

Step 3
Obtain the new equipment.

Note: *The equipment is required in the procedures in the following sections.*

Step 4
Select the appropriate procedure:

- To autoprovision the plug-in units, proceed to Autoprovision Optical Shelf Equipment and Facilities.
- To manually provision the plug-in units, proceed to Manually Provision Optical Shelf Equipment and Facilities.

[58] If none, enter dash (–) or *None*. If no DCM is required, an optical jumper must be installed.

7.4

Autoprovision Optical Shelf Equipment and Facilities

Optical shelf equipment can be installed and automatically provisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the optical shelf plug-in units within the Optical shelf.

Step 2
Proceed to Place ODCC In Service.

7.5
Manually Provision Optical Shelf Equipment and Facilities

Optical plug-in units can be installed and manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the plug-in units within the Optical shelf.

Note: *This procedure can be used to preprovision the slot. In this case, the unit will assume the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 2
Proceed to Place ODCC In Service.

7.6 Place ODCC In Service

An optical data communications channel (ODCC) can be assigned to every OSC facility up to a maximum of two channels per Optical shelf. The ODCC is used for communication with network-side nodes.

Step 1
Use the procedure in Place ODCC In Service, to place the ODCC in service.

Step 2
Proceed to Install Internal Fiber-Optic Cables.

7.7 Install Internal Fiber-Optic Cables

In this section:

Overview Connecting Fiber-optic Cables Core Configuration

The subprocedure in Connecting Optical Shelf Plug-In Units is used to install fiber-optic cables between plug-in units within the Optical shelf. The subprocedure in Connecting DCM) is used to connect dispersion compensation modules (DCMs) to amplifiers (APMA-xxxx) in the Optical shelf.

Danger: *Never handle exposed fiber with bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

7.7.1 Connecting Optical Shelf Plug-In Units

The following figure shows the cables installed at Node A.

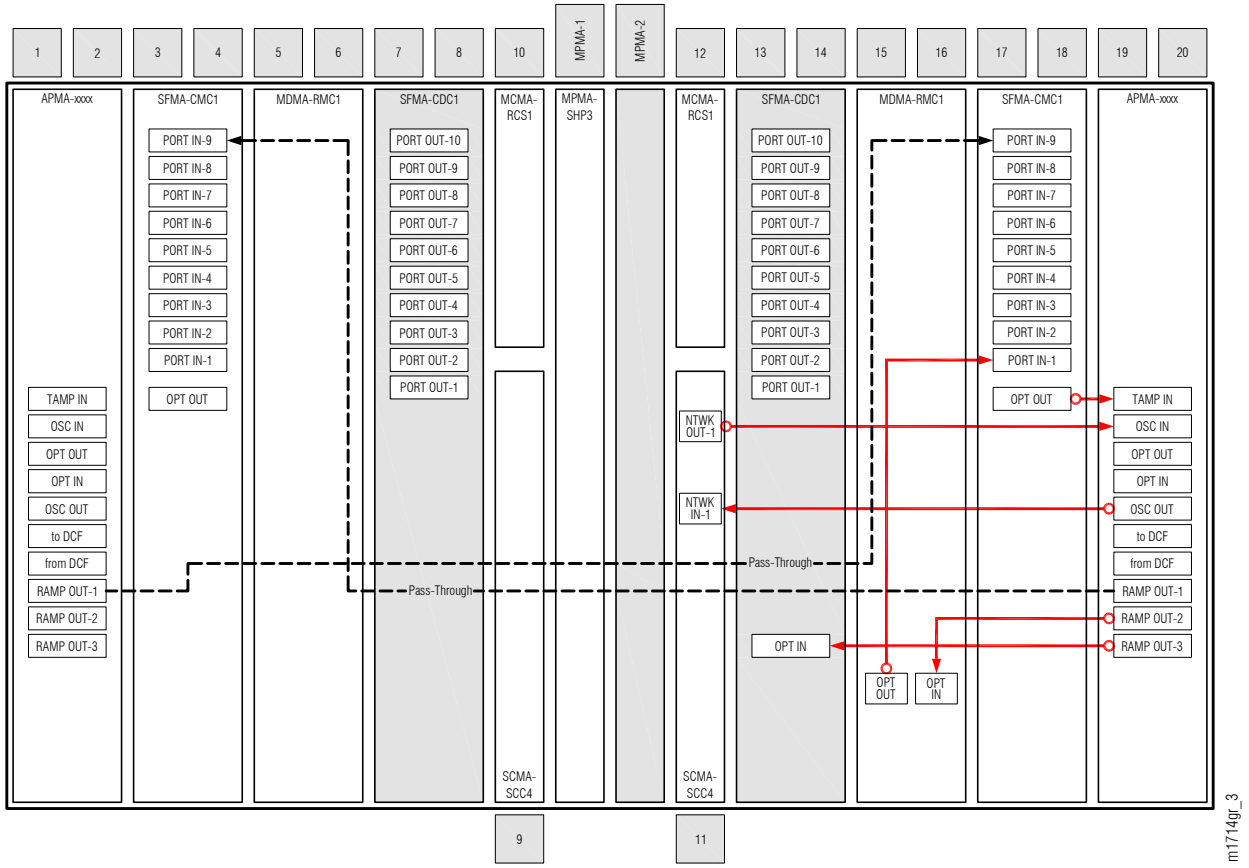


Figure 268: Fiber-Optic Cable Connections to the Amplifier at Node C (FLASHWAVE 7500 Core Configuration)

The following figure shows the cables installed at Node C.

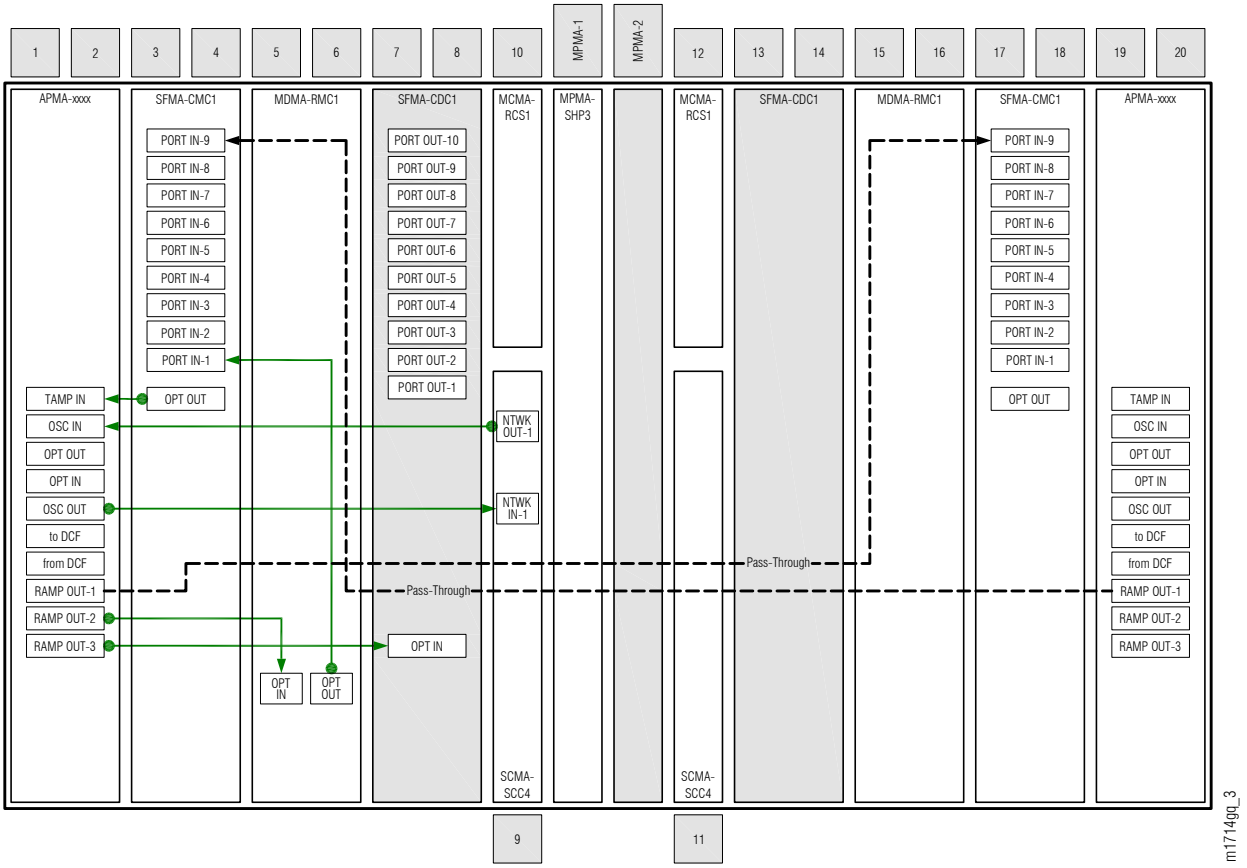


Figure 269: Fiber-Optic Cable Connections to the Amplifier at Node A(FLASHWAVE 7500 Core Configuration)

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

To connect Optical shelf plug-in units, perform the following steps:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Connect Amplifier and WSS Core Switch Unit

Step 1
Obtain and clean two LC-LC fiber-optic cables.

Step 2
Connect the cable ends to the connectors of the Amplifier (APMA-xxxx) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in Figure 268 or Figure 269, as applicable, and listed in Table 83.

Table 83: Amplifier to WSS Core Switch Unit Fiber-Optic Cable Connections (FLASHWAVE 7500 Core Configuration)

From Amplifier		To WSS Core Switch Unit	
Shelf Slot	Connector[59]	Shelf Slot	Connector
1	RAMP OUT-1	17	PORT IN-9
	TAMP IN/TAMP IN-1	3	OPT OUT
19	RAMP OUT-1	3	PORT IN-9
	TAMP IN/TAMP IN-1	17	OPT OUT

Connect Amplifier and Mux/Demux Unit

Step 3
Obtain and clean LC-LC fiber-optic cable.

Step 4
Connect the cable ends to the connectors of the Amplifier (APMA-xxxx) plug-in unit and Mux/Demux (MDMA-RMC1) plug-in unit as shown in Figure 268 or Figure 269, as applicable, and listed in Table 84.

Table 84: Amplifier to Mux/Demux Unit Fiber-Optic Cable Connections (FLASHWAVE 7500 Core Configuration)

From Amplifier		To Mux/Demux Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-2	5	OPT IN
19	RAMP OUT-2	15	OPT IN

[59] The connector on APMA-xxC1 amplifiers is labeled TAMP IN. The connector on APMA-xxU1 amplifiers is labeled TAMP IN-1.

Connect Amplifier and OSC Processing Unit

Step 5
Obtain and clean two LC-LC fiber-optic cables.

Step 6
Connect the cable ends to the connectors of the Amplifier (APMA-xxxx) plug-in unit and OSC Processing (SCMA-SCC4) plug-in unit as shown in Figure 268 or Figure 269, as applicable, and listed in Table 85.

Table 85: Amplifier to OSC Processing Unit Fiber-Optic Cable Connections(FLASHWAVE 7500 Core Configuration)

From Amplifier		To OSC Processing Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	OSC OUT	9	NTWK IN-1
	OSC IN		NTWK OUT-1
19	OSC OUT	11	NTWK IN-1
	OSC IN		NTWK OUT-1

Connect Mux/Demux Unit and WSS Core Switch Unit

Step 7
Obtain and clean LC-LC fiber-optic cable.

Step 8
Connect the cable ends to the connectors of the Mux/Demux unit (MDMA-RMC1) and wavelength selective switch (WSS) Core Switch unit (SFMA-CMC1) as shown in Figure 268 or Figure 269, as applicable, and listed in Table 86.

Table 86: Mux/Demux Unit to WSS Core Switch Unit Fiber-Optic Cable Connections(FLASHWAVE 7500 Core Configuration)

From Mux/Demux Unit		To WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
5	OPT OUT	3	PORT IN-1
15	OPT OUT	17	PORT IN-1

Step 9
Proceed to Connecting DCM.

✔ This procedure is complete.

7.7.2 Connecting DCM

The following figure shows the two fiber-optic cable connections between the Amplifier (APMA-xxxx) plug-in unit and dispersion compensation module (DCM) at Node A.

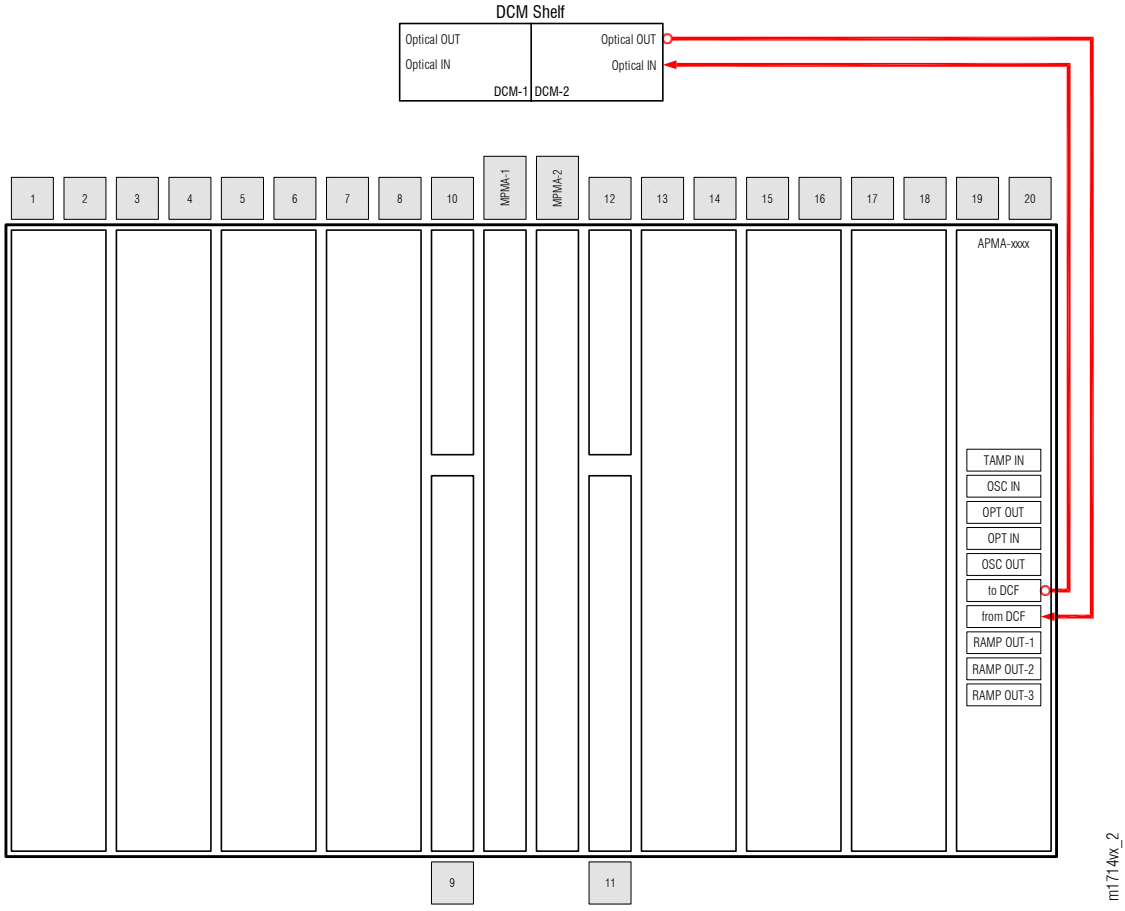


Figure 270: Fiber-Optic Cable Connections between Amplifier and DCM at Node C(FLASHWAVE 7500 Core Configuration)

The following figure shows the two fiber-optic cable connections between the Amplifier and DCM at Node C.

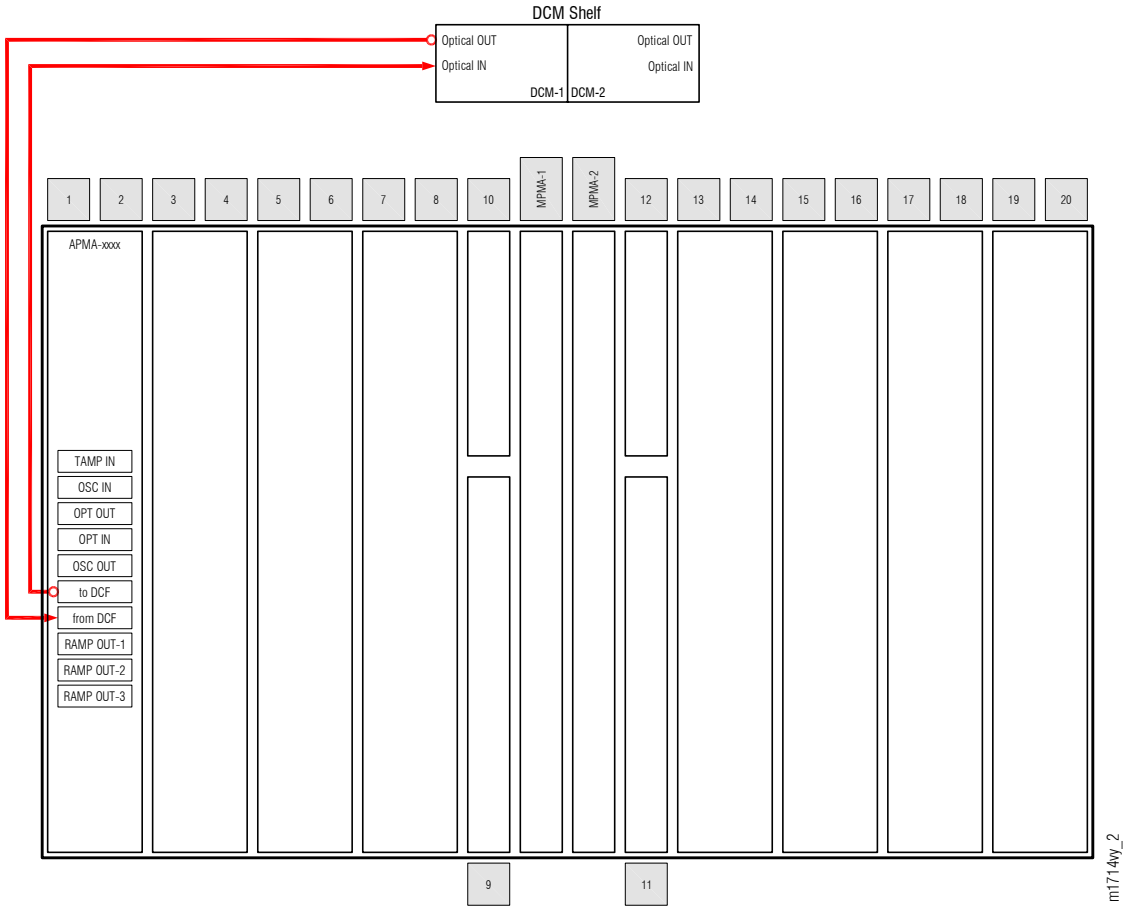


Figure 271: Fiber-Optic Cable Connections between Amplifier and DCM at Node A(FLASHWAVE 7500 Core Configuration)

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Step 1
Obtain and clean two LC-SC fiber-optic cables.

Note: *If no DCM is required, a jumper cable must be installed between the connectors of the amplifier.*

Step 2
Connect the cables to the connectors of the Amplifier (APMA-xxxx) plug-in unit and DCM as shown in Figure 270 or Figure 271, as applicable, and listed in Table 87.

Table 87: Amplifier to DCM Fiber-Optic Cable Connections (FLASHWAVE 7500 Core Configuration)

From Amplifier		To DCM[60]	
Shelf Slot	Connector	Shelf Slot	Connector
1	to DCF	DCM-1	OPT In
1	from DCF	DCM-1	OPT Out
19	to DCF	DCM-2	OPT In
19	from DCF	DCM-2	OPT Out

Step 3

Update inventory information for the DCM modules, as required.

TL1	NETSMART 500

`ED-DCM:TID:AID:CTAG:::`
`KEYWORD=DOMAIN;`
AID:
• OS1-1, OS1-19
KEYWORD=DOMAIN:
• Refer to Table 88.
Example:
`ED-DCM:FUJITSU:OS1-1:CTAG:::`
`DCM1VENDID=FC9682F220-01,`
`DCM1SERIALNO=1234567,`
`DCM3DOM=07-07,`
`DCM3CLEI=ABCD123456,`
`DCM3USI=ABCDEFGH12345678MNOPQRST;`
	In the tree view, select the Equipment tab.
	Expand the appropriate Optical shelf.
	Select amplifier unit in slot 1.
	Entity ▸ *Operations Dialog*
	The Operations dialog box opens.
	Click the DCM tab.
	In the Command Parameters area, enter the DCM inventory information, per your local practice.
	Click Modify.
	Do not close the Operations dialog box.

Table 88: ED-DCM Keyword and Domain Input Parameters

Keyword	Domain	Description
DCMxVENDID (x=1…3)	FCnnnnnnnn-mm	DCM vendor ID, where FCnnnnnnnn is the 10-character FC code and mm is the 2-character hardware revision number (13-character string) ***Example:*** `FC9682F220-01`
DCMxSERIALNO (x=1…3)	nnnnnnn	DCM equipment unit serial number (up to a 7-character string)
DCMxDOM (x=1…3)	yy.mm	DCM date of manufacture, where yy = last two digits of the year and mm = 01…12 (5-character string)

[60] **DCMs are housed in the SFD3 dispersion compensation shelf (FC9512SFD3).**

Table 88: ED-DCM Keyword and Domain Input Parameters (Cont.)

Keyword	Domain	Description
DCMxCLEI (x=1...3)	nnnnnnnnnn	COMMON LANGUAGE® Equipment Identifier (CLEI™) (10-character string) ***Note:*** *The CLEI must be a 10-character string.* ***Note:*** *CLEI attribute is associated with the shelf and provides inventory information about the plug-in unit.*
DCMxUSI(x=1...3)	nnnnnnnnnnnnnnnnnnnnnnnnn	DCM unique serial identifier (USI) (25-character string)

Step 4
Verify the DCM inventory information.

TL1	NETSMART 500

`RTRV-DCM:TID:AID:CTAG;`
AID:
• As identified in previous step
• **ALL** (null)
Example:
`RTRV-DCM:FUJITSU:OS1-1:CTAG;`
	Verify that the values shown in the Current Values area of the Operations dialog are correct.
	Close the Operations dialog box.

Step 5
Proceed to Prepare Linear Network to Convert to Ring Network.

7.8 Prepare Linear Network to Convert to Ring Network

Perform the following steps to prepare to convert the linear network:

Step 1
If not already done, log on the node. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[61]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 2
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Connect Optical Fibers.

[61] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Connect Optical Fibers.

7.9 Connect Optical Fibers

The following figure shows the two fiber-optic cable connections between the Amplifier (APMA-xxxx) plug-in unit at Node A and the Amplifier plug-in unit at Node C.

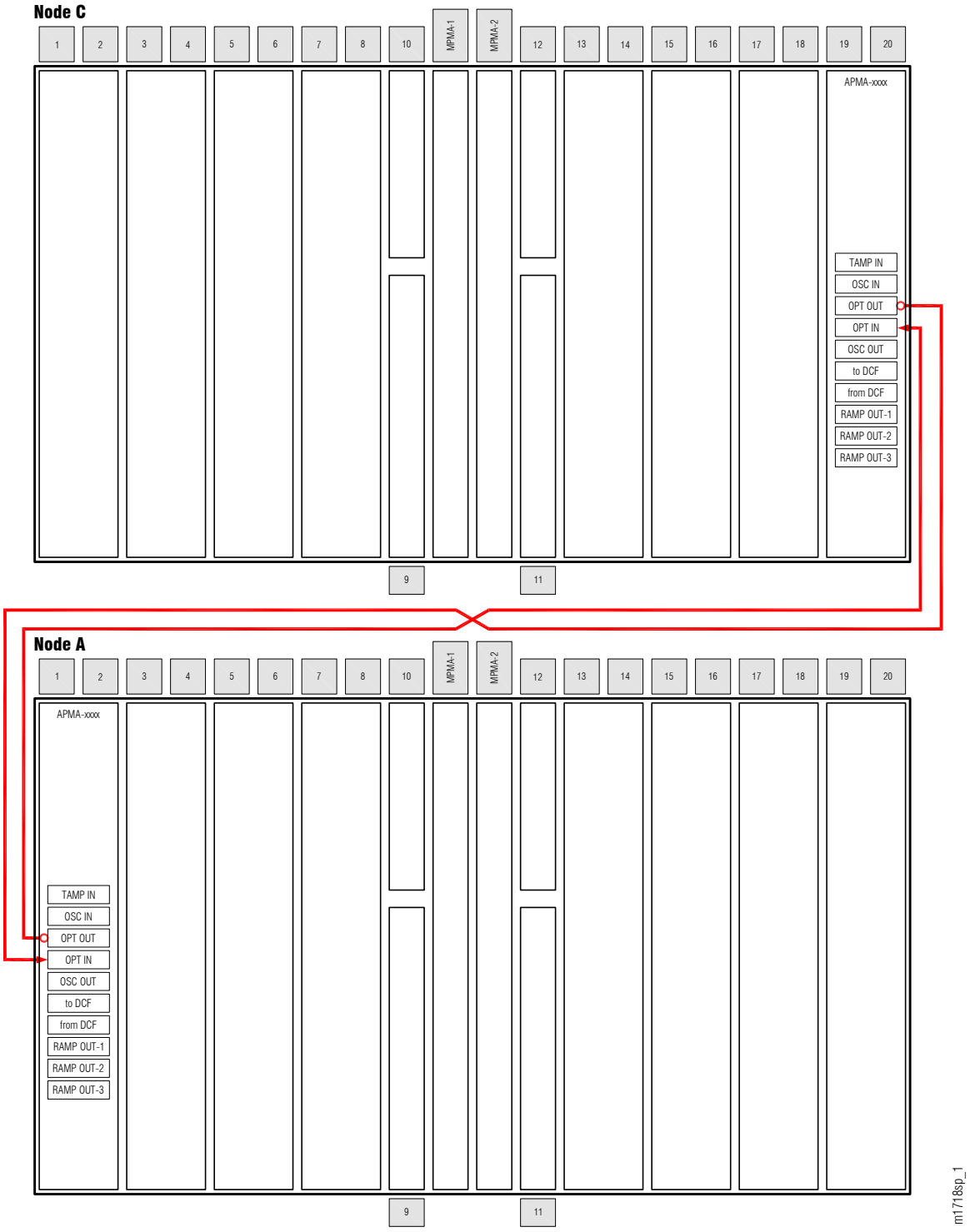


Figure 272: Optical Fiber Connections between Nodes A and C(FLASHWAVE 7500 Core Configuration)

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Step 1
Identify and clean both ends of the two network fiber-optic cables associated with the span (see Figure 272).

Note: *This procedure assumes that both fiber-optic cables include all attenuators required by the network engineering design specification.*

Step 2
Connect the cable ends to the appropriate amplifiers and connectors.

The NOT READY indicators on the amplifier light and then go out after approximately 5 minutes. After the NOT READY indicators go out, the FAIL/SVCE indicators light green on the amplifiers.

Step 3
After the NOT READY indicators go out and the FAIL/SVCE indicators light green, proceed to the next step.

Step 4
Repeat Steps 1 through 3 for each span in the network.

Step 5
Proceed to Establish Ring Network.

7.10
Establish Ring Network

Perform the following steps to verify that the ring network is free of alarms and conditions and return the ring network to normal operation (see Figure 266):

Step 1
If not already done, log on Nodes A, B, C, and D (refer to Step 1 of Prepare Linear Network to Convert to Ring Network. If already logged on, proceed to the next step.

Step 2
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 6.

Note: *Refer to Responding to Alarms and Conditions, for information on clearing alarms and conditions.*

If NO:
Proceed to Step 6.

Step 4
Using the procedure in Reset the Span Loss Variation Alarm References, reset the span loss variation value for each amplifier.

Step 5
Proceed to Step 6.

Step 6
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

The linear network has been converted to a ring network and is ready for optical channel dedicated protection ring (OCh-DPRING)–protected services to be provisioned on it.

Step 7
To add services, refer to Service Addition.

Step 8
To perform acceptance testing, refer to Acceptance Testing.

This procedure is complete.

8
Upgrading Nodes, Core Configuration

In this chapter:

8.1 Node Upgrade Paths and Restrictions Core Configuration

This chapter provides procedures for upgrading a node within a FLASHWAVE® 7500 Core Configuration network.

In Release 5.1, two amplifier units (APMA-M2U1 and APMA-ULU1) were introduced that allow for in-service upgrades of ILA nodes that have the amplifiers installed. Refer to APMA-xxU1 (Universal Amplifier Unit), for complete details on the APMA-xxU1 amplifiers.

In-service upgrades cannot be performed on ILA nodes that have APMA-xxC1 amplifiers installed. For detailed information on the different node applications, refer to Applications.

The following table shows the upgrade paths to follow when performing node upgrades.

Table 89: Node Upgrade Paths

To Upgrade		Related Procedure
From	To	***Note:*** *Be sure to follow the listed sequence for the procedure.*
Upgrade Path for Nodes with APMA-xxU1 Universal Amplifier Units		
ILA Node(in-service upgrade)	Express Node	In-Service Upgrade ILA Node to Express Node
	ROADM Node	In-Service Upgrade ILA Node to ROADM Node
	2D-ROADM Node	In-Service Upgrade ILA Node to 2D-ROADM Node
	HUB Node	In-Service Upgrade ILA Node to ROADM Node Upgrade ROADM Node to HUB Node
Express Node	ROADM Node	In-Service Upgrade Express Node to ROADM Node
	HUB Node	In-Service Upgrade Express Node to ROADM Node Upgrade ROADM Node to HUB Node
ROADM Node	HUB Node	Upgrade ROADM Node to HUB Node
Upgrade Path for Nodes with APMA-xxC1 Amplifier Units		
ILA Node (not an in-service upgrade)	Express Node	Upgrade ILA Node to Express Node
	ROADM Node	Upgrade ILA Node to Express Node In-Service Upgrade Express Node to ROADM Node
	2D-ROADM Node	Upgrade ILA Node to 2D-ROADM Node
	HUB Node	Upgrade ILA Node to Express Node In-Service Upgrade Express Node to ROADM Node Upgrade ROADM Node to HUB Node
Express Node	ROADM Node	In-Service Upgrade Express Node to ROADM Node

Upgrade Path for Nodes with APMA-xxC1 Amplifier Units		
	HUB Node	In-Service Upgrade Express Node to ROADM Node Upgrade ROADM Node to HUB Node
ROADM Node	HUB Node	Upgrade ROADM Node to HUB Node
Symmetric HUB	Asymmetric HUB	Convert a Symmetric HUB Node to an Asymmetric HUB Node

8.2
References

Throughout this chapter, some procedures refer to other documents for more detailed instructions. Be sure to review and follow the referenced procedures within these documents when applicable:

- Introduction to Equipment Installation
- Introduction to System Turn-Up Core Configuration
- Introduction to System Operations General
- Introduction to TL1 Commands
- Introduction to Maintenance and Trouble Clearing
- *NETSMART 500 User Guide*

8.3
In-Service Upgrade ILA Node to Express Node

In this section:

This procedure describes how to perform an in-service upgrade of an ILA node to an Express node. The ILA node must be operating on Release 5.1 (or later) software, and the amplifiers must be APMA-xxU1 Universal Amplifier units.

A flowchart of the overall process is shown in the following figure.

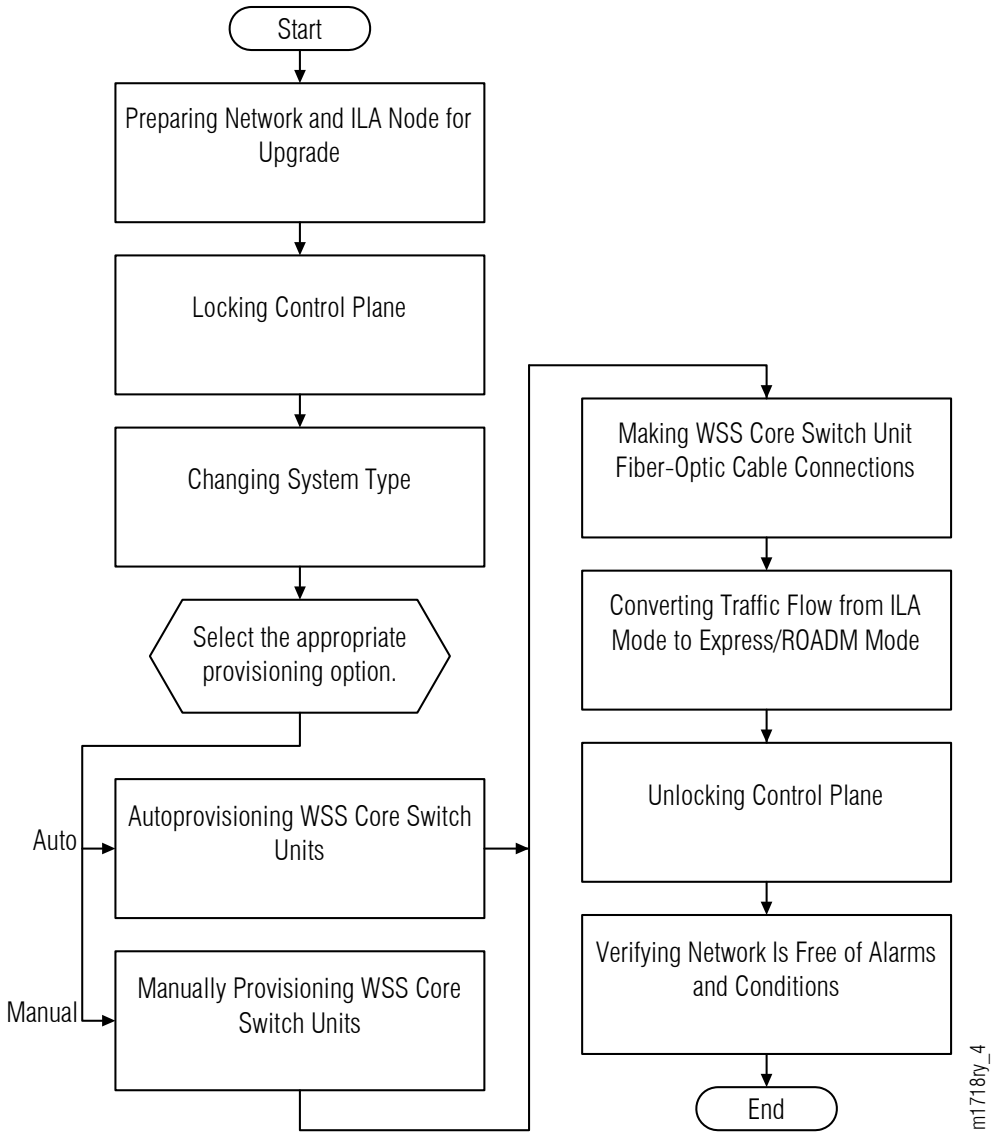


Figure 273: Upgrading ILA Node to Express Node–In-Service (Procedure Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

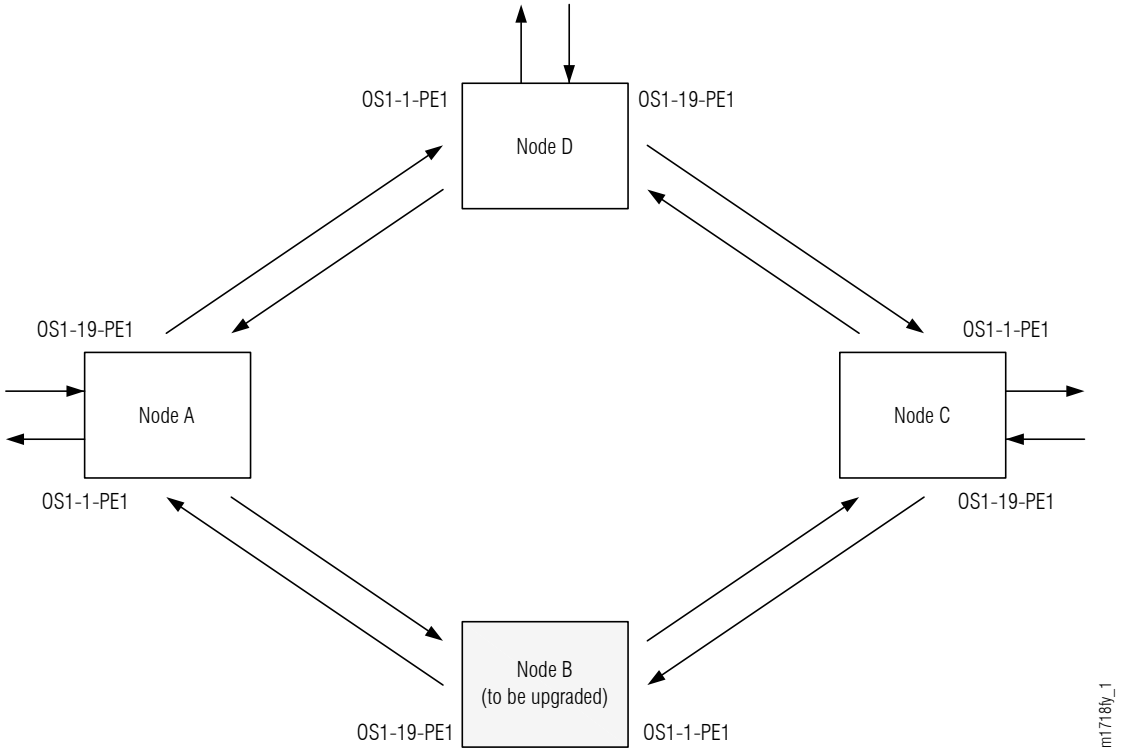


Figure 274: Ring Network Configuration

The procedure can also be used to upgrade linear networks as shown in the following figure.

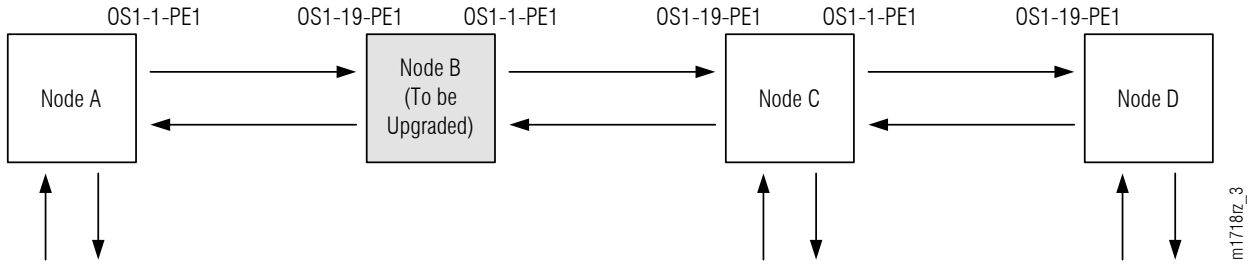


Figure 275: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART® 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.3.1
Preparing Network and ILA Node for Upgrade

Prepare the ILA node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[62]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[62] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

The correct GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 2.

Verify Amplifier Type

Step 6
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 7
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to Express Node, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

Clear Alarms and Conditions on Network

Step 8
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 9
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 10
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 11
Is the active GISSUE correct?

The correct GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 2.

Verify Amplifier Type

Step 12
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 13
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to Express Node, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

✔ This procedure is complete.

8.3.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the value for LOCK is Yes.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

8.3.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	The Confirmation dialog box opens.
	Click Yes.
	The Warning dialog box opens.
	Click Logon.

Note: *Any pass-through traffic is still being carried through the amplifier-to-amplifier connections. The traffic routing does not change until the OPR-MODE command is sent in* Converting Traffic Flow from ILA Mode to Express/ROADM Mode .

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	Click Yes in the pop-up window to continue.
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 of Preparing Network and ILA Node for Upgrade).

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in unit should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the TYPE is FW7500U_OADM.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning WSS Core Switch Units.
- For manual provisioning, proceed to Manually Provisioning WSS Core Switch Units.

8.3.4
Autoprovisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the WSS Core Switch units (SFMA-CMC1) in shelf OS1 of Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

8.3.5
Manually Provisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the WSS Core Switch units (SFMA-CMC1) in shelf OS1 of Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

8.3.6
Making WSS Core Switch Unit Fiber-Optic Cable Connections

Use this procedure to make fiber-optic cable connections between the amplifier units and the WSS Core Switch units.

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections for the ILA node before WSS core switch unit installation and cabling.

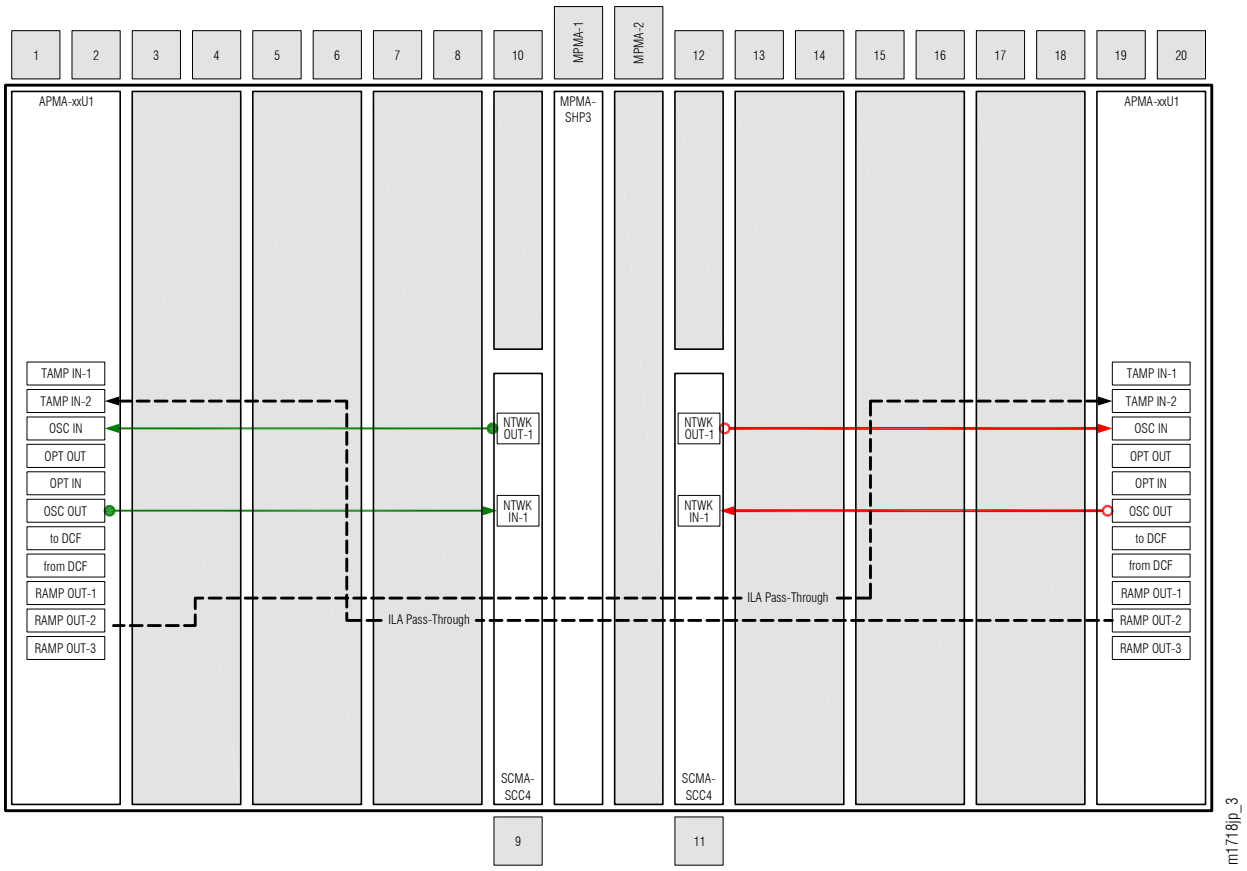


Figure 276: ILA Node Cabling Before WSS Core Switch Unit Installation and Cabling

The following figure shows the fiber-optic cable connections after the WSS Core Switch units are installed and cabled.

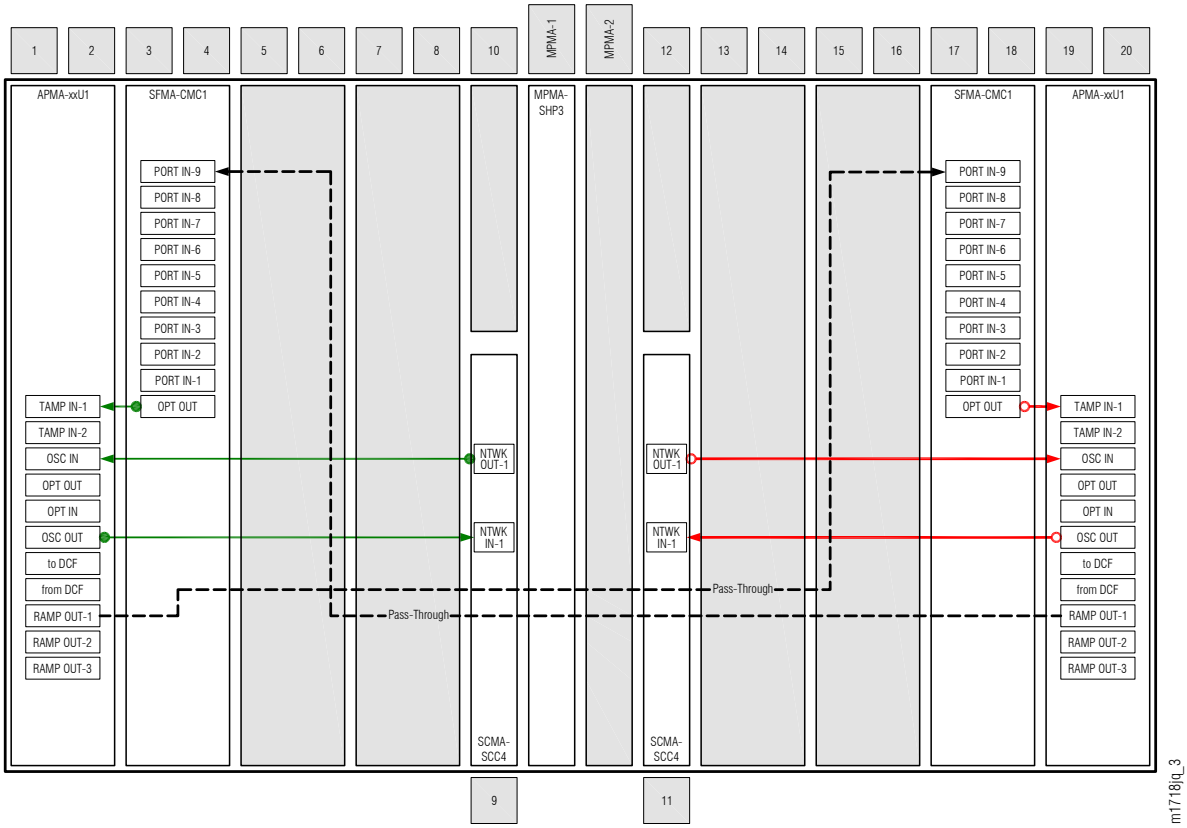


Figure 277: ILA Node Cabling After WSS Core Switch Unit Installation and Cabling

Caution: *To avoid a disruption in traffic, do not remove the cables between TAMP IN-2 and RAMP OUT-2 (PC2 and PC6 on both units) until the procedure in* Converting Traffic Flow from ILA Mode to Express/ROADM Mode *, is completed.*

Make fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 2
Connect the cables to the connectors of the amplifier (APMA-xxU1) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in the preceding figure and listed in the following table.

Table 90: Amplifier Unit and WSS Core Switch Unit Fiber-Optic Cable Connections

Amplifier Unit		WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-1	3	OPT OUT
	RAMP OUT-1	17	PORT IN-9
19	TAMP IN-1	17	OPT OUT
	RAMP OUT-1	3	PORT IN-9

Step 3
Proceed to Converting Traffic Flow from ILA Mode to Express/ROADM Mode .

8.3.7 Converting Traffic Flow from ILA Mode to Express/ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the Express mode (traffic flows through WSS Core Switch units). This procedure affects the switch in traffic flow in less than 50 milliseconds. Additionally, this procedure allows you to perform required validations before completing the in-service traffic switch.

There are three modes of operation for this procedure:

- Test mode (MODE=TEST)—Performs the required tests/validations (refer to the following table). A transient condition is reported based on the test result:
  - OPR-MODECOMPLD—Successful test/validation
  - OPR-MODE-FAIL—Unsuccessful test/validation
- Automatic mode (MODE=AUTO)—Performs the required tests/validations (refer to the following table), and then switches the system mode to OADM if all tests/validations are completed successfully. If any test/validation fails, the OPR-MODE-FAIL transient condition is reported with the cause of the failure.
- Override mode (MODE=OVRD)—Switches the system mode to OADM without performing any tests/validations. The override mode is ideal when the system does not have any traffic.

Caution: *Forced switching (MODE=OVRD) of the operation modes can result in traffic hits. If the node has pass-through traffic, Fujitsu recommends that the test mode or automatic mode of operation be used.*

Note: *The automatic mode of conversion is used in this procedure.*

The following table provides a detailed list of the tests and validations performed by the system when the test mode or automatic mode is used when converting operation modes. The tests and validations are listed in the order in which they are performed.

Table 91: Test Mode and Automatic mode System Tests and Validations

System Test/Validation	Description
System alarms	The system monitors the following alarms during the in-service conversion test mode: • Common unit failures–FLT, RMVD, MEA, WARMUP, FVM • Amplifier units–MLSPRE, MLSPOST, ALSPRE, ALSPOST, LDONPRE, LDONPOST, SAPPRE, and SAPPOST • Amplifiers ports–INDWN on PC1and PC6, POS (high and low) on PC1, POS (high and low) on PC2 • WSS CORE Switch unit–INDWN on PC9 and LOL • WDM facility–LOS, PMI, BDIO • OSC facility–BERSF, BERSD, LOS, LOF, MISCON, CNTFAIL, DCCFAIL, TIM-S, INTROPF, LNR • WCH facility–UNEQ-O /AIS-O, NOLIGHT ***Note:*** *The system monitors the alarms throughout the test mode.*
PM validity check	The system performs the following PM validity checks during the in-service conversion test mode: • APMA-M2U1 unit–OPT on PC1 and PC3, OPR on PE2 • APMA-ULU1 unit–OPR on P1
Optical power level measurements	The system checks that the following optical power level measurements are within specified values: • Amplifier RAMP OUT-1 output port (PC1) and WSS Core Switch unit PORT IN-9 input port (PC9) • WSS Core Switch unit OPT OUT output port (PE1) and amplifier TAMP IN-1 input port (PC1)
Optical test pattern	The system performs optical test patterns to validate the signal flow of the active pass-through traffic between the amplifier (PC1) and the WSS Core Switch port (PE1). ***Note:*** *The testing is done by turning the WSS Core Switch unit VATT on and off for applicable channels.*

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=AUTO;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=AUTO;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select AUTO from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

The ILA-to-Express conversion process begins with the system automatically creating pass-through cross-connects for any existing ILA pass-through traffic. The system then goes into the test and validation mode and performs the actions listed in Table 91. The CONVIP condition is generated during the conversion process and clears when the conversion completes or terminates.

Note: *If the operation terminates because of the failure of any of the test or validation checks or alarms, the OPR-MODE-FAIL standing condition, containing the cause of the failure, is raised. Refer to Responding to Alarms and Conditions for information on clearing alarms. To perform the conversion regardless of alarms, use MODE=OVRD.*

When the conversion process successfully completes, the OPR-MODE-COMPLD transient condition is raised, and the direct connections between the amplifiers (PC2 and PC6 on both units) are automatically deleted.

Step 3
Remove the two ILA pass-through cables listed in the following table.

Table 92: Pass-Through Cable Connections between Amplifier Units

Amplifier Unit		Amplifier Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-2	19	RAMP OUT-2
1	RAMP OUT-2	19	TAMP IN-2

Step 4
Continue to Unlocking Control Plane.

8.3.8 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Verifying Network Is Free of Alarms and Conditions.

8.3.9
Verifying Network Is Free of Alarms and Conditions

Step 1
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	
	Click Yes to continue.

This procedure is complete.

8.4
In-Service Upgrade ILA Node to ROADM Node

In this section:

This procedure describes how to perform an in-service upgrade of an ILA node to a ROADM node. The ILA node must be operating on Release 5.1 (or later) software, and the amplifiers must be APMA-xxU1 Universal Amplifier units.

A flowchart of the overall process is shown in the following figure.

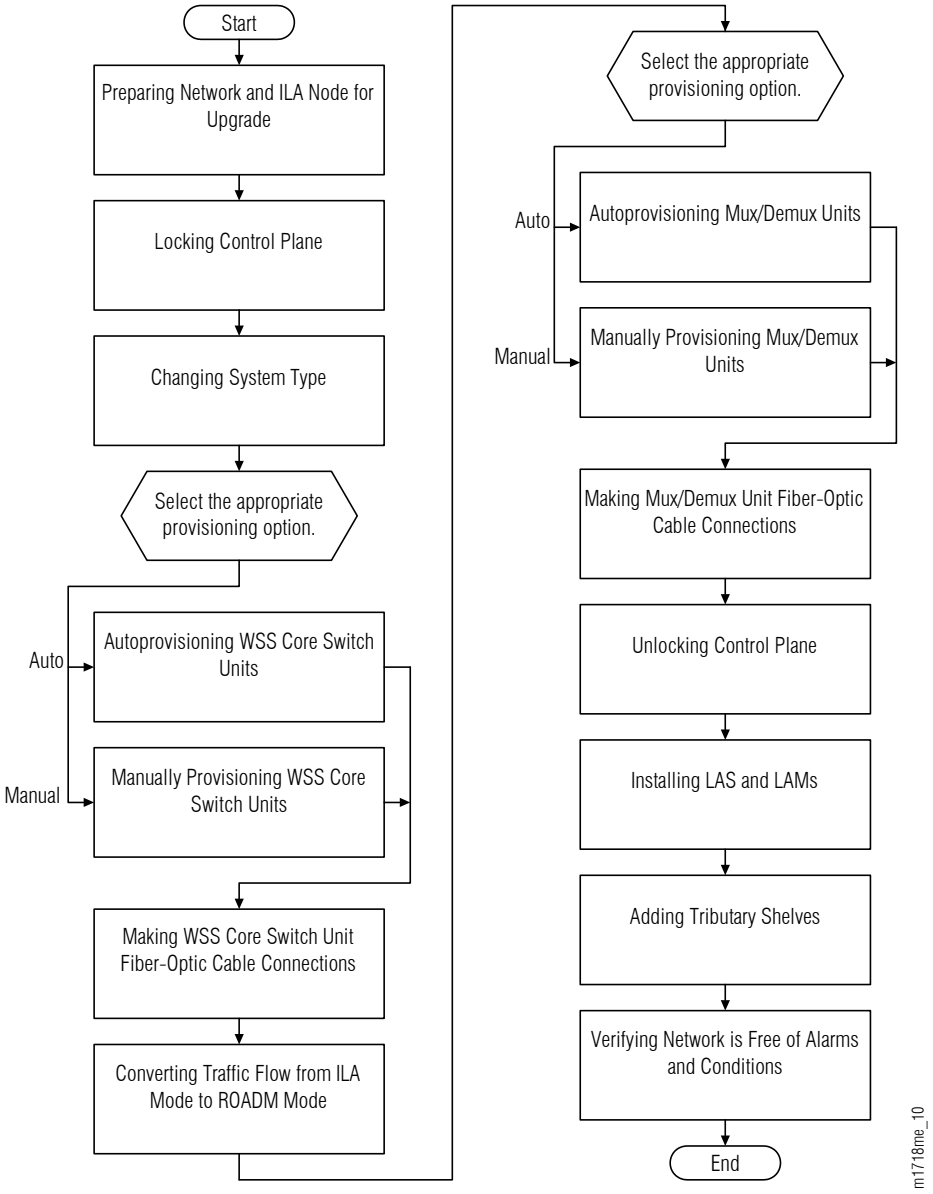


Figure 278: Upgrading ILA Node to ROADM Node–In-Service (Procedure Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

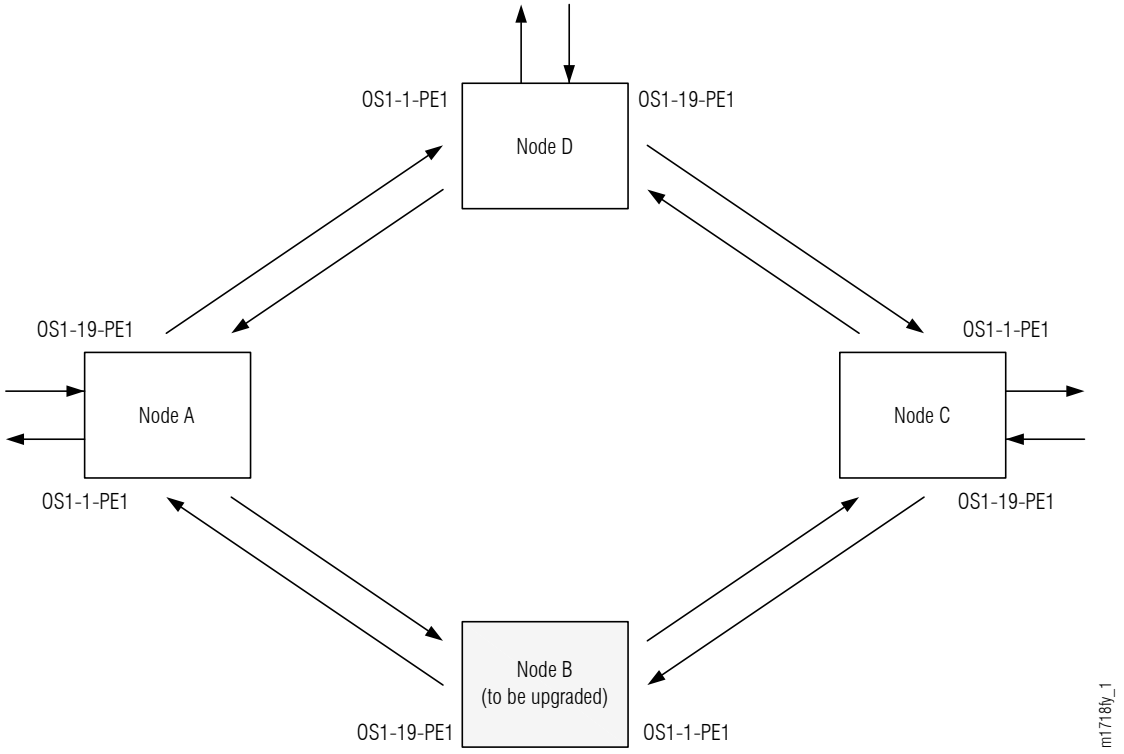


Figure 279: Ring Network Configuration

This procedure can also be used to upgrade linear networks as shown in the following figure.

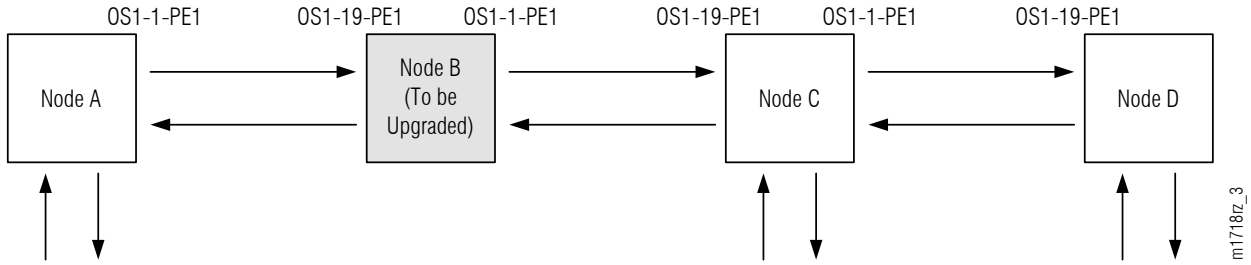


Figure 280: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.4.1
Preparing Network and ILA Node for Upgrade

Prepare the ILA node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[63]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[63] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

The correct GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 2.

Verify Amplifier Type

Step 6
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 7
Are the amplifiers of the correct type?

If YES:
Proceed to Step 8.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to Express Node, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

Step 8
Proceed to Locking Control Plane.

Clear Alarms and Conditions on Network

Step 9
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 10
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 11
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 12
Is the active GISSUE correct?

The correct GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 2.

Verify Amplifier Type

Step 13
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 14
Are the amplifiers of the correct type?

If YES:
Proceed to Step 15.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to Express Node, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

Step 15
Proceed to Locking Control Plane.

✔ This procedure is complete.

8.4.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the value for LOCK is Yes.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

8.4.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	The Confirmation dialog box opens.
	Click Yes.
	The Warning dialog box opens.
	Wait approximately 5 to 20 minutes for the system to restart.
	Click Logon.

Note: *Any pass-through traffic is still being carried through the amplifier-to-amplifier connections. The traffic routing does not change until the OPR-MODE command is sent in* Converting Traffic Flow from ILA Mode to ROADM Mode .

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	Click Yes in the pop-up window to continue.
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 of Preparing Network and ILA Node for Upgrade).

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the TYPE is FW7500U_OADM.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning WSS Core Switch Units.
- For manual provisioning, proceed to Manually Provisioning WSS Core Switch Units.

8.4.4 Autoprovisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the WSS Core Switch units (SFMA-CMC1) in shelf OS1 of Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

8.4.5 Manually Provisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the WSS Core Switch units (SFMA-CMC1) in shelf OS1 of Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

8.4.6 Making WSS Core Switch Unit Fiber-Optic Cable Connections

Use this procedure to make fiber-optic cable connections between the amplifier units and the WSS Core Switch units.

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections for the ILA node before WSS core switch unit installation and cabling.

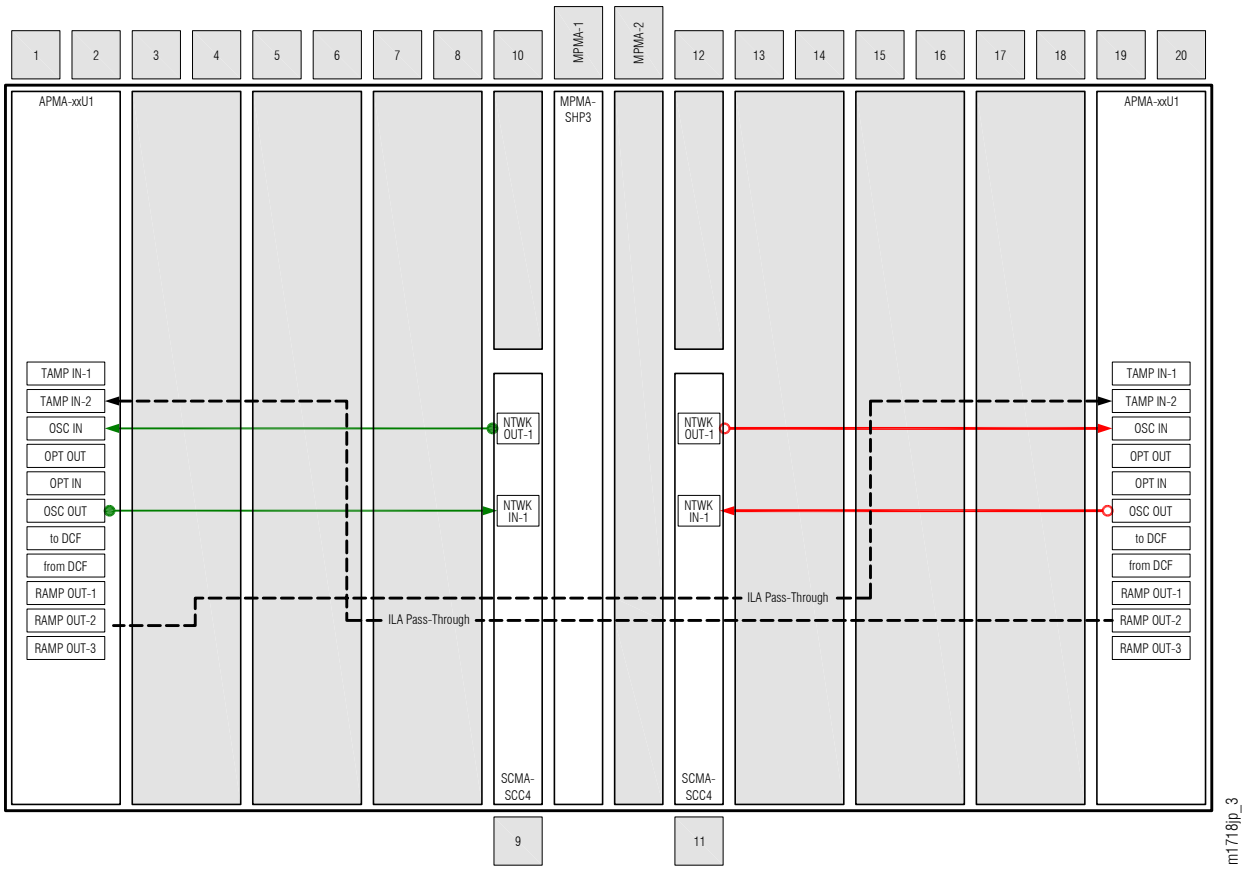


Figure 281: ILA Node Cabling Before WSS Core Switch Unit Installation and Cabling

The following figure shows the fiber-optic cable connections after the ILA cables are removed and the WSS Core Switch units are installed and cabled.

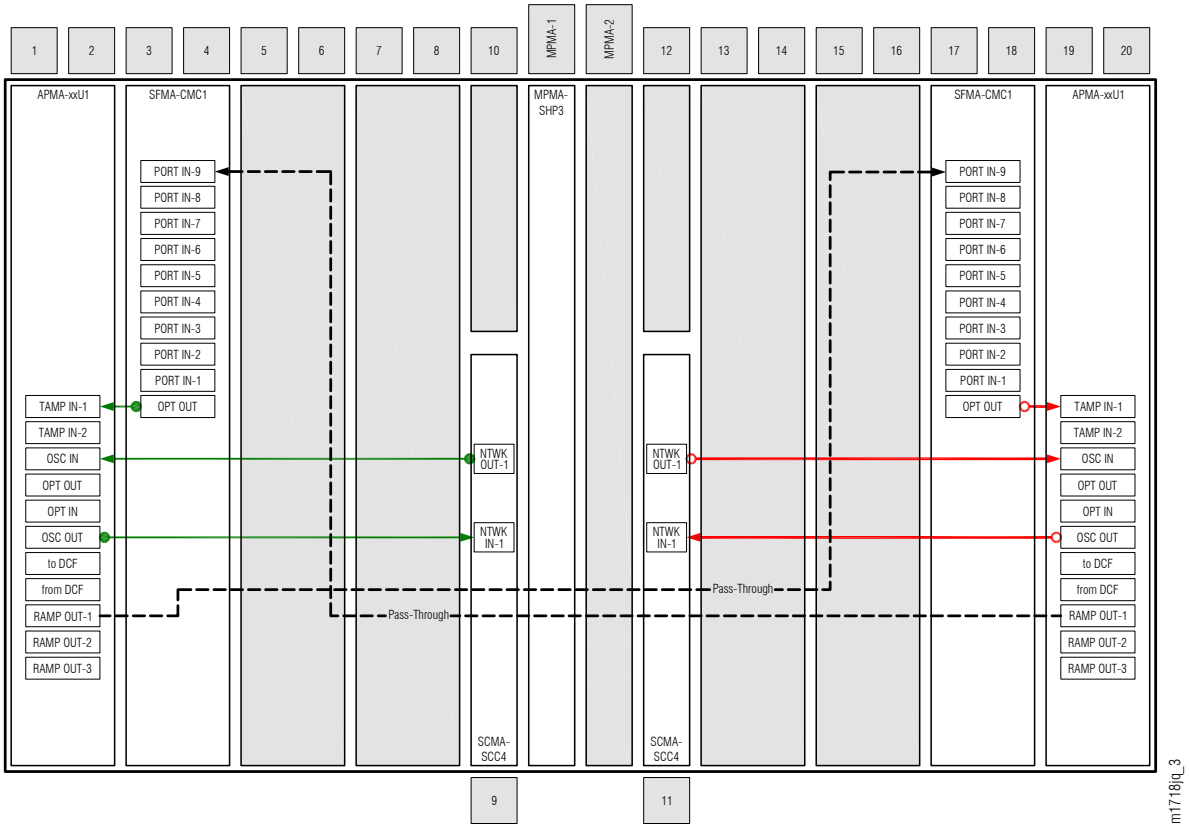


Figure 282: ILA Node Cabling After WSS Core Switch Unit Installation and Cabling

Caution: *To avoid a disruption in traffic, do not remove the cables between TAMP IN-2 and RAMP OUT-2 (PC2 and PC6 on both units) until the procedure in* Converting Traffic Flow from ILA Mode to ROADM Mode, *is completed.*

Make fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 2
Connect the cables to the connectors of the amplifier (APMA-xxU1) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in the preceding figure and listed in the following table.

Table 93: Amplifier Unit and WSS Core Switch Unit Fiber-Optic Cable Connections

Amplifier Unit		WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-1	3	OPT OUT
	RAMP OUT-1	17	PORT IN-9
19	TAMP IN-1	17	OPT OUT
	RAMP OUT-1	3	PORT IN-9

Step 3
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode .

8.4.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through WSS Core Switch units). This procedure affects the switch in traffic flow in less than 50 milliseconds. Additionally, this procedure allows you to perform required validations before completing the in-service traffic switch.

There are three modes of operation for this procedure:

- Test mode (MODE=TEST)—Performs the required tests/validations (refer to the following table). A transient condition is reported based on the test result:
  - OPR-MODECOMPLD—Successful test/validation
  - OPR-MODE-FAIL—Unsuccessful test/validation
- Automatic mode (MODE=AUTO)—Performs the required tests/validations (refer to the following table) and then switches the system mode to OADM if all tests/validations are completed successfully. If any test/validation fails, the OPR-MODE-FAIL transient condition is reported with the cause of the failure.
- Override mode (MODE=OVRD)—Switches the system mode to OADM without performing any tests/validations. The override mode is ideal when the system does not have any traffic.

Caution: *Forced switching (MODE=OVRD) of the operation modes can result in traffic hits. If the node has pass-through traffic, Fujitsu recommends that the test mode or automatic mode of operation be used.*

Note: *The automatic mode of conversion is used in this procedure.*

The following table provides a detailed list of the tests and validations performed by the system when the test mode or automatic mode is used when converting operation modes. The tests and validations are listed in the order in which they are performed.

Table 94: Test Mode and Automatic mode System Tests and Validations

System Test/Validation	Description
System Alarms	The system monitors the following alarms during the in-service conversion test mode: • Common unit failures–FLT, RMVD, MEA, WARMUP, FVM • Amplifier units–MLSPRE, MLSPOST, ALSPRE, ALSPOST, LDONPRE, LDONPOST, SAPPRE, and SAPPOST • Amplifiers ports–INDWN on PC1and PC6, POS (high and low) on PC1, POS (high and low) on PC2 • WSS CORE Switch unit–INDWN on PC9 and LOL • WDM facility–LOS, PMI, BDIO • OSC facility–BERSF, BERSD, LOS, LOF, MISCON, CNTFAIL, DCCFAIL, TIM-S, INTROPF, LNR • WCH facility–UNEQ-O /AIS-O, NOLIGHT ***Note:*** *The system monitors the alarms throughout the test mode.*
PM validity check	The system performs the following PM validity checks during the in-service conversion test mode: • APMA-M2U1 unit–OPT on PC1 and PC3, OPR on PE2 • APMA-ULU1 unit–OPR on P1
Optical power level measurements	The system checks that the following optical power level measurements are within specified values: • Amplifier RAMP OUT-1 output port (PC1) and WSS Core Switch unit PORT IN-9 input port (PC9) • WSS Core Switch unit OPT OUT output port (PE1) and amplifier TAMP IN-1 input port (PC1)
Optical test pattern	The system performs optical test patterns to validate the signal flow of the active pass through traffic between the amplifier (PC1) and the WSS Core Switch port (PE1). ***Note:*** *The testing is done by turning the WSS Core Switch unit VATT on and off for applicable channels.*

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=AUTO;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=AUTO;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select AUTO from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

The ILA-to-ROADM conversion process begins with the system automatically creating pass-through cross-connects for any existing ILA pass-through traffic. The system then goes into the test and validation mode and performs the actions listed in Table 94. The CONVIP condition is generated during the conversion process and clears when the conversion completes or terminates.

Note: *If the operation terminates because of the failure of any of the test or validation checks or alarms, the OPR-MODE-FAIL standing condition, containing the cause of the failure, is raised. Refer to Responding to Alarms and Conditions for information on clearing alarms. To perform the conversion regardless of alarms, use MODE=OVRD.*

When the conversion process successfully completes, the OPR-MODE-COMPLD transient condition is raised, and the direct connections between the amplifiers (PC2 and PC6 on both units) are automatically deleted.

Step 3
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning Mux/Demux Units.
- For manual provisioning, proceed to Manually Provisioning Mux/Demux Units.

8.4.8 Autoprovisioning Mux/Demux Units

The Mux/Demux units (MDMA-RMC1) can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the Mux/Demux (MDMA-RMC1) units in shelf OS1 of Node B

Step 2
Proceed to Making Mux/Demux Unit Fiber-Optic Cable Connections.

8.4.9
Manually Provisioning Mux/Demux Units

The Mux/Demux units (MDMA-RMC1) can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in to Manually Provision Optical Shelf Equipment, install and manually provision the Mux/Demux (MDMA-RMC1) units in shelf OS1 of Node B.

Step 2
Proceed to Making Mux/Demux Unit Fiber-Optic Cable Connections.

8.4.10
Making Mux/Demux Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the cables after the ILA pass-through connections are removed and the DMUX IN cables are installed.

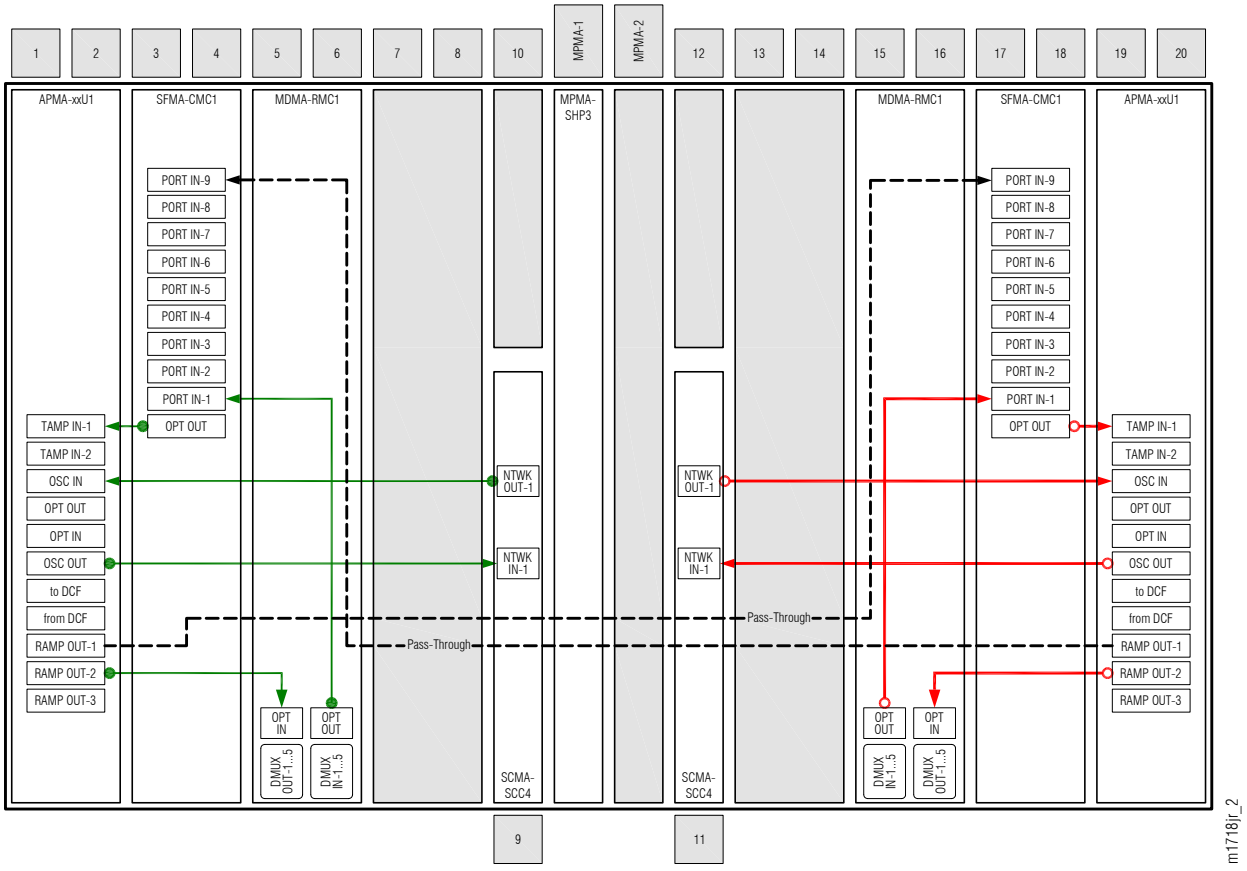


Figure 283: Fiber-Optic Cable Connections between Optical Shelf Plug-In Units

To install internal fiber-optic cables, perform the following steps:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Connect Amplifier Units and Mux/Demux Units

The ILA pass-through connections (see Figure 282) are no longer needed. The following steps guide you through disconnecting the TAMP IN-2 end of the pass-through connections on the amplifiers and making connections to the Mux/Demux units.

Step 1
Disconnect the fiber-optic cable from connector TAMP IN-2 of the Amplifier plug-in unit located in slot 19.

Step 2
Reconnect this cable end to connector OPT IN of the MDMA-RMC1 Mux/Demux plug-in unit located in slot 5 as shown in Figure 283 and listed in the following table.

Step 3
Disconnect the fiber-optic cable from connectors TAMP IN-2 of the Amplifier plug-in unit located in slot 1.

Step 4
Reconnect this cable end to connector OPT IN of the MDMA-RMC1 Mux/Demux plug-in unit located in slot 15 as shown in Figure 283 and listed in the following table.

Table 95: Amplifier and Mux/Demux Unit Fiber-Optic Cable Connections

Amplifier		Mux/Demux Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-2	5	OPT IN
19	RAMP OUT-2	15	OPT IN

Connect Mux/Demux Unit and WSS Core Switch Unit

Step 5
Obtain two LC-LC fiber-optic cables, and clean the connectors.

Step 6
Connect the cables to the connectors of the Mux/Demux (MDMA-RMC1) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in Figure 283 and listed in the following table.

Table 96: Mux/Demux Unit and WSS Core Switch Unit Fiber-Optic Cable Connections

Mux/Demux Unit		WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
5	OPT OUT	3	PORT IN-1
15	OPT OUT	17	PORT IN-1

Step 7
Proceed to Unlocking Control Plane.

✔ This procedure is complete.

8.4.11 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Installing LAS and LAMs.

8.4.12 Installing LAS and LAMs

After completing the subprocedures in Preparing Network and ILA Node for Upgrade through Unlocking Control Plane, refer to Table 97, for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 97: Install LAS and LAMs

Task	Practice and Section
Install LAS shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

8.4.13 Adding Tributary Shelves

Use the following procedure to add Tributary shelves.

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 98: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors

Table 98: Adding Tributary Shelf (Cont.)

Task	Practice and Section
Provision synchronization and/or Tributary shelf OSC units, if required.[64]	Provision Synchronization and/or Tributary Shelf OSC Units

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

8.4.14 Verifying Network Is Free of Alarms and Conditions

Step 1
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

[64] Refer to procedure for applicability.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

8.5
In-Service Upgrade ILA Node to 2D-ROADM Node

In this section:

This procedure describes how to perform an in-service upgrade of an ILA node to a 2D-ROADM node. The ILA node must be operating on Release 5.1 (or later) software, and the amplifiers must be APMA-xxU1 Universal Amplifier units.

Note: *If the ILA node is using a release earlier than Release 5.1 and/or amplifiers other than APMA-xxU1, follow the procedure in* Upgrade ILA Node to 2D-ROADM Node*, to perform protection switching to prevent an interruption in service.*

A flowchart of the overall process is shown in the following figure.

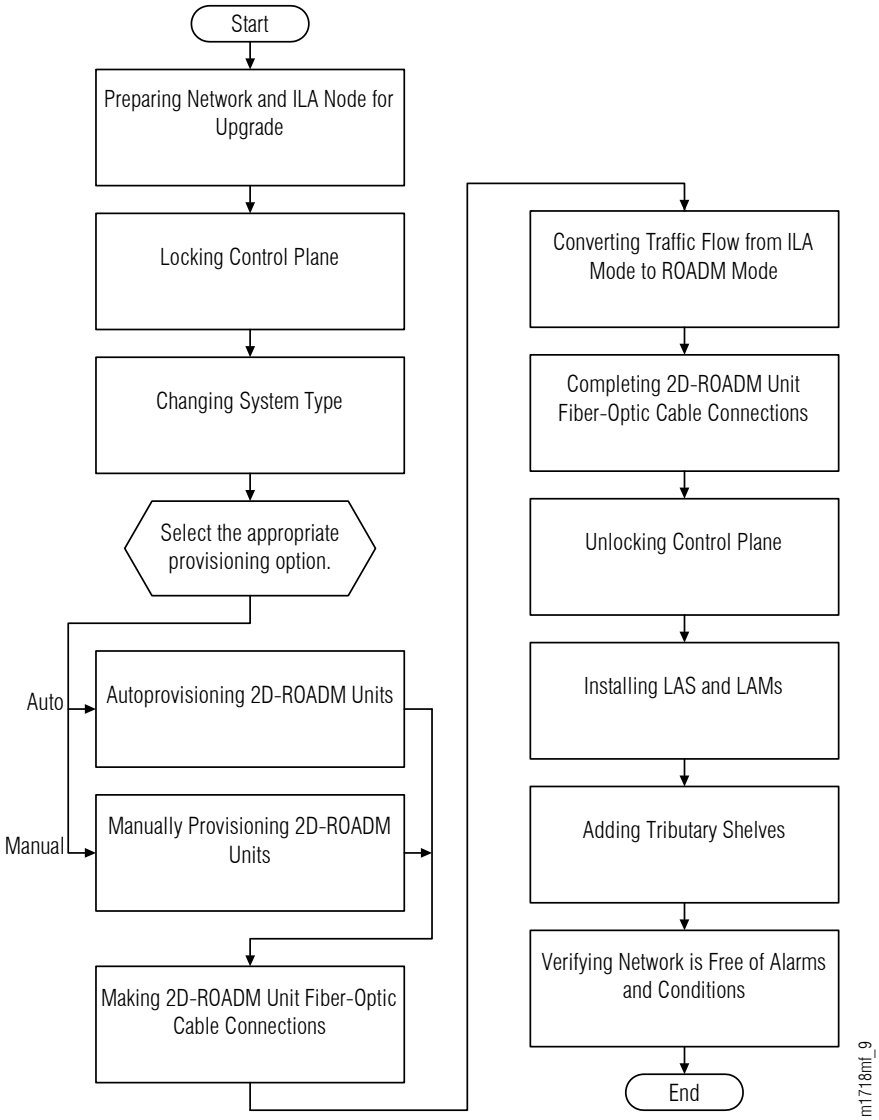


Figure 284: ILA Node to 2D-ROADM Node In-Service Upgrade (Procedure Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

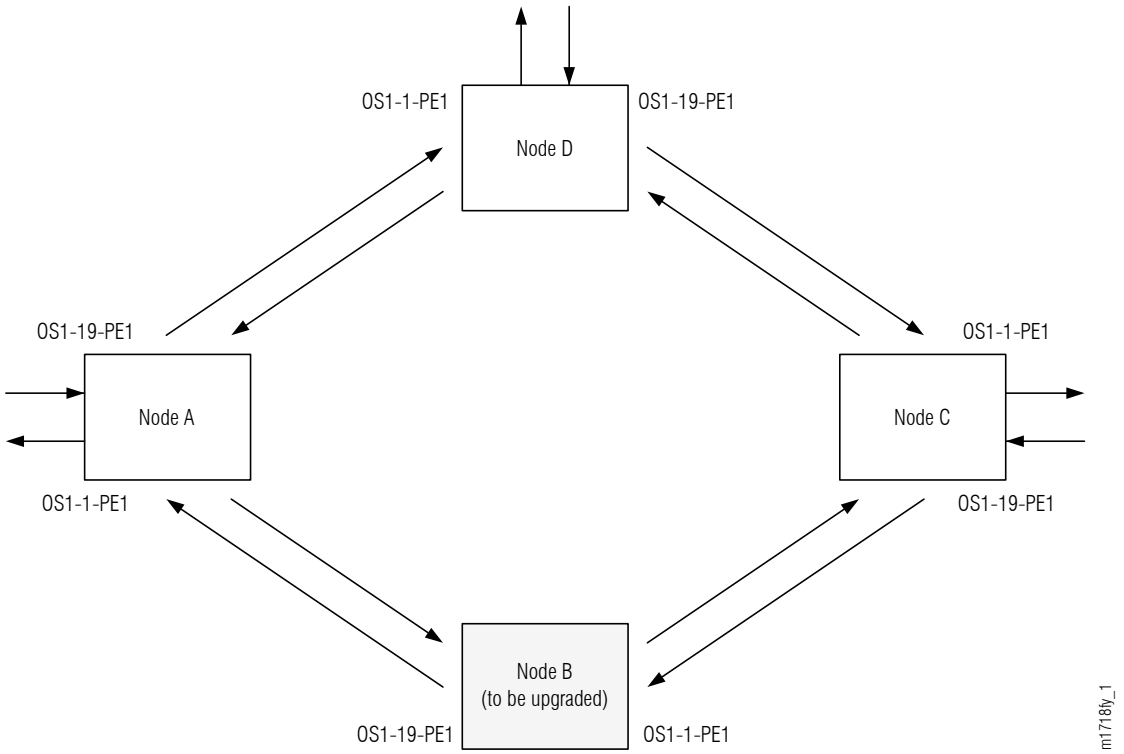


Figure 285: Ring Network Configuration

This procedure can also be used to upgrade linear networks as shown in the following figure.

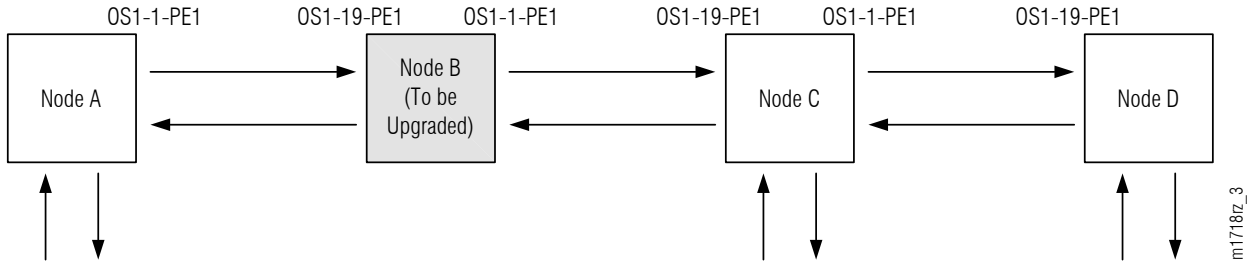


Figure 286: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.5.1
Preparing Network and ILA Node for Upgrade

Prepare the ILA node for the upgrade as follows:

Step 1
If not already done, log on Nodes A, B, C, and D. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[65]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[65] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat this procedure.

Verify Amplifier Type

Step 6
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 7
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to Express Node, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

Clear Alarms and Conditions on Network

Step 8
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 9
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 10
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 11
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat this procedure.

Verify Amplifier Type

Step 12
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 13
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to Express Node, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

✔ This procedure is complete.

8.5.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the value for LOCK is Yes.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

8.5.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	The Confirmation dialog box opens.
	Click Yes.
	The Warning dialog box opens.
	Click Logon.

Note: *Any pass-through traffic is still being carried through the amplifier-to-amplifier connections. The traffic routing does not change until the OPR-MODE command is sent in* Converting Traffic Flow from ILA Mode to ROADM Mode.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	Click Yes in the pop-up window to continue.
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the TYPE is FW7500U_OADM.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning 2D-ROADM Units.
- For manual provisioning, proceed to Manually Provisioning 2D-ROADM Units.

8.5.4 Autoprovisioning 2D-ROADM Units

The 2D-ROADM units (SFMA-RDC1) can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

8.5.5 Manually Provisioning 2D-ROADM Units

The 2D-ROADM units (SFMA-RDC1) can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

8.5.6 Making 2D-ROADM Unit Fiber-Optic Cable Connections

Use this procedure to make fiber-optic cable connections between the amplifier units and the 2D-ROADM units.

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections for the ILA node before the 2D-ROADM units are installed and cabled.

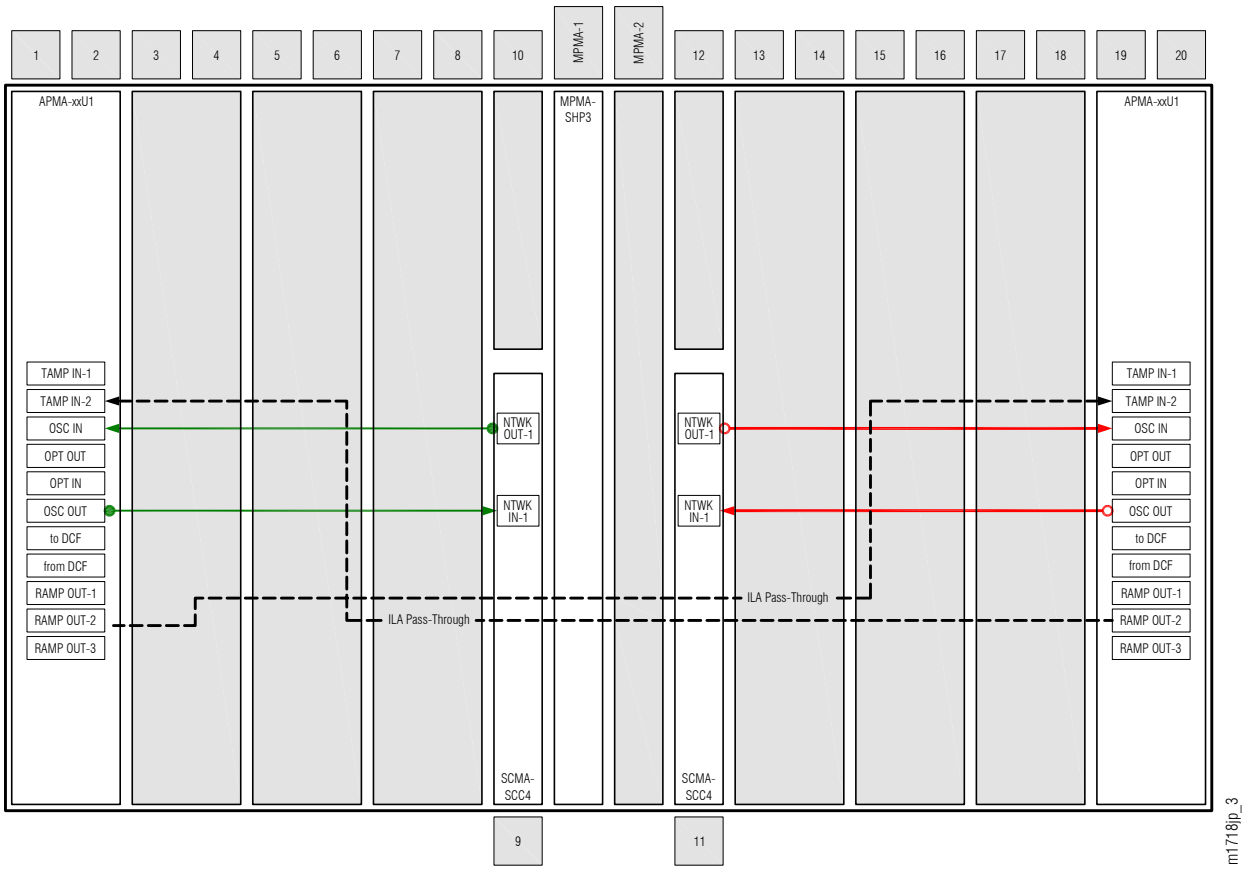


Figure 287: ILA Node Cabling Before 2D-ROADM Unit Installation and Cabling

The following figure shows the fiber-optic cable connections after the 2D-ROADM units are installed and cabled.

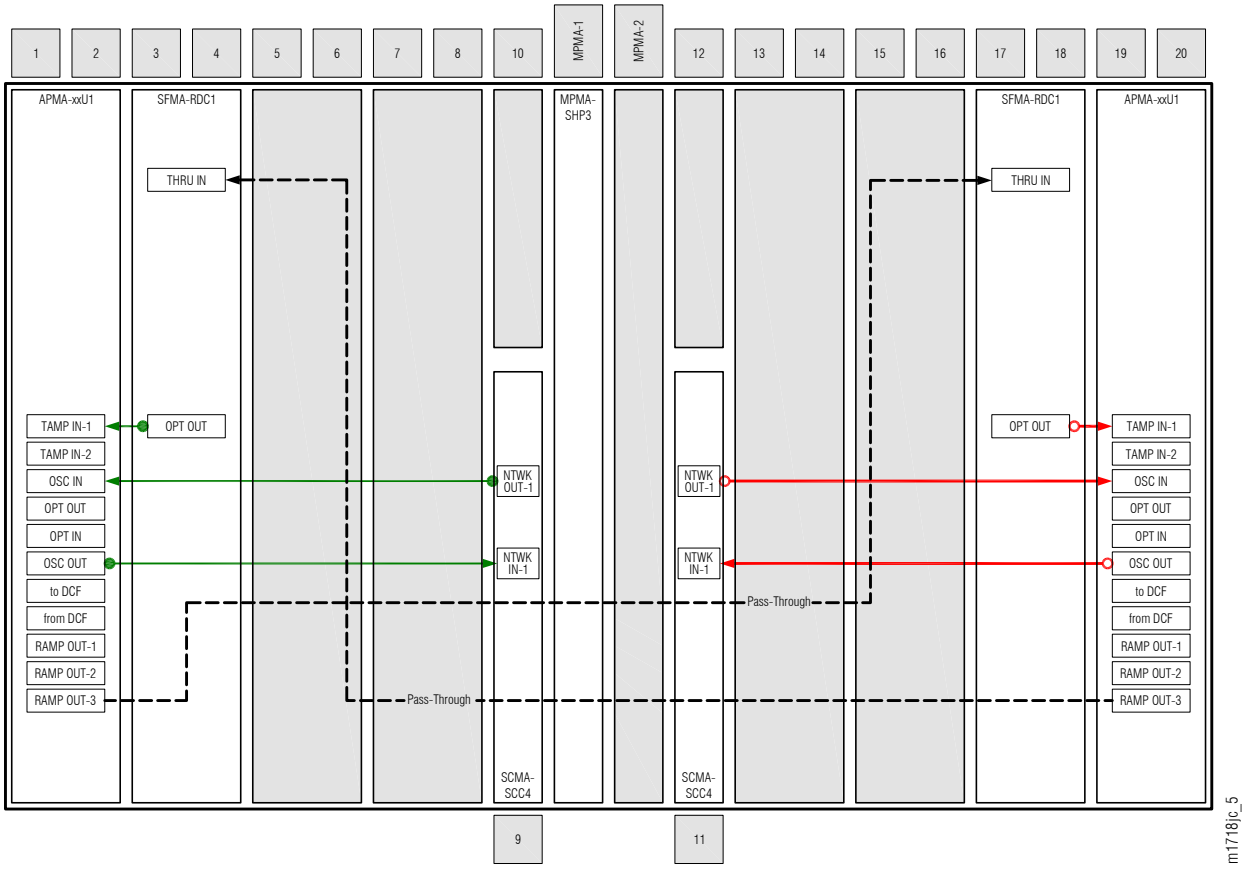


Figure 288: ILA Node Cabling After 2D-ROADM Unit Installation and Initial Cabling

Note: *Do not disconnect the ILA cables until the 2D-ROADM connections are made as described in* Completing 2D-ROADM Unit Fiber-Optic Cable Connections.

Make fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 2
Connect the cables to the connectors of the amplifier (APMA-xxU1) plug-in units and 2D-ROADM (SFMA-RDC1) plug-in units as shown in the preceding figure and listed in the following table.

Table 99: Amplifier Unit and 2D-ROADM Unit Fiber-Optic Cable Connections

Amplifier Unit		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-1	3	OPT OUT
	RAMP OUT-3	17	THRU IN
19	TAMP IN-1	17	OPT OUT
	RAMP OUT-3	3	THRU IN

Step 3
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode.

8.5.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through 2D-ROADM units). This procedure affects the switch in traffic flow in less than 50 milliseconds. Additionally, this procedure allows you to perform the required validations before completing the in-service traffic switch.

There are three modes of operation for this procedure:

- Test mode (MODE=TEST)—Performs the required tests/validations (refer to the following table). A transient condition is reported based on the test result:
  - OPR-MODECOMPLD—Successful test/validation
  - OPR-MODE-FAIL—Unsuccessful test/validation
- Automatic mode (MODE=AUTO)—Performs the required tests/validations (refer to the following table) and then switches the system mode to OADM if all tests/validations are completed successfully. If any test/validation fails, the OPR-MODE-FAIL transient condition is reported with the cause of the failure.
- Override mode (MODE=OVRD)—Switches the system mode to OADM without performing any tests/validations. The override mode is ideal when the system does not have any traffic.

Caution: *Forced switching (MODE=OVRD) of the operation modes can result in traffic hits. If the node has pass-through traffic, Fujitsu recommends that the test mode or automatic mode of operation be used.*

Note: *The automatic mode of conversion is used in this procedure.*

The following table provides a detailed list of the tests and validations performed by the system when the test mode or automatic mode is used when converting operation modes. The tests and validations are listed in the order in which they are performed.

Table 100: Test Mode and Automatic mode System Tests and Validations

System Test/Validation	Description
System alarms	The system monitors the following alarms during the in-service conversion test mode: • Common unit failures–FLT, RMVD, MEA, WARMUP, FVM • Amplifier units–MLSPRE, MLSPOST, ALSPRE, ALSPOST, LDONPRE, LDONPOST, SAPPRE, and SAPPOST • Amplifiers ports–INDWN on PC1and PC6, POS (high and low) on PC1, POS (high and low) on PC2 • WSS CORE Switch unit–INDWN on PC9 and LOL • WDM facility–LOS, PMI, BDIO • OSC facility–BERSF, BERSD, LOS, LOF, MISCON, CNTFAIL, DCCFAIL, TIM-S, INTROPF, LNR • WCH facility–UNEQ-O /AIS-O, NOLIGHT ***Note:*** *The system monitors the alarms throughout the test mode.*
PM validity check	The system performs the following PM validity checks during the in-service conversion test mode: • APMA-M2U1 unit–OPT on PC2, OPR on PE2 • APMA-ULU1 unit–OPR on P1
Optical power level measurements	The system checks that the following optical power level measurements are within specified values: • Amplifier RAMP OUT-2 output port (PC1) and 2D-ROADM unit DMUX IN input port (PE1) • 2D-ROADM unit OPT OUT output port (PE1) and amplifier TAMP IN-1 input port (PC1)
Optical test pattern	The system performs optical test patterns to validate the signal flow of the active pass through traffic between the amplifier (PC1) and the 2D-ROADM port (PE1).

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=AUTO;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=AUTO;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select AUTO from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

The ILA–to–2D-ROADM conversion process begins with the system automatically creating pass-through cross-connects for any existing ILA pass-through traffic. The system then goes into the test and validation mode and performs the actions listed in Table 100. The conversion in process (CONVIP) condition is generated during the conversion process and clears when the conversion completes or terminates.

Note: *If the operation terminates due to the failure of any of the test or validation checks or alarms, the OPR-MODE-FAIL standing condition, containing the cause of the failure, is raised. Refer to Responding to Alarms and Conditions for information on clearing alarms. To perform the conversion regardless of alarms, use MODE=OVRD.*

When the conversion process successfully completes, the OPR-MODE-COMPLD transient condition is raised, and the direct connections between the amplifiers (PC2 and PC6 on both units) are automatically deleted.

Step 3
Proceed to Completing 2D-ROADM Unit Fiber-Optic Cable Connections.

8.5.8
Completing 2D-ROADM Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the cables installed.

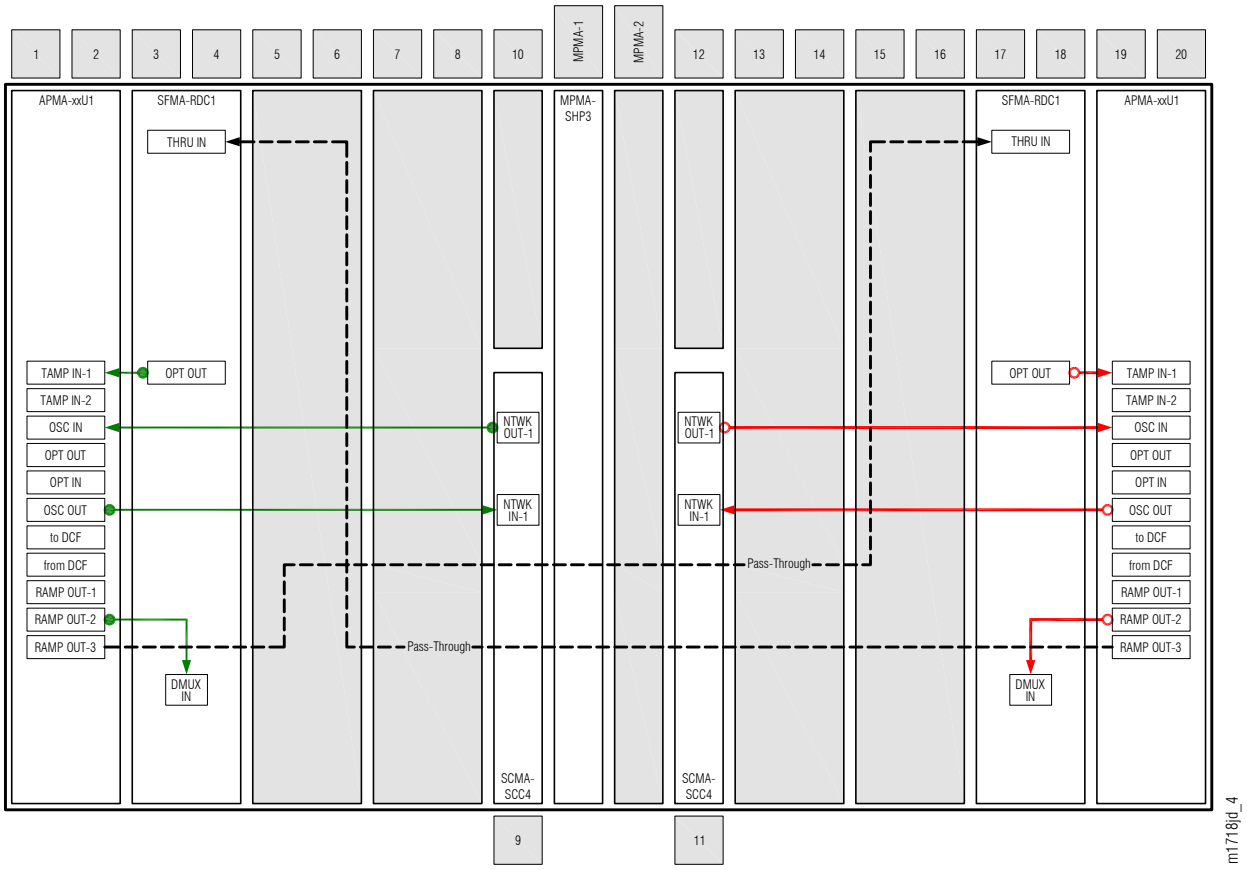


Figure 289: 2D-ROADM Unit Cabling with Drop

To install internal fiber-optic cables, perform the following steps:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

The ILA pass-through connections are no longer needed. The following steps guide you through disconnecting the TAMP IN-2 end of the pass-through connections on the amplifiers and making connections to the 2D-ROADM units.

Step 1
Move the terminal connection of the ILA pass-through cables (see Figure 288) as follows:

a) Disconnect the fiber-optic cable from connector TAMP IN-2 of the Amplifier plug-in unit located in slot 19.

b) Reconnect this cable end to connector DMUX IN of the SFMA-RDC1 plug-in unit located in slot 3 as shown in Figure 289 and listed in the following table.

c) Disconnect the fiber-optic cable from connector TAMP IN-2 of the Amplifier plug-in unit located in slot 1.

d) Reconnect this cable end to connector DMUX IN of the SFMA-RDC1 plug-in unit located in slot 17 as shown in Figure 289 and listed in the following table.

Table 101: Amplifier and 2D-ROADM Unit Fiber-Optic Cable Connections

Amplifier		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-2	3	DMUX IN
19	RAMP OUT-2	17	DMUX IN

Step 2
Proceed to Unlocking Control Plane.

8.5.9 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Installing LAS and LAMs.

8.5.10 Installing LAS and LAMs

After completing the subprocedures in Preparing Network and ILA Node for Upgrade through Unlocking Control Plane, refer to Table 102, for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 102: Install LAS and LAMs

Task	Practice and Section
Install LAS shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

8.5.11 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 103: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision synchronization and/or Tributary shelf OSC units, if required[66].	Provision Synchronization and/or Tributary Shelf OSC Units

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

8.5.12 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify the network is free of alarms and conditions.

Step 1
At each node, retrieve alarms and conditions.

[66] Refer to procedure for applicability.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	
	Click Yes to continue.

This procedure is complete.

8.6
Upgrade ILA Node to Express Node

In this section:

A flowchart of the overall process is shown in the following figure.

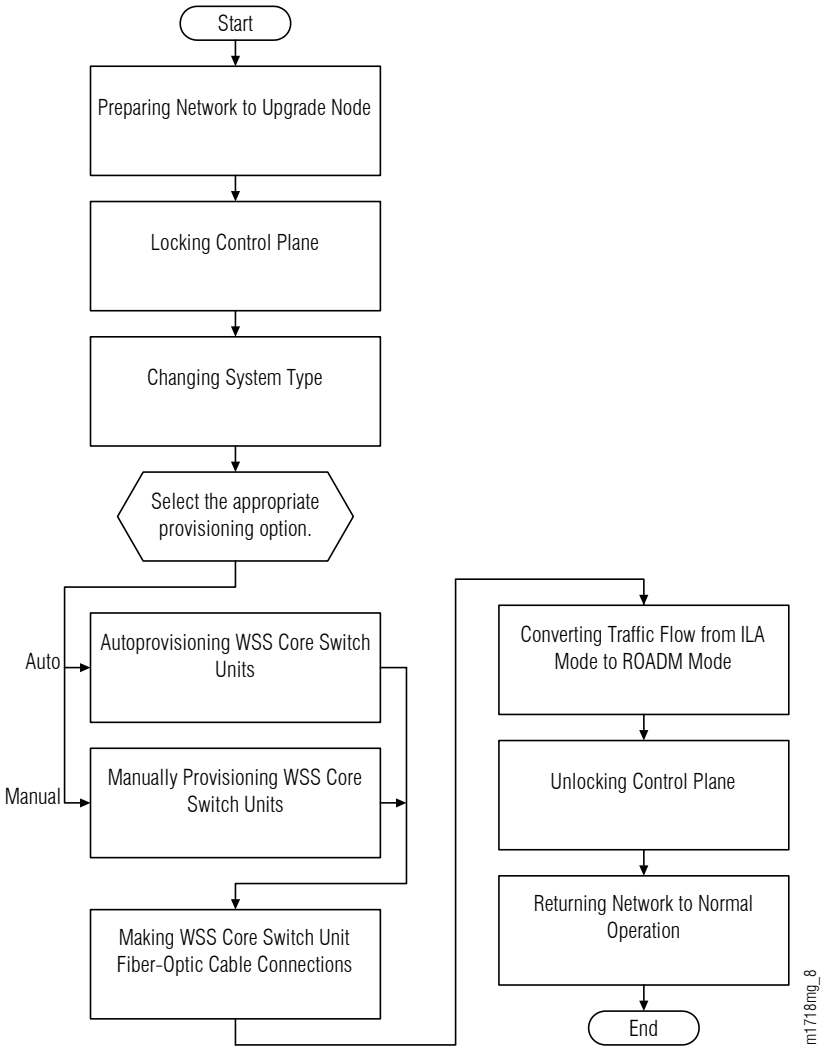


Figure 290: Upgrading ILA Node to Express Node (Procedure Flowchart)

This procedure describes how to prepare a ring or linear network to upgrade one of the nodes from an ILA node to an Express node. This procedure is written for the example 4-node ring shown in the following figure.

The following figure illustrates a ring network in which Node B is the node that is to be upgraded. Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

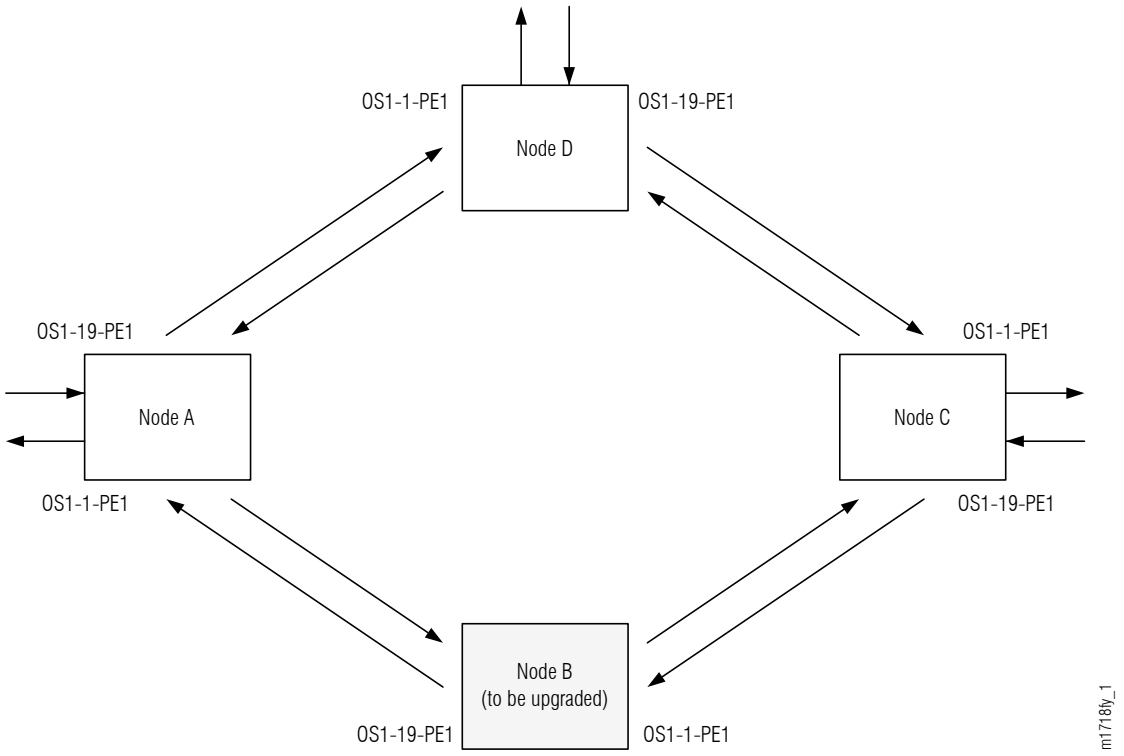


Figure 291: Ring Network Configuration

The procedure can also be used for linear networks; however, protection switching is not possible. See the following figure.

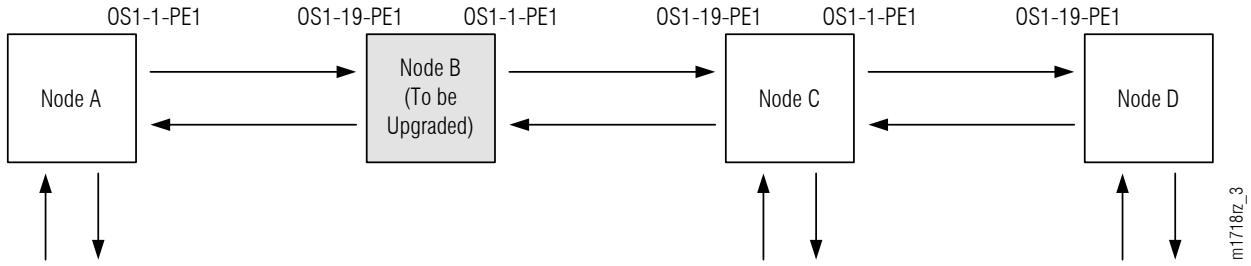


Figure 292: Linear Network Configuration

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.6.1 Preparing Network to Upgrade Node

Prepare the network for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to Setting Up Craft Interface (TL1 Session through TERM1) through Setting Up Craft Interface (NETSMART 500 Session through TERM2).*

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500	

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[67]
		For **TERM2** (TCP/IP):
		TID: FUJITSU
		User ID: ROOT
		Password: ROOT/(Route66K)
		Conn. Mode: TCP/IP
		IP Address: 192.168.1.1
		Port: 2024

	Click Logon. The NETSMART 500 NE View opens. The Security Message dialog box opens. Click OK. ***Note:*** *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*	

Clear Alarms and Conditions

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[67] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 4
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 5
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct-connect application (although it may still be protected).*

Step 6
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 7.

Step 7
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 8.

If NO:
Proceed to Step 9.

Step 8
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then go to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 9
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 10
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs) if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 11
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then go to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 12
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 13
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 14
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 104: Decision Table (Node A)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[68]	SST	
OS1-1-PE1-c	DEF	Yes
	SWITCH	No
OS1-19-PE1-c	DEF	No

[68] c = 1...40 (channel number)

Table 104: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[68]	SST	
	SWITCH	Yes

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 15.

If NO:
Proceed to Step 17.

Step 15
At Node A, for each channel identified in Step 14, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 16
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 104).

[68] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 17
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 18
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 19
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 20
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 21
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 22
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 23.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 23.

Step 23
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 14.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 24
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 25
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 26
Are any dropped channels currently taking traffic from OS1-19-PE1 (refer to the following table)?

Table 105: Decision Table (Node C)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[69]	SST	
OS1-1-PE1-c	DEF	No
	SWITCH	Yes
OS1-19-PE1-c	DEF	Yes

[69] c = 1...40 (channel number)

Table 105: Decision Table (Node C) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[69]	SST	
	SWITCH	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 27.

If NO:
Proceed to Step 29.

Step 27
At Node C, for each channel identified in Step 26, initiate a manual protection switch away from the OS1-19-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 28
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-19-PE1 (refer to Table 105).

[69] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 29
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 30
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 31
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-19-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-19-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 32
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 33
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 34
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 35.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 35.

Step 35
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-19-PE1.

Note: *Use the same criteria used in Step 26.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 36
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 37
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 38
For each drop cross-connect identified in Step 37, identify the ***break direction***, OS1-1-PE1 or OS1-19-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Traveling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 39
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 106: Decision Table (Node D)

Retrieved Cross-Connect Values		Break Direction[70]	Is Current Traffic Dropped from the Break Direction?
PSWDEF[71]	SST		
OS1-1-PE1-c	DEF	OS1-1-PE1	Yes
		OS1-19-PE1	No
	SWITCH	OS1-1-PE1	No
		OS1-19-PE1	Yes
OS1-19-PE1c	DEF	OS1-1-PE1	No
		OS1-19-PE1	Yes
	SWITCH	OS1-1-PE1	Yes
		OS1-19-PE1	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable, and then go to Step 40.

If NO:
Proceed to Step 42.

Step 40
At Node D, for each channel identified in Step 39, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

70 Refer to Step 38.
71 c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 41
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 106).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 42
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 43
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 44
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 45
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 46
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 47
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 48.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 48.

Step 48
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-19-PE1).

Note: *Use the same criteria used in Step 39.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Verify that no dropped channels are currently taking traffic.
	Close the Properties dialog box.

Step 49
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D) and Perform Forced Protection Switches (Node D) for each nonadjacent node.

Step 50
Proceed to Locking Control Plane.

Clear Alarms and Conditions

Step 51
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 52
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 53
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 54
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct-connect application (although it may still be protected).*

Step 55
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 56.

Step 56
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 57.

If NO:
Proceed to Step 9.

Step 57
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then go to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 58
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 59
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs) if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 60
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then go to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 61
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 62
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 63
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 107: Decision Table (Node A)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[72]	SST	
OS1-1-PE1-c	DEF	Yes
	SWITCH	No
OS1-19-PE1-c	DEF	No

[72] c = 1...40 (channel number)

Table 107: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[72]	SST	
	SWITCH	Yes

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 64.

If NO:
Proceed to Step 66.

Step 64
At Node A, for each channel identified in Step 63, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 65
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 107).

[72] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 66
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 67
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 68
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 69
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 70
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 71
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 72.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 72.

Step 72
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 14.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 73
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 74
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 75
Are any dropped channels currently taking traffic from OS1-19-PE1 (refer to the following table)?

Table 108: Decision Table (Node C)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[73]	SST	
OS1-1-PE1-c	DEF	No
	SWITCH	Yes
OS1-19-PE1-c	DEF	Yes

[73] c = 1...40 (channel number)

Table 108: Decision Table (Node C) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[73]	SST	
	SWITCH	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 76.

If NO:
Proceed to Step 78.

Step 76
At Node C, for each channel identified in Step 75, initiate a manual protection switch away from the OS1-19-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1...4
  • s = 1, 19
  • c = 1...40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 77
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-19-PE1 (refer to Table 108).

[73] **c = 1...40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 78
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 79
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 80
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-19-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-19-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 81
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 82
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 83
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 84.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 84.

Step 84
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-19-PE1.

Note: *Use the same criteria used in Step 26.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 85
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 86
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 87
For each drop cross-connect identified in Step 86, identify the ***break direction***, OS1-1-PE1 or OS1-19-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Traveling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 88
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 109: Decision Table (Node D)

Retrieved Cross-Connect Values		Break Direction[74]	Is Current Traffic Dropped from the Break Direction?
PSWDEF[75]	SST		
OS1-1-PE1-c	DEF	OS1-1-PE1	Yes
		OS1-19-PE1	No
	SWITCH	OS1-1-PE1	No
		OS1-19-PE1	Yes
OS1-19-PE1c	DEF	OS1-1-PE1	No
		OS1-19-PE1	Yes
	SWITCH	OS1-1-PE1	Yes
		OS1-19-PE1	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable, and then go to Step 89.

If NO:
Proceed to Step 91.

Step 89
At Node D, for each channel identified in Step 88, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

[74] Refer to Step 87.
[75] c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 90
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 109).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 91
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 92
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 93
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 94
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 95
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 96
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 97.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 97.

Step 97
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-19-PE1).

Note: *Use the same criteria used in Step 39.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 98
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D) and Perform Forced Protection Switches (Node D) for each nonadjacent node.

Step 99
Proceed to Locking Control Plane.

✔ This procedure is complete.

8.6.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

8.6.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
 	
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	
	The Confirmation dialog box opens.
	Click OK.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
 	
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	
	Click Yes in the pop-up window to continue.
	
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

The conversion in progress (CONVIP) condition is raised. The condition clears once the conversion process completes or terminates.

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning WSS Core Switch Units.
- For manual provisioning, proceed to Manually Provisioning WSS Core Switch Units.

8.6.4 Autoprovisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the WSS Core Switch units (SFMA-CMC1) in shelf OS1 of Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

8.6.5 Manually Provisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the WSS Core Switch units (SFMA-CMC1) in shelf OS1 of Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

8.6.6 Making WSS Core Switch Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections before the upgrade.

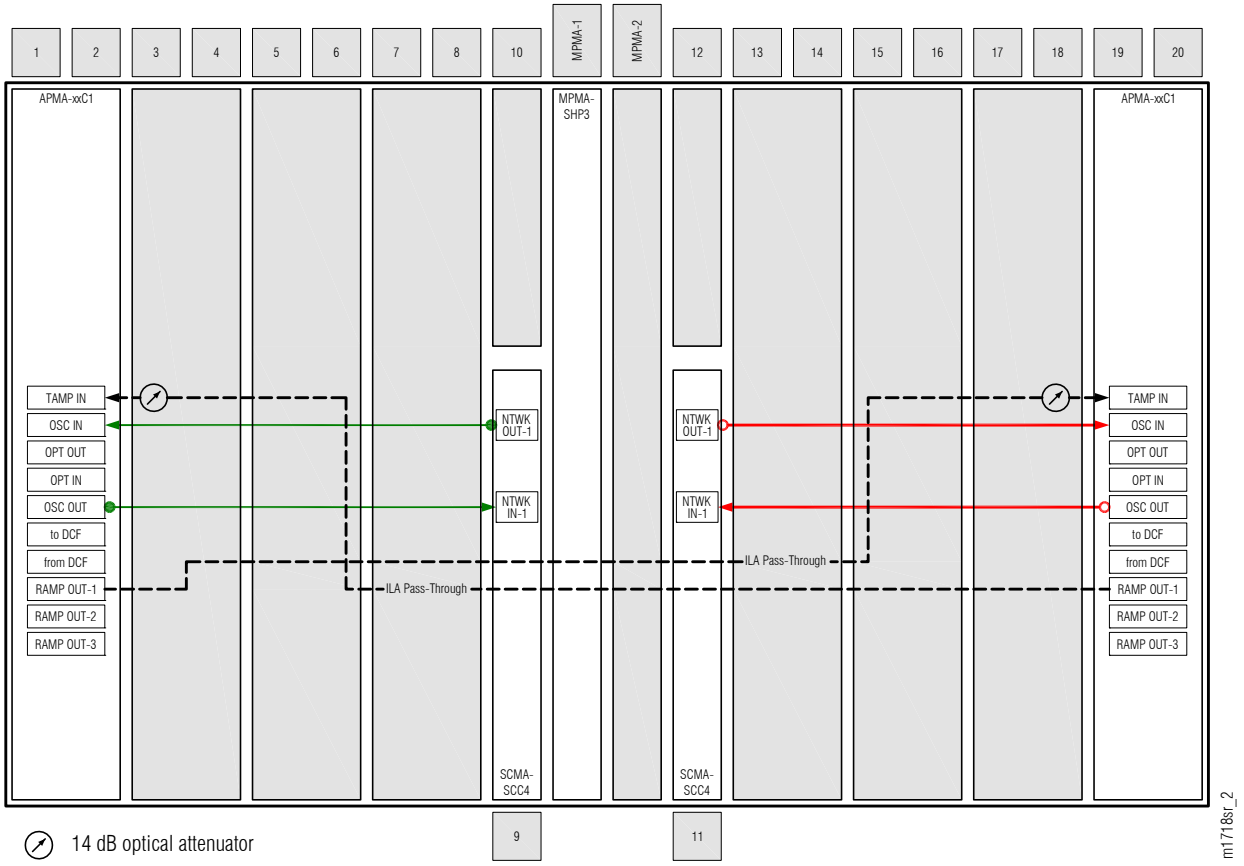


Figure 293: Cabling Before Upgrade (ILA Node)

The following figure shows the fiber-optic cable connections after the upgrade.

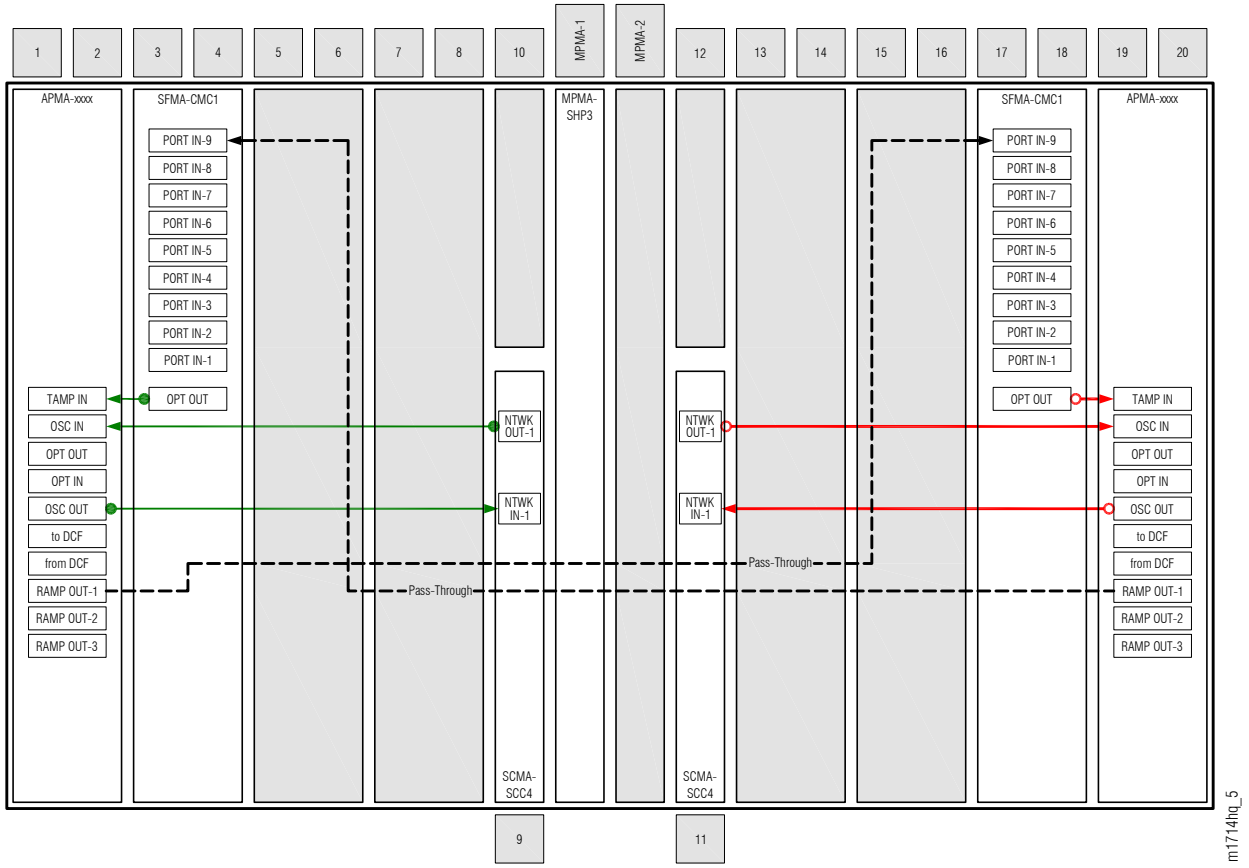


Figure 294: Cabling After Upgrade (Express Node)

Change fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Move Terminal End of Pass-Through Cable Connections

Step 1
Move the terminal connection of OS1-19-PE1–to–OS1-1-PE1 pass-through cable as follows:

a) Disconnect the fiber-optic cable and the 14 dB optical attenuator from connector TAMP IN of the Amplifier plug-in unit located in slot 1. See Figure 293.

b) Remove the 14 dB optical attenuator from the end of the cable.

c) Reconnect this cable end to connector PORT IN-9 of the WSS Core Switch plug-in unit located in slot 3.

Step 2
Move the terminal connection of OS1-1-PE1–to–OS1-19-PE1 pass-through cable as follows:

a) Disconnect the fiber-optic cable and the 14 dB optical attenuator from connector TAMP IN of the Amplifier plug-in unit located in slot 19. See Figure 293.

b) Remove the 14 dB optical attenuator from the end of the cable.

c) Reconnect this cable end to connector PORT IN-9 of the WSS Core Switch plug-in unit located in slot 17.

Connect Amplifier and WSS Core Switch Units

Step 3
Obtain two LC-LC fiber-optic cables, and clean the connectors.

Step 4
Connect the cables to the connectors of the amplifier (APMA-xxxx) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in Figure 294 and listed in the following table.

Table 110: Amplifier Unit and WSS Core Switch Unit Fiber-Optic Cable Connections

Amplifier Unit		WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN	3	OPT OUT
19	TAMP IN	17	OPT OUT

Step 5
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode .

✔ This procedure is complete.

8.6.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through WSS Core Switch units).

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=OVRD;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=OVRD;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select OVRD from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

Step 3
Proceed to Unlocking Control Plane.

8.6.8 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
 	
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the Control Plane tab.
	
	For the LOCK command parameter, click No.
	Click Modify.
	
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
 	
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	
	Close the Operations dialog box.

Step 4
Proceed to Returning Network to Normal Operation.

8.6.9 Returning Network to Normal Operation

To release protection switches and verify that the network is free of alarms and conditions, perform the following steps:

Note: *Perform Steps 5 through 14 for each node in the ring network.*

Provision Pass-Through Cross-Connects for Node B

Note: *These steps are used in combination with the steps in Record Pass-Through Channels for Node B, to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 1
If not already done, log on Nodes A, B, C, and D (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Obtain the record of pass-through channels that was recorded when performing the steps in Record Pass-Through Channels for Node B.

Step 3
At Node B, for each WCH channel previously identified, provision pass-through cross-connects in both directions.

TL1	NETSMART 500

`ENT-CRS-WCH:TID:fromAID,toAID:CTAG :::KEYWORD=DOMAIN;`
fromAID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40
toAID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40
KEYWORD=DOMAIN:
• CKTID = Character string of up to 45 alphanumeric characters, including hyphens (-), delineated by escape quotes (\")
• **Null**
Example:
`(for channel 34)`
`ENT-CRS-WCH:FUJITSU-NODEB: OS1-1-PE1-34,OS1-19-PE1-34:CTAG; ENT-CRS-WCH:FUJITSU-NODEB: OS1-19-PE1-34,OS1-1-PE1-34:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	The Cross-Connects window opens.
	From the View Rate drop-down list, select XC_WCH.
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment or facility associated with the fromAID.
	From a different drop-down list, select the equipment or facility associated with the toAID.
	Click on the fromAID to begin drawing a line that represents the connection.
	Click on the toAID to terminate the line.
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	Entity ▸ *Operations Dialog*
	Click Create.
	The dashed line becomes solid.
	Close the Operations dialog box.
	Do not close the Cross-Connects window.

Step 4
At Node B, verify that pass-through cross-connects have been provisioned in both directions for each WCH channel previously identified in Record Pass-Through Channels for Node B.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Verify that the provisioning parameters are correct.
	Close the Properties dialog box.

Release Protection Switches

Step 5
Retrieve conditions to identify the forced protection switches.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 6
Release each forced protection switch.

TL1	NETSMART 500

`RLS-PROTNSW-WCH:TID:AID:CTAG;`
AID:
• OS1-s-PE1-c
  • s = 1, 19 (slot number)
  • c = 1...40 (channel number)
Example:
`RLS-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-1:CTAG;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Release tab.
	Click Release.

Step 7
Retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 8
Identify all OCh-DPRING–protected drop cross-connects that have parameter SST=SWITCH.

Note: *The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 9
Do local procedures require switch back to the preferred path?

If YES:
Proceed to Step 10.

If NO:
Proceed to Step 14.

Step 10
For each channel identified in Step 8, initiate a manual protection switch.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 11
At Node A, retrieve all cross-connects, and confirm that all OCh-DPRING–protected drop cross-connects are switched to the preferred path (SST=DEF).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 12
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 13
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 14.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 14.

Step 14
Repeat Steps 5 through 13 for each node in the ring network.

Verify Network Is Free of Alarms and Conditions

Step 15
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 16
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 17.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 17.

Step 17
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

✔ This procedure is complete.

8.7
Upgrade ILA Node to 2D-ROADM Node

In this section:

Note: *This procedure applies to ILA nodes running a software release earlier than Release 5.1 and/or using an amplifier other than the AMPA-xxU1 Universal Amplifier unit. For systems running software later than Release 5.1 and using AMPA-xxU1 Universal Amplifier units, follow the procedure given in* In-Service Upgrade ILA Node to 2D-ROADM Node*, to upgrade an ILA node to a 2D-ROADM node.*

A flowchart of the overall process is shown in the following figure.

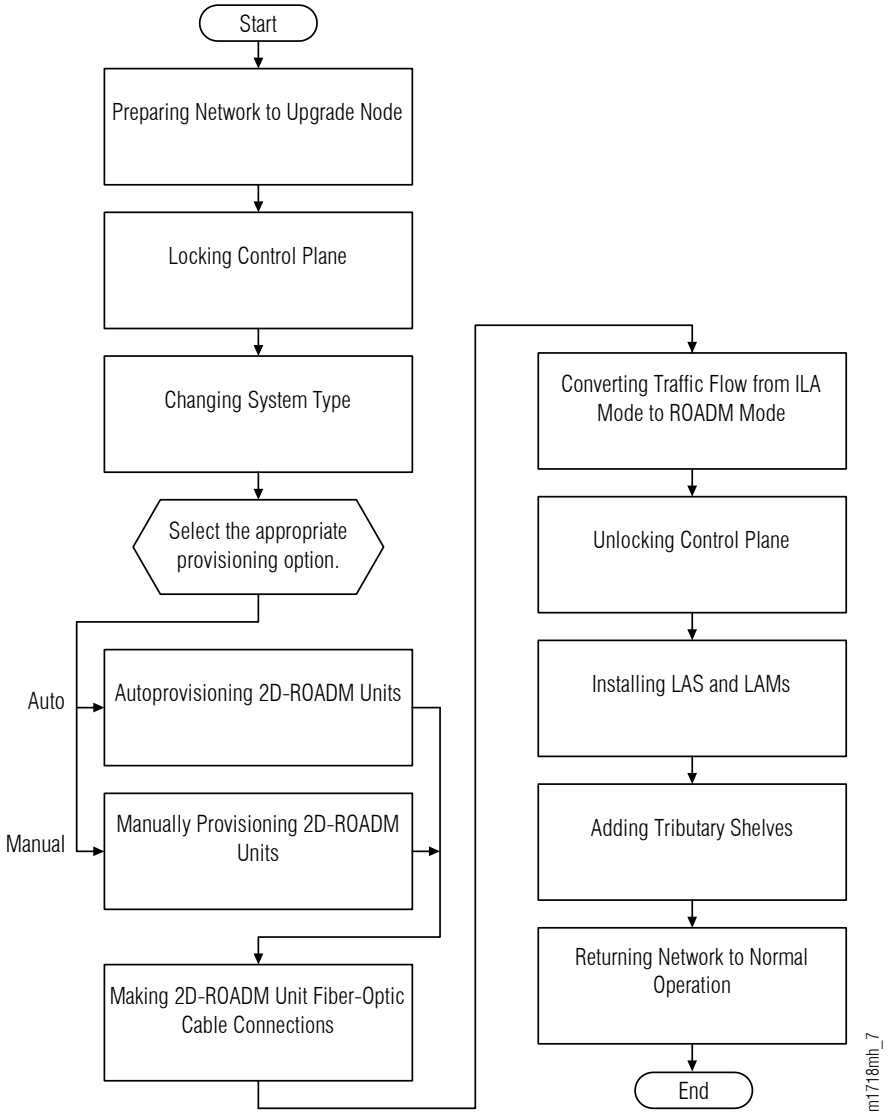


Figure 295: Upgrading ILA Node to 2D-ROADM Node (Procedure Flowchart)

This procedure describes how to prepare a ring network to upgrade one of the nodes in the ring from an ILA node to a 2D-ROADM node. This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

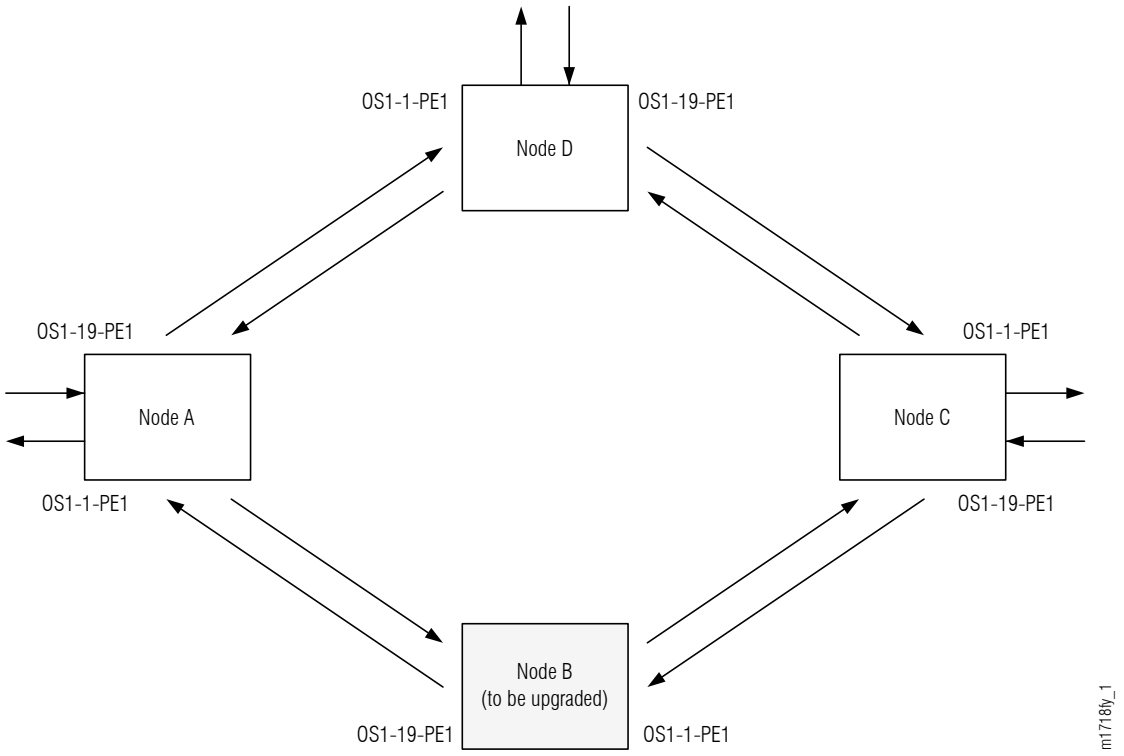


Figure 296: Ring Network Configuration

The procedure can also be used for linear networks; however, protection switching is not possible. See the following figure.

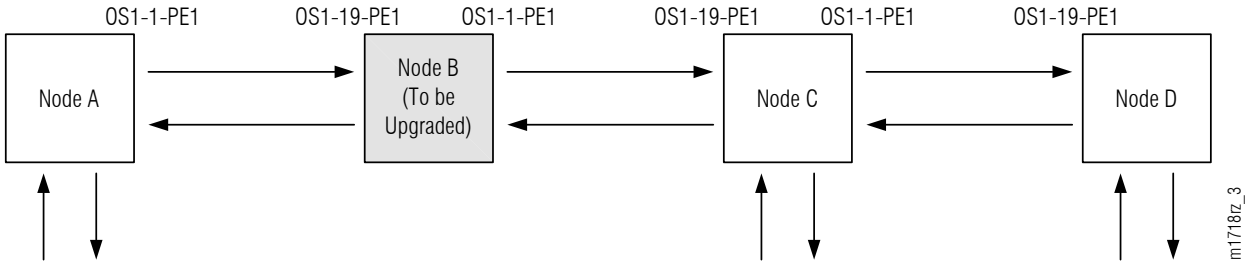


Figure 297: Linear Network Configuration

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.7.1 Preparing Network to Upgrade Node

Prepare the network for the upgrade as follows:

Step 1

If not already done, log on Nodes A, B, C, and D. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to Setting Up Craft Interface (TL1 Session through TERM1) through Setting Up Craft Interface (NETSMART 500 Session through TERM2).*

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[76]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[76] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 4
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 5
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct connect application (although it may still be protected).*

Step 6
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 7.

Step 7
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 8.

If NO:
Proceed to Step 9.

Step 8
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then go to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 9
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 10
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs) if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 11
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then go to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 12
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 13
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 14
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 111: Decision Table (Node A)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[77]	SST	
OS1-1-PE1-c	DEF	Yes
	SWITCH	No
OS1-19-PE1-c	DEF	No

[77] **c = 1...40 (channel number)**

Table 111: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[77]	SST	
	SWITCH	Yes

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 15.

If NO:
Proceed to Step 17.

Step 15
At Node A, for each channel identified in Step 14, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 16
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 111).

[77] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 17
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 18
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 19
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 20
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 21
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 22
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 23.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 23.

Step 23
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 12.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 24
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 25
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 26
Are any dropped channels currently taking traffic from OS1-19-PE1 (refer to the following table)?

Table 112: Decision Table (Node C)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[78]	SST	
OS1-1-PE1-c	DEF	No
	SWITCH	Yes
OS1-19-PE1-c	DEF	Yes

[78] c = 1...40 (channel number)

Table 112: Decision Table (Node C) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[78]	SST	
	SWITCH	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 27.

If NO:
Proceed to Step 29.

Step 27
At Node C, for each channel identified in Step 26, initiate a manual protection switch away from the OS1-19-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 28
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-19-PE1 (refer to Table 112).

[78] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 29
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 30
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 31
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-19-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-19-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 32
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 33
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 34
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 35.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 35.

Step 35
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-19-PE1.

Note: *Use the same criteria used in Step 24.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 36
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 37
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 38
For each drop cross-connect identified in Step 37, identify the ***break direction***, OS1-1-PE1 or OS1-19-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Traveling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 39
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 113: Decision Table (Node D)

Retrieved Cross-Connect Values		Break Direction[79]	Is Current Traffic Dropped from the Break Direction?
PSWDEF[80]	SST		
OS1-1-PE1-c	DEF	OS1-1-PE1	Yes
		OS1-19-PE1	No
	SWITCH	OS1-1-PE1	No
		OS1-19-PE1	Yes
OS1-19-PE1c	DEF	OS1-1-PE1	No
		OS1-19-PE1	Yes
	SWITCH	OS1-1-PE1	Yes
		OS1-19-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable, and then go to Step 40.

If NO:
Proceed to Step 42.

Step 40
At Node D, for each channel identified in Step 39, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

79 Refer to Step 38.
80 c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 41
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 113).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 42
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 43
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 44
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 45
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 46
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 47
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 48.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 48.

Step 48
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-19-PE1).

Note: *Use the same criteria used in Step 36.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 49
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 50
Proceed to Locking Control Plane.

Clear Alarms and Conditions

Step 51
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 52
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 53
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 54
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct connect application (although it may still be protected).*

Step 55
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 56.

Step 56
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 57.

If NO:
Proceed to Step 9.

Step 57
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then go to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 58
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 59
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs) if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 60
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then go to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 61
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 62
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 63
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 114: Decision Table (Node A)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[81]	SST	
OS1-1-PE1-c	DEF	Yes
	SWITCH	No
OS1-19-PE1-c	DEF	No

[81] c = 1...40 (channel number)

Table 114: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[81]	SST	
	SWITCH	Yes

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 64.

If NO:
Proceed to Step 66.

Step 64
At Node A, for each channel identified in Step 63, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 65
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 114).

[81] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 66
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 67
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 68
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 69
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 70
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 71
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 72.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 72.

Step 72
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 12.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 73
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 74
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 75
Are any dropped channels currently taking traffic from OS1-19-PE1 (refer to the following table)?

Table 115: Decision Table (Node C)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[82]	SST	
OS1-1-PE1-c	DEF	No
	SWITCH	Yes
OS1-19-PE1-c	DEF	Yes

[82] c = 1...40 (channel number)

Table 115: Decision Table (Node C) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[82]	SST	
	SWITCH	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 76.

If NO:
Proceed to Step 78.

Step 76
At Node C, for each channel identified in Step 75, initiate a manual protection switch away from the OS1-19-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 77
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-19-PE1 (refer to Table 115).

[82] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 78
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 79
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 80
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-19-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-19-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 81
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 82
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 83
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 84.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 84.

Step 84
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-19-PE1.

Note: *Use the same criteria used in Step 24.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 85
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 86
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 87
For each drop cross-connect identified in Step 86, identify the ***break direction***, OS1-1-PE1 or OS1-19-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Traveling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 88
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 116: Decision Table (Node D)

Retrieved Cross-Connect Values		Break Direction[83]	Is Current Traffic Dropped from the Break Direction?
PSWDEF[84]	SST		
OS1-1-PE1-c	DEF	OS1-1-PE1	Yes
		OS1-19-PE1	No
	SWITCH	OS1-1-PE1	No
		OS1-19-PE1	Yes
OS1-19-PE1c	DEF	OS1-1-PE1	No
		OS1-19-PE1	Yes
	SWITCH	OS1-1-PE1	Yes
		OS1-19-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable, and then go to Step 89.

If NO:
Proceed to Step 91.

Step 89
At Node D, for each channel identified in Step 88, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

83 Refer to Step 87.
84 c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 90
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 116).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 91
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 92
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 93
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 94
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 95
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 96
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 97.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 97.

Step 97
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-19-PE1).

Note: *Use the same criteria used in Step 36.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 98
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 99
Proceed to Locking Control Plane.

✔ This procedure is complete.

8.7.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

8.7.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
 	
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	
	The Confirmation dialog box opens.
	Click OK.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
 	
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	
	Click Yes in the pop-up window to continue.
	
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

The conversion in progress (CONVIP) condition is raised. The condition clears once the conversion process completes or terminates.

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning 2D-ROADM Units.
- For manual provisioning, proceed to Manually Provisioning 2D-ROADM Units.

8.7.4 Autoprovisioning 2D-ROADM Units

The 2D-ROADM units can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

8.7.5 Manually Provisioning 2D-ROADM Units

The 2D-ROADM units can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

8.7.6 Making 2D-ROADM Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections before the upgrade.

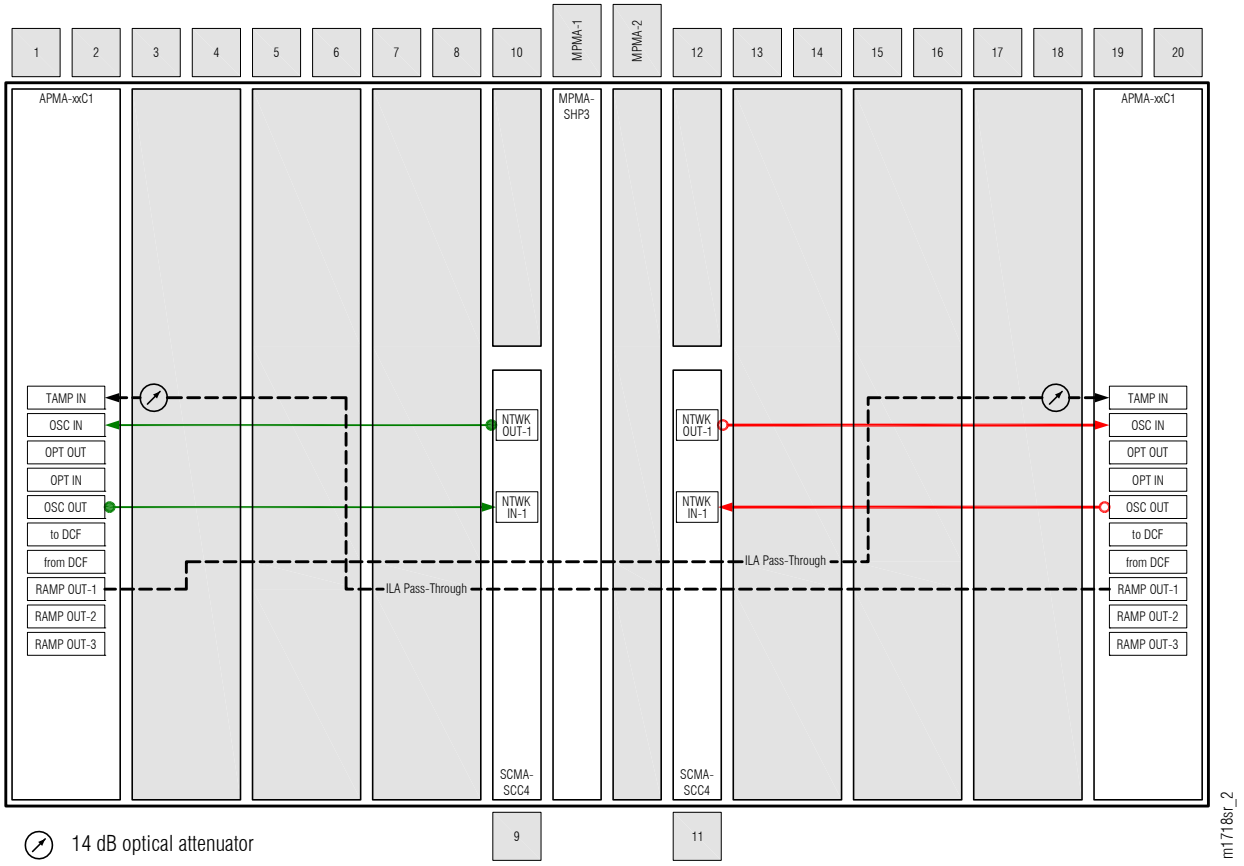


Figure 298: Cabling Before Upgrade (ILA Node)

The following figure shows the fiber-optic cable connections after the upgrade.

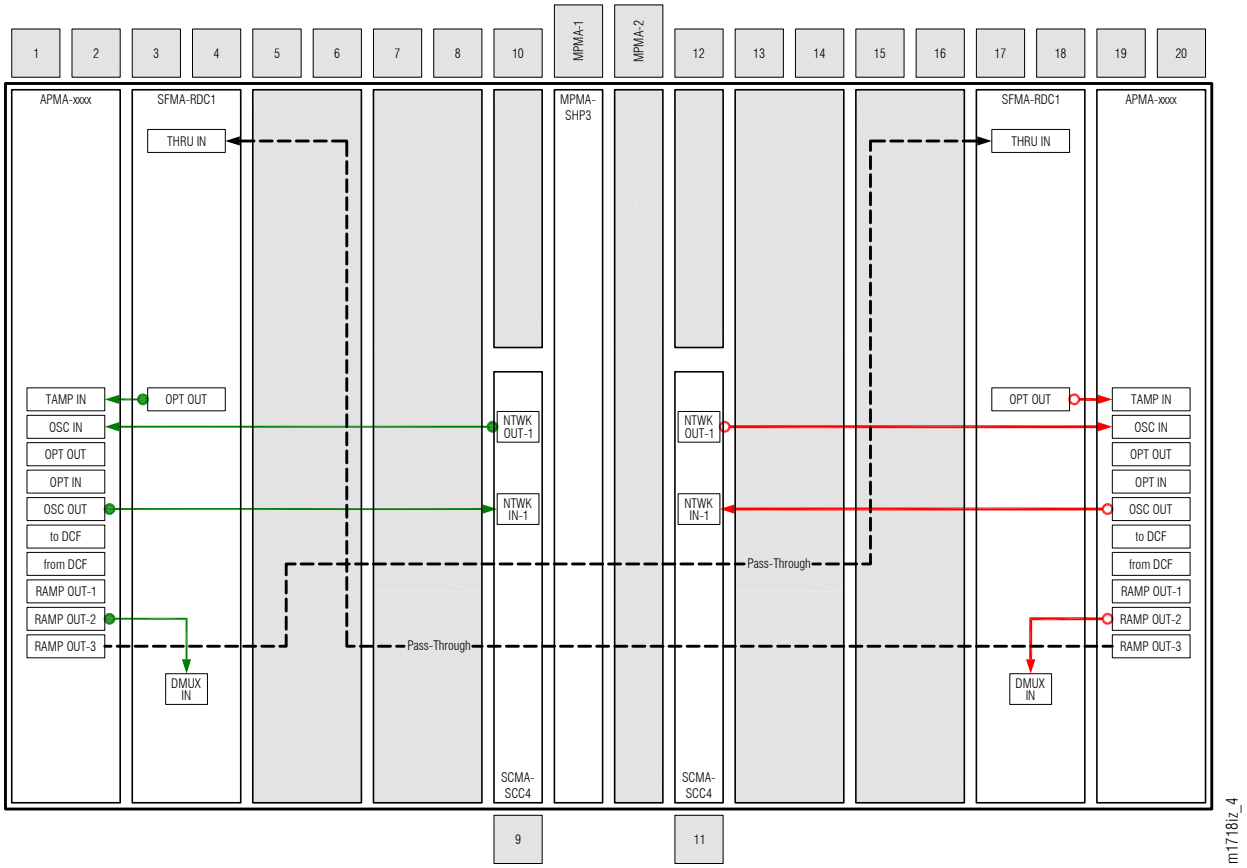


Figure 299: Cabling After Upgrade (2D-ROADM Node)

Change fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Remove ILA Pass-Through Cables and Attenuators

Step 1

Disconnect and remove the ILA pass-through cables shown in Figure 298 and listed in the following table.

Note: *The optical attenuators located at the TAMP IN connectors are removed in the next step.*

Table 117: Pass-Through Connections between APMA-xxC1 Amplifiers

From Amplifier (APMA-xxC1)		To Amplifier (APMA-xxC1)	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-1	19	TAMP IN
1	TAMP IN	19	RAMP OUT-1

Step 2
Disconnect and remove the two 14 dB optical attenuators from the TAMP IN connectors of the Amplifier plug-in units located in slots 1 and 19.

Install Pass-Through Cables

Step 3
Obtain and clean two LC-LC fiber-optic cables.

Step 4
Connect the cable ends to the appropriate plug-in units and connectors as shown in Figure 299 and listed in the following table.

Table 118: Pass-Through Cable Connections (2D-ROADM Configuration)

Amplifier (APMA-xxxx)		2D ROADM Unit (SFMA-RDC1)	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-3	17	THRU IN
19	RAMP OUT-3	3	THRU IN

Connect Amplifier and 2D-ROADM Units

Step 5
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 6
Connect the cables to the connectors of the amplifier (APMA-xxxx) plug-in units and 2D-ROADM (SFMA-RDC1) plug-in units as shown in Figure 299 and listed in the following table.

Table 119: Amplifier Unit and 2D-ROADM Unit Fiber-Optic Cable Connections

Amplifier Unit		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN	3	OPT OUT
19	TAMP IN	17	OPT OUT
1	RAMP OUT-2	3	DMUX IN
19	RAMP OUT-2	17	DMUX IN

Step 7
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode.

✔ This procedure is complete.

8.7.7
Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through 2D-ROADM units). T

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=OVRD;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=OVRD;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select OVRD from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

Step 3
Proceed to Unlocking Control Plane.

8.7.8 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Installing LAS and LAMs.

8.7.9 Installing LAS and LAMs

After completing the subprocedures in Preparing Network to Upgrade Node through Unlocking Control Plane, refer to Table 120 for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 120: Install LAS and LAMs

Task	Practice and Section
Install LAS shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

8.7.10 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 121: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors

Table 121: Adding Tributary Shelf (Cont.)

Task	Practice and Section
Provision synchronization and/or Tributary shelf OSC units, if required[85].	Provision Synchronization and/or Tributary Shelf OSC Units

Step 2
Proceed to Returning Network to Normal Operation.

8.7.11 Returning Network to Normal Operation

To release protection switches and verify that the network is free of alarms and conditions, perform the following steps:

Note: *Perform Steps 5 through 13 for each node in the ring network.*

Provision Pass-Through Cross-Connects for Node B

Note: *These steps are used in combination with the steps in Record Pass-Through Channels for Node B, to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 1
If not already done, log on Nodes A, B, C, and D (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Obtain the record of pass-through channels that was recorded when performing the steps in Record Pass-Through Channels for Node B.

Step 3
At Node B, for each WCH channel previously identified, provision pass-through cross-connects in both directions.

[85] Refer to procedure for applicability.

TL1	NETSMART 500

`ENT-CRS-WCH:TID:fromAID,toAID:CTAG :::KEYWORD=DOMAIN;`
fromAID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40
toAID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40
KEYWORD=DOMAIN:
• CKTID = Character string of up to 45 alphanumeric characters, including hyphens (-), delineated by escape quotes (\")
• **Null**
Example:
`(for channel 34) ENT-CRS-WCH:FUJITSU-NODEB: OS1-1-PE1-34,OS1-19-PE1-34:CTAG; ENT-CRS-WCH:FUJITSU-NODEB: OS1-19-PE1-34,OS1-1-PE1-34:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	The Cross-Connects window opens.
	From the View Rate drop-down list, select XC_WCH.
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment or facility associated with the fromAID.
	From a different drop-down list, select the equipment or facility associated with the toAID.
	Click on the fromAID to begin drawing a line that represents the connection.
	Click on the toAID to terminate the line.
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	Entity ▸ *Operations Dialog*
	Click Create.
	The dashed line becomes solid.
	Close the Operations dialog box.
	Do not close the Cross-Connects window.

Step 4
At Node B, verify that pass-through cross-connects have been provisioned in both directions for each WCH channel previously identified in Record Pass-Through Channels for Node B.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Verify that the provisioning parameters are correct.
	Close the Properties dialog box.

Release Protection Switches

Step 5
Retrieve conditions to identify the forced protection switches.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 6
Release each forced protection switch.

TL1	NETSMART 500

`RLS-PROTNSW-WCH:TID:AID:CTAG;`
AID:
• OS1-s-PE1-c
  • s = 1, 19 (slot number)
  • c = 1…40 (channel number)
 	
Example:
`RLS-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-1:CTAG;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Release tab.
	Click Release.

Step 7
Retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 8
Identify all OCh-DPRING–protected drop cross-connects that have parameter SST=SWITCH.

Note: *The value of SST (**DEF** or **SWITCH**) indicates whether the preferred path is currently used (**DEF**) or not (**SWITCH**).*

Step 9
Do local procedures require switch back to the preferred path?

If YES:
Proceed to Step 10.

If NO:
Proceed to Step 14.

Step 10
For each channel identified in Step 8, initiate a manual protection switch.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 11
At Node A, retrieve all cross-connects, and confirm that all OCh-DPRING–protected drop cross-connects are switched to the preferred path (SST=DEF).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 12
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 13
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 14.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 14.

Step 14
Repeat Steps 5 through 13 for each node in the network, then go to Step 15.

Verify Network Is Free of Alarms and Conditions

Step 15
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 16
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 17.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 17.

Step 17
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

✔ This procedure is complete.

8.8 In-Service Upgrade Express Node to ROADM Node

In this section:

A flowchart of the overall process is shown in the following figure.

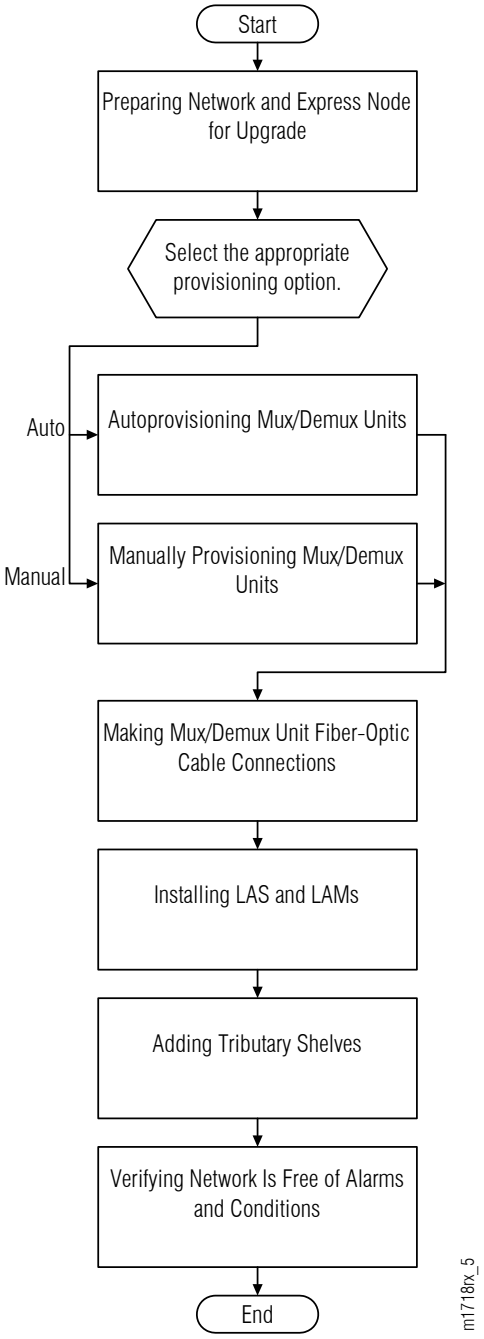


Figure 300: Upgrading Express Node to ROADM Node–In-Service (Procedure Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Nodes A and C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

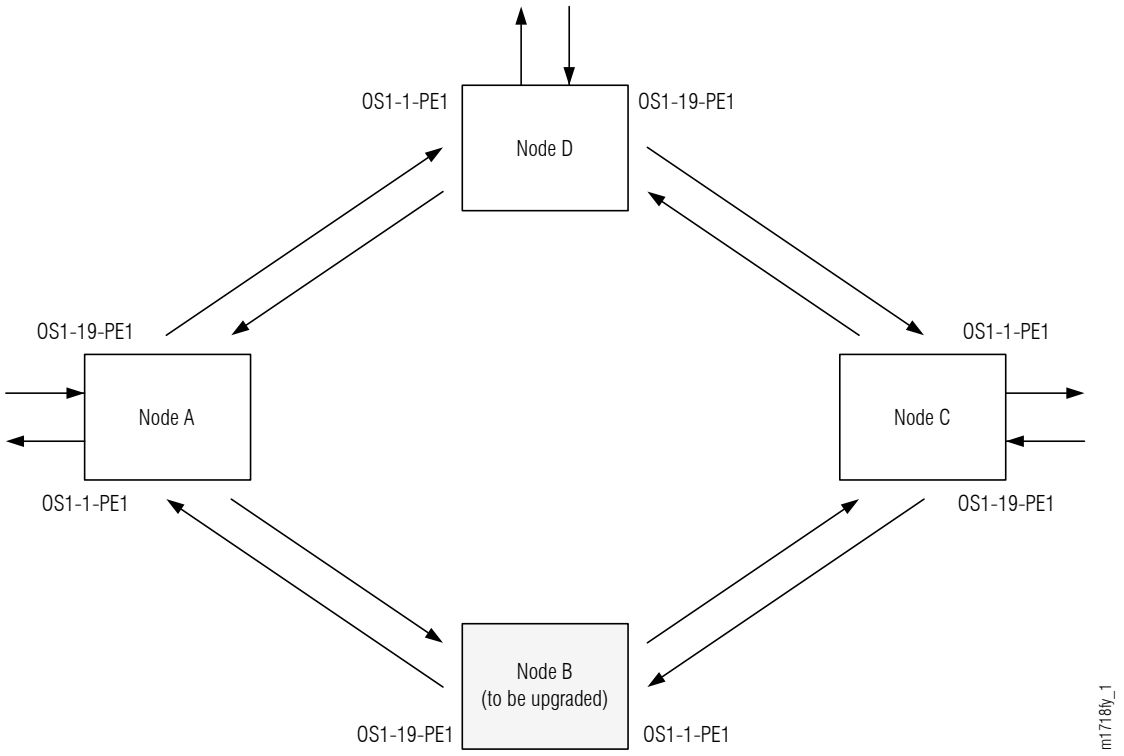


Figure 301: Ring Network Configuration

This procedure can also be used to upgrade linear networks as shown in the following figure.

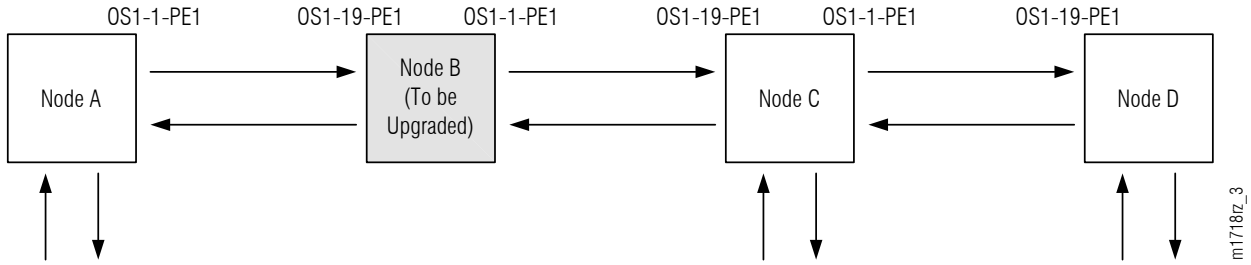


Figure 302: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.8.1
Preparing Network and Express Node for Upgrade

Prepare the Express node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[86]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[86] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

The correct GISSUE value for FLASHWAVE 7500 Release 7.1 software is 07-01-2.

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 4.

Step 6
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning Mux/Demux Units.
- For manual provisioning, proceed to Manually Provisioning Mux/Demux Units.

Clear Alarms and Conditions on Network

Step 7
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 8
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 9
At Node B retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	Close the Properties dialog box.

Step 10
Is the active GISSUE correct?

The correct GISSUE value for FLASHWAVE 7500 Release 7.1 software is 07-01-2.

If YES:
Proceed to Step 11.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 9.

Step 11
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning Mux/Demux Units.
- For manual provisioning, proceed to Manually Provisioning Mux/Demux Units.

✔ This procedure is complete.

8.8.2 Autoprovisioning Mux/Demux Units

The Mux/Demux units (MDMA-RMC1) can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Use the procedure in Autoprovision Optical Shelf Equipment and Facilities to provision the Mux/Demux (MDMA-RMC1) units.

Step 2
Proceed to Making Mux/Demux Unit Fiber-Optic Cable Connections.

8.8.3 Manually Provisioning Mux/Demux Units

The Mux/Demux units (MDMA-RMC1) can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Use the procedure in to Manually Provision Optical Shelf Equipment, to provision the Mux/Demux (MDMA-RMC1) units.

Step 2
Proceed to Making Mux/Demux Unit Fiber-Optic Cable Connections.

8.8.4 Making Mux/Demux Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections for the Express node before the DMUX IN/OUT cables are installed.

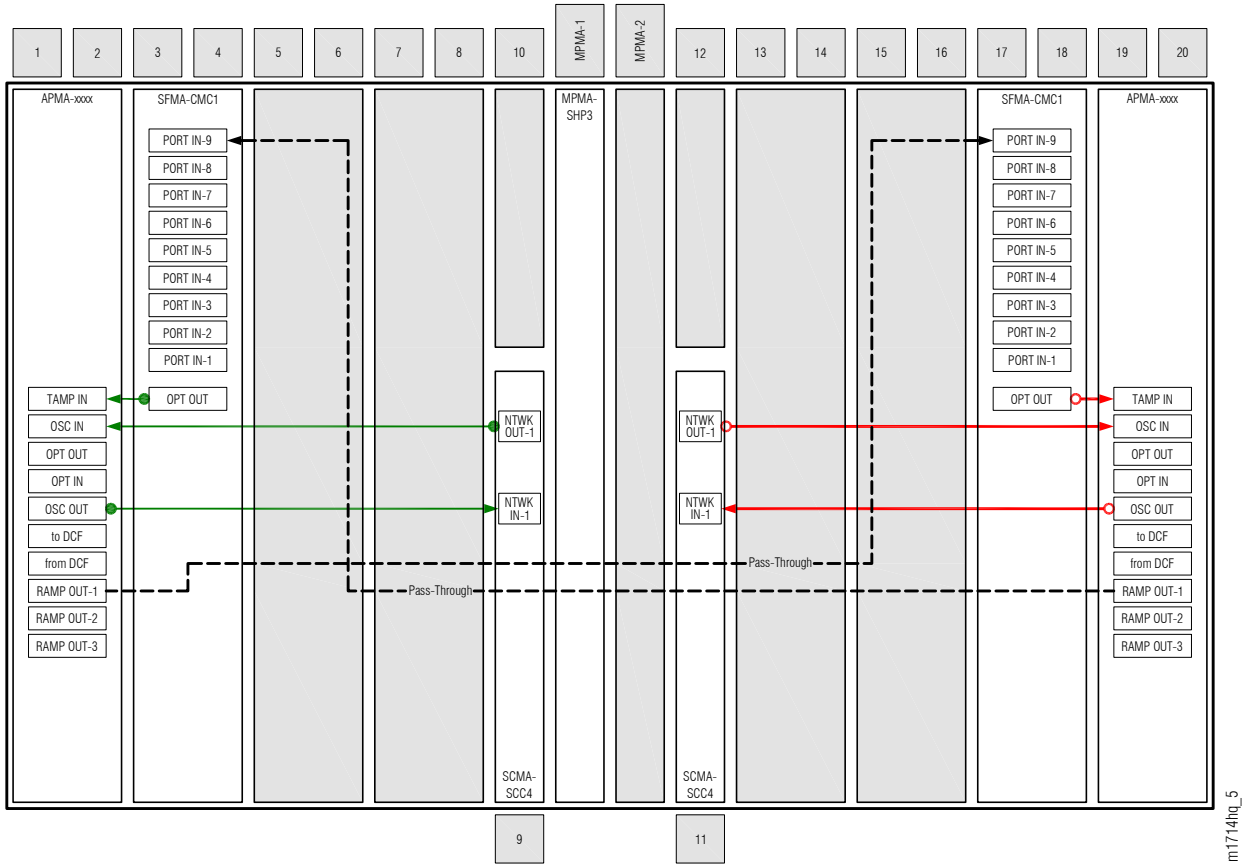


Figure 303: Express Node Cabling Before WSS Core Switch Unit Installation and Cabling

The following figure shows the cables after the DMUX IN/OUT cables are installed.

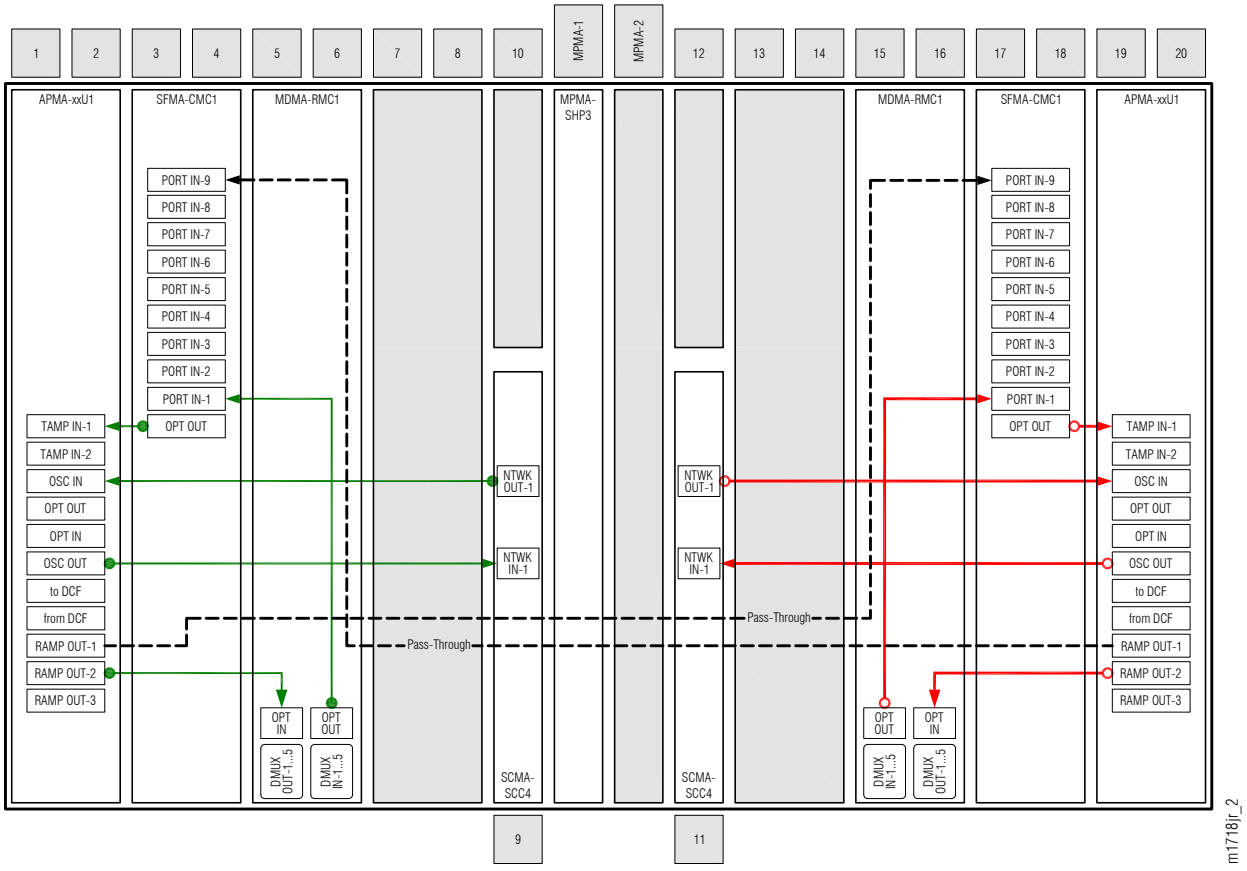


Figure 304: Fiber-Optic Cable Connections between Optical Shelf Plug-In Units

To install internal fiber-optic cables, perform the following steps:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 2
Connect the cables to the connectors of the Mux/Demux (MDMA-RMC1) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in Figure 304 and listed in the following table.

Table 122: Mux/Demux Unit and WSS Core Switch Unit Fiber-Optic Cable Connections

Mux/Demux Unit		WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
5	OPT OUT	3	PORT IN-1
15	OPT OUT	17	PORT IN-1

Step 3
Connect the cables to the connectors of the amplifier (AMPA-xxU1) plug-in units and Mux/Demux (MDMA-RMC1) plug-in units as shown in Figure 304 and listed in the following table.

Table 123: Amplifier Unit and Mux/Demux Unit Fiber-Optic Cable Connections

Amplifier Unit		Mux/Demux Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-2	5	OPT IN
19	RAMP OUT-2	15	OPT IN

Step 4
Proceed to Installing LAS and LAMs.

8.8.5
Installing LAS and LAMs

This subsection contains detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Using the procedures referenced in Table 124, install LAS and LAMs.

Table 124: Install LAS and LAMs

Task	Practice and Section
Install LAS shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

8.8.6 Adding Tributary Shelves

Use the following procedure to add Tributary shelves.

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 125: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable
Create Tributary shelf entity, and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision synchronization and/or Tributary shelf OSC units, if required[87].	Provision Synchronization and/or Tributary Shelf OSC Units

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

8.8.7 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify the network is free of alarms and conditions:

Step 1
At each node, retrieve alarms and conditions.

[87] Refer to procedure for applicability.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	
	Click Yes to continue.

This procedure is complete.

8.9
Upgrade ROADM Node to HUB Node

In this section:

The flowchart is shown in the following figure.

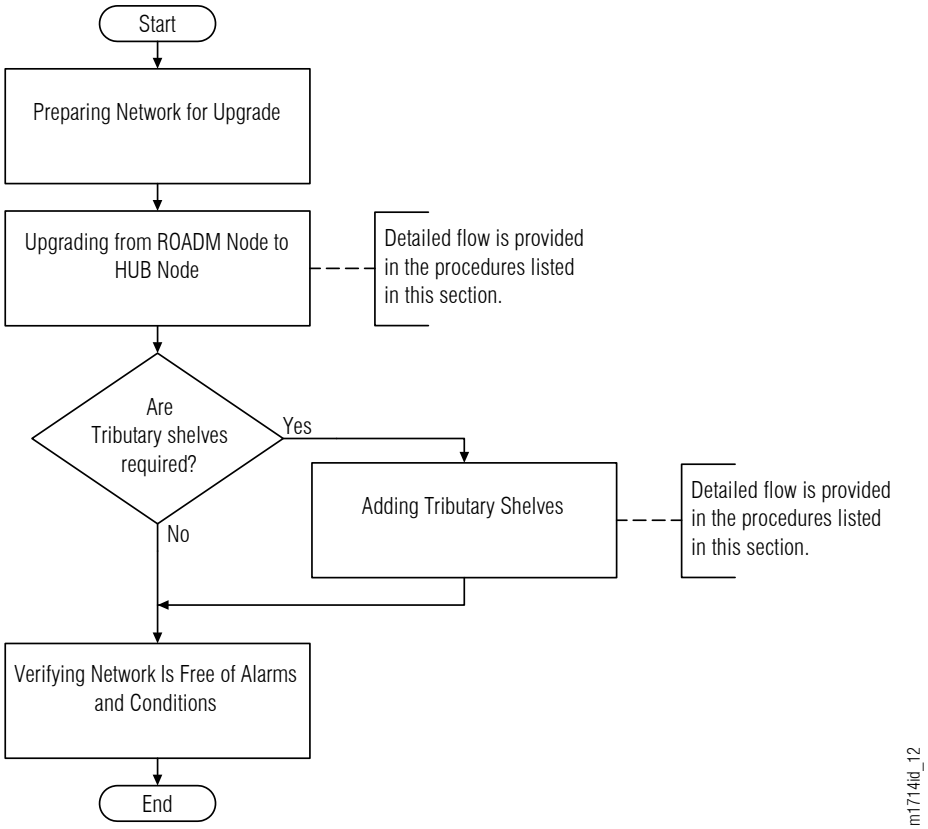


Figure 305: Upgrading ROADM Node to HUB Node (Procedural Flowchart)

The FLASHWAVE 7500 Core Configuration supports HUB nodes which include more than one Optical shelf. HUB nodes are typically used to interconnect rings and to route traffic from one ring to another within the optical domain.

The degree of connectivity of a HUB node is defined as the number of network connections to the node. The following figure illustrates the concept of degrees of connectivity. For example, a ROADM node is a two-degree node, and a HUB node that is part of two interconnected rings is a 4-degree node. The Core Configuration

supports up to an eight degree symmetric HUB node. The Core Configuration also supports asymmetric HUB nodes that allow up to 12 degrees of connectivity.

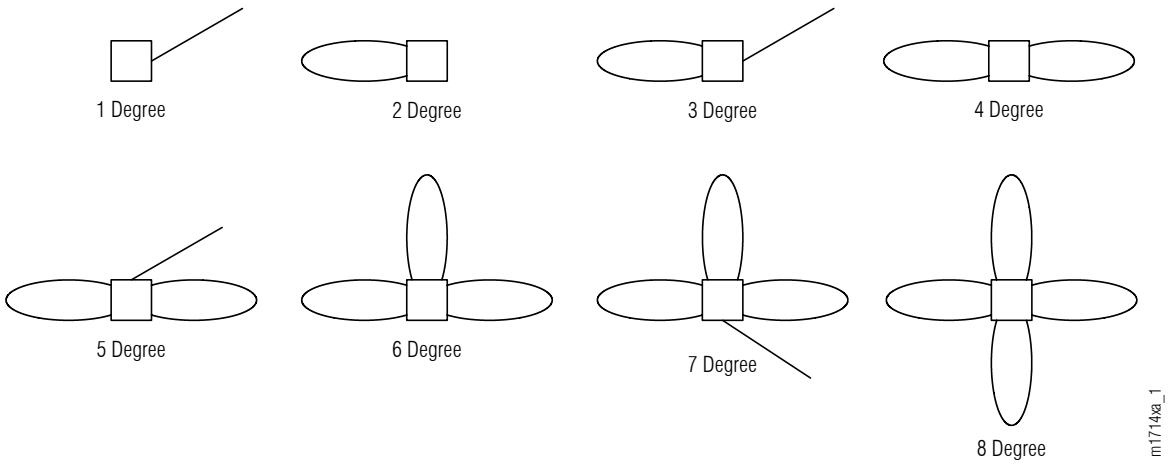


Figure 306: Degrees of Connectivity (Core Configuration, HUB Node)

For more information on HUB applications, refer to Core, Small, and ETSI Configuration Applications.

Attention: *Before adding shelves or services, ensure that all prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

8.9.1 Preparing Network for Upgrade

Prepare the node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	
	Comm. Port: COMx (for example, COM2)
	
	Configure: use default[88]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 2

At each node, retrieve alarms and conditions.

[88] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Upgrading from ROADM Node to HUB Node.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Upgrading from ROADM Node to HUB Node.

8.9.2 Upgrading from ROADM Node to HUB Node

The procedures related to the upgrade from ROADM node to HUB node are given in Introduction to Equipment Installation and Introduction to System Turn-Up Core Configuration. The following table lists the procedures in the order in which they are completed.

Step 1
Follow the procedures listed in the following table to upgrade from ROADM Node to HUB Node.

Table 126: Upgrade Procedures–ROADM Node to HUB Node

Task	Practice and Section
Install Auxiliary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAS shelf.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install DCM shelf.	Installing the 23-Inch DCM Shelf

Table 126: Upgrade Procedures–ROADM Node to HUB Node (Cont.)

Task	Practice and Section
Install power, ground, and alarm cables to Auxiliary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Auxiliary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Install RICC cable to Auxiliary shelf.	Installing RICC Cable (Optical Shelf)
Verify shelf labeling and intershelf connections.	Verify Shelf Labeling Verify LAN Connections Verify RICC Connections
Create Auxiliary shelf and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision Auxiliary shelf equipment and facilities.	Provision Optical Shelf Equipment and Facilities
Install intrashelf fiber-optic cables.	Install Intrashelf Fiber-Optic Cables
Install LAMs and MPO connections.	Install LAMs and MPO Connections
Connect DCMs or install loopback cables.	Connect DCMs or Install Loopback Cables
Interconnect optical shelves.	Provision HUB Interconnections
Connect network fiber-optic cables.	Connect Network Fiber-Optic Cables

Step 2
Proceed to Adding Tributary Shelves.

8.9.3 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 127: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)

Table 127: Adding Tributary Shelf (Cont.)

Task	Practice and Section
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision synchronization and/or Tributary shelf OSC units, if required[89].	Provision Synchronization and/or Tributary Shelf OSC Units

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

8.9.4 Verifying Network Is Free of Alarms and Conditions

Step 1
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 2.

Step 2
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

[89] Refer to procedure for applicability.

8.10 Convert a Symmetric HUB Node to an Asymmetric HUB Node

In this section:

Starting with Release 6.1, the FLASHWAVE 7500 Core Configuration supports the asymmetric HUB node, which is functionally similar to, but more flexible than, the symmetric HUB node. Both versions of the HUB node (symmetric and asymmetric) use the same hardware components, but the asymmetric HUB node provides more freedom for interconnecting network degrees. Refer to Core Configuration, for more information.

Each HUB interconnection (symmetric or asymmetric) involves three components:

- Two LC-LC fiber-optic cables installed between WSS HUB Switch units (SFMA-CDC1) and WSS Core Switch units (SFMA-CMC1)
- One LAN cable installed between RICC connectors on backplane of the applicable Optical shelves
- Two equipment connections created (using the ENT-CONN-EQPT command or equivalent) to inform the system of the LC-LC fiber-optic cable connections

The conversion procedure (Converting a Symmetric HUB Node to an Asymmetric HUB Node) assumes that the node is configured as a symmetric HUB node (HUBMODE=AUTO) and may include HUB interconnections (provisioned at turn-up) that need to be preserved. When keyword HUBMODE is changed from AUTO to MANUAL (using the ED-SYS command or equivalent), the system automatically preserves existing HUB interconnections. Keyword MODE for each HUB equipment connection is automatically changed from AUTO to MAN (refer to RTRV-CONN-EQPT), but the HUB equipment connections are otherwise unchanged.

8.10.1 Converting a Symmetric HUB Node to an Asymmetric HUB Node

Convert a symmetric HUB node to an asymmetric HUB node as follows:

Step 1
If not already done, log on the node. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10 non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	
	Comm. Port: COMx (for example, COM2)
	
	Configure: use default[90]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms

Step 2
Retrieve any alarms and conditions being reported on the node.

[90] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500
RTRV-ALM-ALL:TID::CTAG; *Example:* RTRV-ALM-ALL:FUJITSU::CTAG; RTRV-COND-ALL:TID::CTAG; *Example:* RTRV-COND-ALL:FUJITSU::CTAG;	*NE* ▸ *Alarms* The Active Alarms window opens. *View* ▸ *Filter* The Alarm Filter dialog box opens. Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box. Click Close. Verify the condition in the Active Alarms window. Close the Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Change HUBMODE

Step 4
Set the value of HUBMODE to MANUAL.

TL1	NETSMART 500
ED-SYS:TID::CTAG:::HUBMODE=MANUAL; *Example:* ED-SYS:FUJITSU::CTAG:::HUBMODE=MANUAL;	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Attributes tab. Set HUBMODE to MANUAL. Click Modify. Do not close the Operations dialog box.

Step 5
Verify that HUBMODE is set to MANUAL.

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
 	
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	Verify the setting of HUBMODE.
	
	Close the Operations dialog box.

Step 6
Retrieve any alarms and conditions being reported on the node.

TL1	NETSMART 500

`RTRV-ALM-ALL:TID::CTAG;`
 	
Example:
`RTRV-ALM-ALL:FUJITSU::CTAG;`
`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 7
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 8.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 8.

Step 8
Log off the node.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	
	Click Yes to continue.

This procedure is complete.

To provision asymmetric HUB node connections, refer to Provision HUB Interconnections–Asymmetric HUB Node.

To provision multi-TID HUB connections, refer to Provision Multi-TID HUB Connection.

Clear Alarms

Step 9
Retrieve any alarms and conditions being reported on the node.

TL1	NETSMART 500

`RTRV-ALM-ALL:TID::CTAG;`
 	
Example:
`RTRV-ALM-ALL:FUJITSU::CTAG;`
`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 10
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 4.

Change HUBMODE

Step 11
Set the value of HUBMODE to MANUAL.

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::HUBMODE=MANUAL;`
 	
Example:
`ED-SYS:FUJITSU::CTAG:::HUBMODE=MANUAL;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the Attributes tab.
	Set HUBMODE to MANUAL.
	Click Modify.
	
	Do not close the Operations dialog box.

Step 12
Verify that HUBMODE is set to MANUAL.

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
 	
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	Verify the setting of HUBMODE.
	
	Close the Operations dialog box.

Step 13
Retrieve any alarms and conditions being reported on the node.

TL1	NETSMART 500

`RTRV-ALM-ALL:TID::CTAG;`
 	
Example:
`RTRV-ALM-ALL:FUJITSU::CTAG;`
`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 14
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 15.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 15.

Step 15
Log off the node.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

To provision asymmetric HUB node connections, refer to Provision HUB Interconnections–Asymmetric HUB Node.

To provision multi-TID HUB connections, refer to Provision Multi-TID HUB Connection.

✔ This procedure is complete.

9
Upgrading Nodes, Small/ETSI Configuration

In this chapter:

9.1 Node Upgrade Paths and Restrictions, Small or ETSI Configuration

This chapter describes procedures for upgrading a node within a FLASHWAVE® 7500 Small or ETSI Configuration network.

In Release 5.1, two amplifier units (APMA-M2U1 and APMA-ULU1) are introduced that allow for in-service upgrades of ILA nodes that have the amplifiers installed. Refer to APMA-xxU1 (Universal Amplifier Unit) for complete details on the APMA-xxU1 amplifiers.

In-service upgrades cannot be performed on ILA nodes that have APMA-xxC1 amplifiers installed. For detailed information on the different node applications, refer to Applications.

The following table shows the upgrade paths to follow when performing node upgrades.

Note: *The procedure in Upgrade ILA Node to 40-Ch Express Node (In-Service)–Applicable to Small and ETSI Configuration Systems applies only to systems using the APMA-xxU1 amplifier. All other procedures apply to systems using either the APMA-xxC1 amplifier or the APMA-xxU1 amplifier.*

Table 128: Node Upgrade Paths

Applicable Configurations	To Upgrade		Perform the Listed Procedures in the Order Listed
	From	To	
Upgrade Path for 32-Ch Systems			
Small Configuration	ILA Node	Express Node	Upgrade ILA Node to 32-Ch Express Node–Applicable to Small Configuration Systems
		ROADM Node	Upgrade ILA Node to 32-Ch Express Node–Applicable to Small Configuration Systems Upgrade 32-Ch Express Node to 32-Ch ROADM Node–Applicable to Small Configuration Systems
		FOADM Node	Upgrade ILA Node to 32-Ch Express Node–Applicable to Small Configuration Systems Upgrade 32-Ch Express Node to 32-Ch FOADM Node–Applicable to Small Configuration Systems
Small Configuration	Express Node	FOADM Node	Upgrade 32-Ch Express Node to 32-Ch FOADM Node–Applicable to Small Configuration Systems
		ROADM Node	Upgrade 32-Ch Express Node to 32-Ch ROADM Node–Applicable to Small Configuration Systems

Upgrade Path for 40-Ch Systems			
Small Configuration ETSI Configuration	ILA Node(in-service upgrade)	Express Node	Upgrade ILA Node to 40-Ch Express Node (In-Service)–Applicable to Small and ETSI Configuration Systems
		2D-ROADM Node	In-Service Upgrade ILA Node to 2D-ROADM Node Upgrade ILA Node to 2D-ROADM Node
		WSS Node	Upgrade ILA Node to 40-Ch Express Node (In-Service)–Applicable to Small and ETSI Configuration Systems Upgrade 40-Ch Express Node to 40-Ch WSS Node–Applicable to Small and ETSI Configuration Systems
		HUB Node	Upgrade ILA Node to 40-Ch Express Node (In-Service)–Applicable to Small and ETSI Configuration Systems[91] Upgrade 40-Ch Express Node to 40-Ch WSS Node–Applicable to Small and ETSI Configuration Systems Upgrade 40-Ch WSS Node to HUB Node–Applicable to Small and ETSI Configuration Systems

[91] This procedure is applicable only to systems using the xxU1 amplifier.

9.2
References

Throughout this chapter, some procedures refer to other documents for more detailed instructions. Be sure to review and follow the referenced procedures within these documents when applicable:

- Introduction to Equipment Installation
- Introduction to System Turn-Up Small and ETSI Configuration
- Introduction to System Operations General
- Introduction to TL1 Commands
- Introduction to Maintenance and Trouble Clearing
- *NETSMART 500 User Guide*

9.3
Upgrade ILA Node to 32-Ch Express Node
Applicable to Small Configuration Systems

In this section:

The procedural flowchart is shown in the following figure.

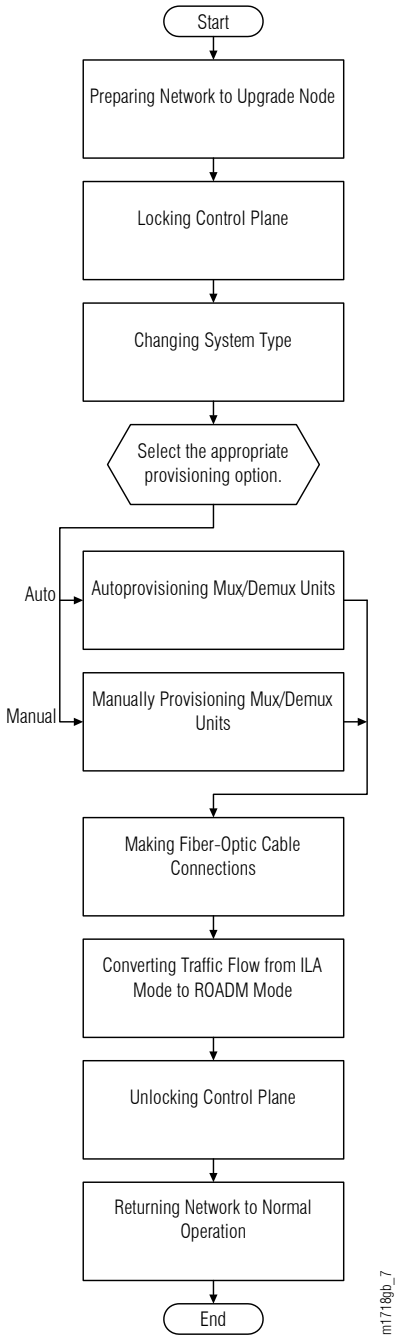


Figure 307: Upgrading ILA Node to Express Node (Procedural Flowchart)

This procedure describes how to prepare a ring network to upgrade one of the nodes in the ring from an ILA node to an Express node. This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than

four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

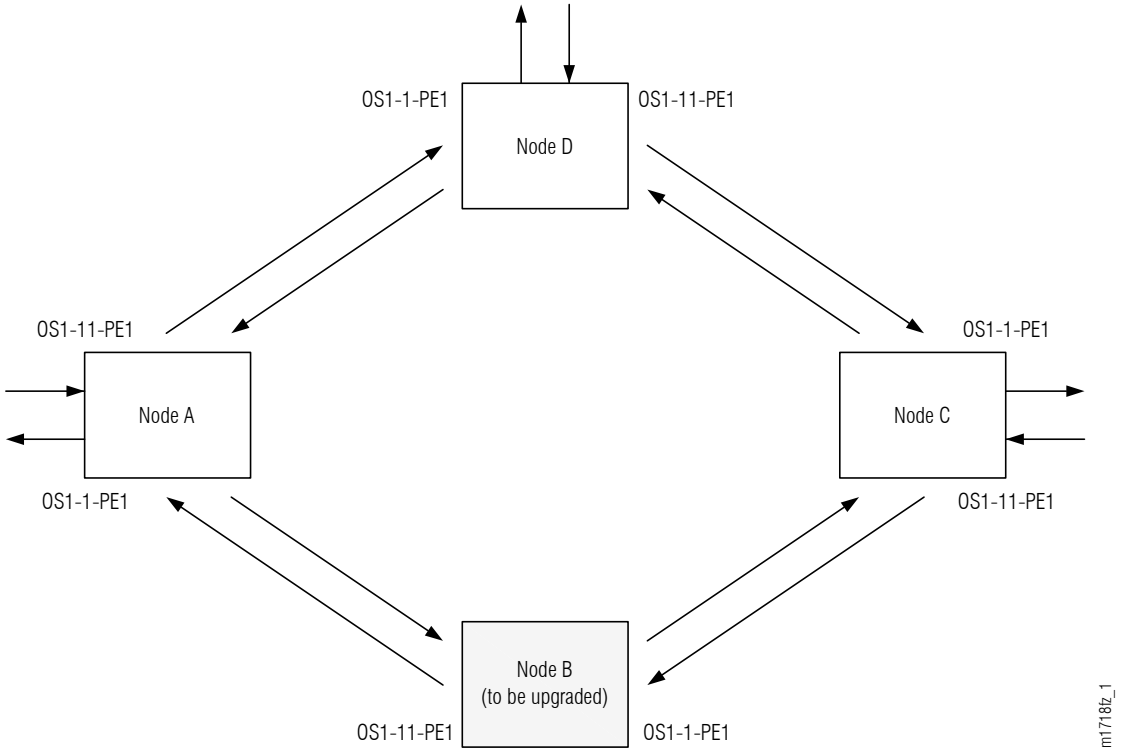


Figure 308: Ring Network Configuration

This procedure can also be used to upgrade a linear network. However, protection switching is not possible. See the following figure.

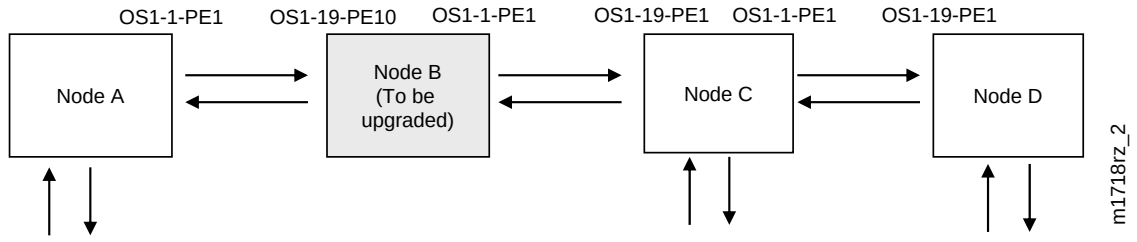


Figure 309: Linear Network Configuration

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART® 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

9.3.1 Preparing Network to Upgrade Node

Prepare the ring for the upgrade as follows:

Step 1

If not already done, log on Nodes A, B, C, and D. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to Setting Up Craft Interface (TL1 Session through TERM1) through Setting Up Craft Interface (NETSMART 500 Session through TERM2).*

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal®). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500	

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[92]
		For **TERM2** (TCP/IP):
		TID: FUJITSU
		User ID: ROOT
		Password: ROOT/(Route66K)
		Conn. Mode: TCP/IP
		IP Address: 192.168.1.1
		Port: 2024

	Click Logon. The NETSMART 500 NE View opens. The Security Message dialog box opens. Click OK. ***Note:*** *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*	

Clear Alarms and Conditions

Step 2
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

[92] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 4
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 5
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct-connect application (although it may still be protected).*

Step 6
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 7.

Step 7
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 8.

If NO:
Proceed to Step 9.

Step 8
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then proceed to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 9
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 10
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs), if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 11
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then proceed to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 12
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 13
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 14
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 129: Decision Table (Node A)

Retrieved Cross-Connect Values			Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF	Channel Number	SST	
OS1-1-PE1-c	c = 5...36	DEF	Yes
		SWITCH	No
OS1-11-PE1-c	c = 5...36	DEF	No

Table 129: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values			Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF	Channel Number	SST	
		SWITCH	Yes

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable; then proceed to Step 15.

If NO:
Proceed to Step 17.

Step 15
At Node A, for each channel identified in Step 14, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA: OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 16
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 129).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 17
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 18
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 19
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA: OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 20
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 21
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 22
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 23.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 23.

Step 23
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 14.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 24
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 25
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 26
Are any dropped channels currently taking traffic from OS1-11-PE1 (refer to the following table)?

Table 130: Decision Table (Node A)

Retrieved Cross-Connect Values			Is Current Traffic Dropped from OS1-11-PE1?
PSWDEF	Channel Number	SST	
OS1-1-PE1-c	c = 5…36	DEF	No
		SWITCH	Yes
OS1-11-PE1-c	c = 5…36	DEF	Yes

Table 130: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values			Is Current Traffic Dropped from OS1-11-PE1?
PSWDEF	Channel Number	SST	
		SWITCH	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable; then proceed to Step 27.

If NO:
Proceed to Step 29.

Step 27
At Node C, for each channel identified in Step 26, initiate a manual protection switch away from the OS1-11-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC: OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 28
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-11-PE1 (refer to Table 130).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 29
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 30
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 31
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-11-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-11-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC: OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 32
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 33
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 34
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 35.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 35.

Step 35
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-11-PE1.

Note: *Use the same criteria used in Step 26.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 36
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 37
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 38
For each drop cross-connect identified in Step 37, identify the ***break direction***, OS1-1-PE1 or OS1-11-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Travelling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 39
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 131: Decision Table (Node D)

Retrieved Cross-Connect Values			Break Direction[93]	Is Current Traffic Dropped from the Break Direction?
PSWDEF	Channel Number	SST		
OS1-1-PE1-c	c = 5...36	DEF	OS1-1-PE1	Yes
			OS1-11-PE1	No
		SWITCH	OS1-1-PE1	No
			OS1-11-PE1	Yes
OS1-11-PE1c	c = 5...36	DEF	OS1-1-PE1	No
			OS1-11-PE1	Yes
		SWITCH	OS1-1-PE1	Yes
			OS1-11-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs), if applicable, and then proceed to Step 40.

If NO:
Proceed to Step 42.

Step 40
At Node D, for each channel identified in Step 39, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-11-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

[93] **Refer to Step 38.**

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-11:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 41
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 131).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 42
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 43
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 44
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-11-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-11:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 45
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 46
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 47
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 48.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 48.

Step 48
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-11-PE1).

Note: *Use the same criteria used in Step 39.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 49
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 50
Proceed to Locking Control Plane.

Clear Alarms and Conditions

Step 51
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 52
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 53
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 54
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct-connect application (although it may still be protected).*

Step 55
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 56.

Step 56
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 57.

If NO:
Proceed to Step 9.

Step 57
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then proceed to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to Equipment and Facility Provisioning.*

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in Provision Pass-Through Cross-Connects for Node B, to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 58
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 59
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs), if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1…40), record the channel number c.*

Step 60
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then proceed to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 61
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 62
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**DEF** or **SWITCH**) indicates whether the preferred path is currently used (**DEF**) or not (**SWITCH**).*

Step 63
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 132: Decision Table (Node A)

Retrieved Cross-Connect Values			Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF	Channel Number	SST	
OS1-1-PE1-c	c = 5...36	DEF	Yes
		SWITCH	No
OS1-11-PE1-c	c = 5...36	DEF	No
		SWITCH	Yes

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable; then proceed to Step 64.

If NO:
Proceed to Step 66.

Step 64
At Node A, for each channel identified in Step 63, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA: OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 65
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 132).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
   TID DATE TIME
M CTAG COMPLD
   "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 66
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 67
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 68
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA: OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 69
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 70
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 71
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 72.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 72.

Step 72
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 14.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 73
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
   TID DATE TIME
M CTAG COMPLD
   "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 74
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 75
Are any dropped channels currently taking traffic from OS1-11-PE1 (refer to the following table)?

Table 133: Decision Table (Node A)

Retrieved Cross-Connect Values			Is Current Traffic Dropped from OS1-11-PE1?
PSWDEF	Channel Number	SST	
OS1-1-PE1-c	c = 5...36	DEF	No
		SWITCH	Yes
OS1-11-PE1-c	c = 5...36	DEF	Yes
		SWITCH	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs) if applicable; then proceed to Step 76.

If NO:
Proceed to Step 78.

Step 76
At Node C, for each channel identified in Step 75, initiate a manual protection switch away from the OS1-11-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC: OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 77
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-11-PE1 (refer to Table 133).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
   TID DATE TIME
M CTAG COMPLD
   "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 78
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 79
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 80
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-11-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-11-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC: OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 81
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 82
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 83
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 84.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 84.

Step 84
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-11-PE1.

Note: *Use the same criteria used in Step 26.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 85
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
   TID DATE TIME
M CTAG COMPLD
   "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 86
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 87
For each drop cross-connect identified in Step 86, identify the ***break direction***, OS1-1-PE1 or OS1-11-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is* ***not*** *the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Travelling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 88
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 134: Decision Table (Node D)

Retrieved Cross-Connect Values			Break Direction[94]	Is Current Traffic Dropped from the Break Direction?
PSWDEF	Channel Number	SST		
OS1-1-PE1-c	c = 5...36	DEF	OS1-1-PE1	Yes
			OS1-11-PE1	No
		SWITCH	OS1-1-PE1	No
			OS1-11-PE1	Yes
OS1-11-PE1c	c = 5...36	DEF	OS1-1-PE1	No
			OS1-11-PE1	Yes
		SWITCH	OS1-1-PE1	Yes
			OS1-11-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs), if applicable, and then proceed to Step 89.

If NO:
Proceed to Step 91.

Step 89
At Node D, for each channel identified in Step 88, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-11-PE1).

[94] **Refer to Step 87.**

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-11:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 90
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 134).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 91
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 92
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 93
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-11-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-11:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 94
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 95
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 96
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 97.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 97.

Step 97
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-11-PE1).

Note: *Use the same criteria used in Step 39.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 98
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 99
Proceed to Locking Control Plane.

✔ This procedure is complete.

9.3.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
 	
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the Control Plane tab.
	
	For the LOCK command parameter, click Yes.
	Click Modify.
	
	The Confirmation dialog box opens.
	Click OK.
	
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
 	
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

9.3.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_S_ILA to FW7500U_S.

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_S_ILA to FW7500U_S.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_S;`
Example:
`ED-SYS:FUJITSU::CTAG:::TYPE=FW7500U_S;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_S.
	• Click Modify.
	The Confirmation dialog box opens.
	Click YES.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

Step 5
Verify that the system type is FW7500U_S.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 6
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning Mux/Demux Units.
- For manual provisioning, proceed to Manually Provisioning Mux/Demux Units.

9.3.4 Autoprovisioning Mux/Demux Units

The Mux/Demux unit (MDXP-MDC3) unit can be autoprovisioned as described in Autoprovision Optical/ILA Shelf Equipment and Facilities.

Note: *For Mux/Demux unit slot locations, refer to* Slot Labels and AIDs.

Note: *All equipment except shelves can be autoprovisioned. Shelves require manual provisioning to be placed in service.*

Step 1
Using the procedure in Autoprovision Optical/ILA Shelf Equipment and Facilities, install and provision the Mux/Demux unit.

Step 2
Proceed to Making Fiber-Optic Cable Connections.

9.3.5 Manually Provisioning Mux/Demux Units

The Mux/Demux units (MDXP-MDC3) can be manually provisioned as described in Manually Provision Optical/ILA Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit will assume the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical/ILA Shelf Equipment, install and manually provision the Mux/Demux unit.

Step 2
Proceed to Making Fiber-Optic Cable Connections.

9.3.6
Making Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figures shows the fiber-optic cable connections before the upgrade.

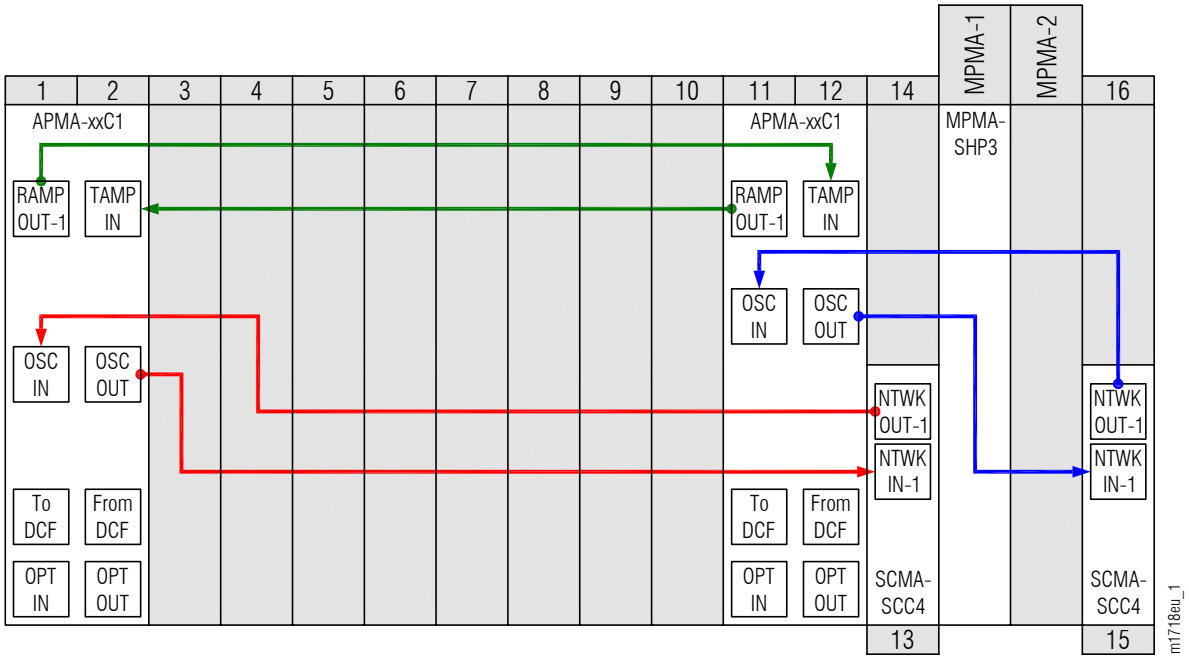


Figure 310: Cabling Before Upgrade (ILA Node)

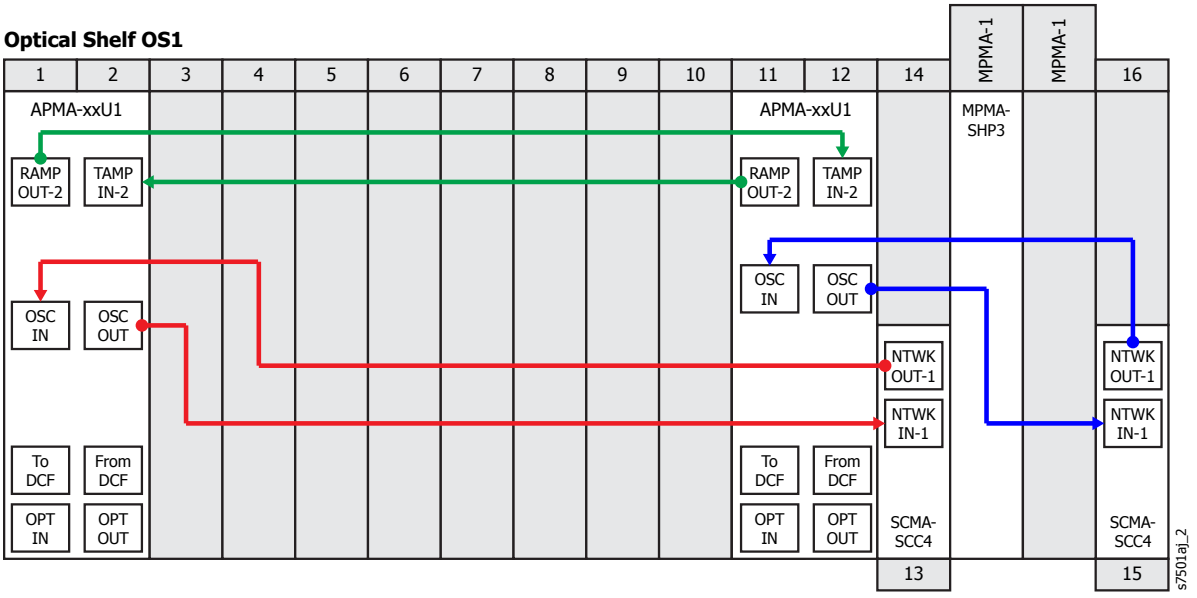


Figure 311: Cabling Before Upgrade (ILA Node with M2U1 and/or ULU1)

The following figures shows the fiber-optic cable connections after the upgrade is complete.

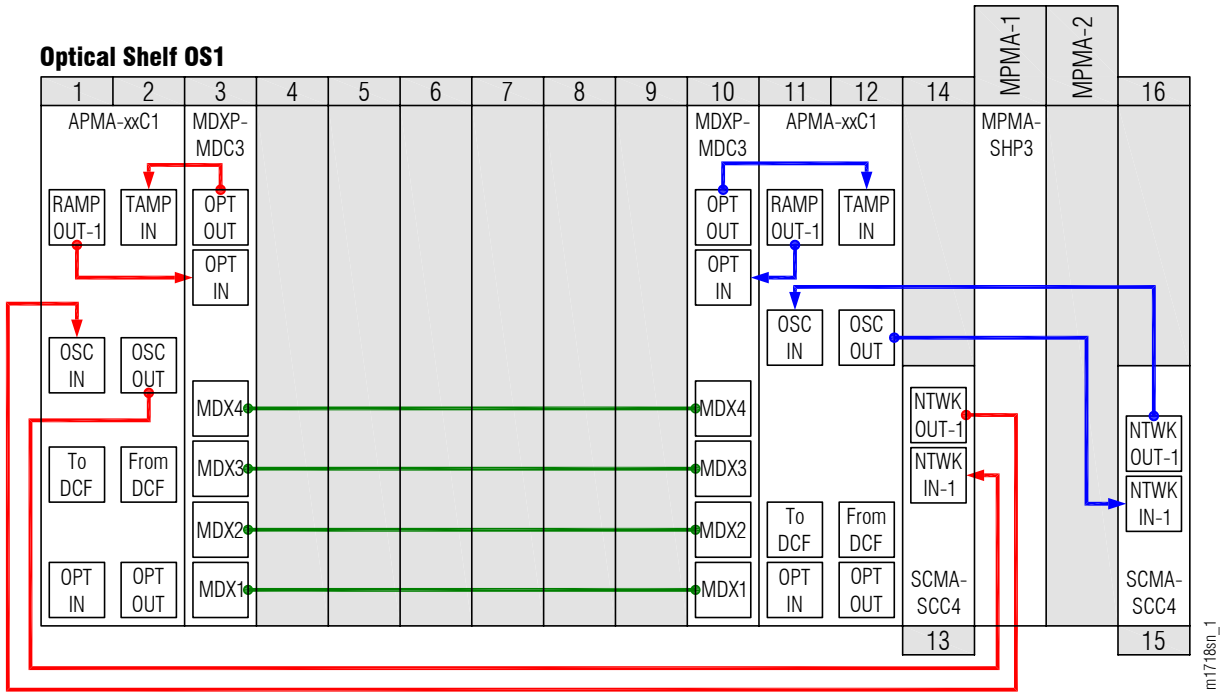


Figure 312: Cabling After Upgrade (Express Node)

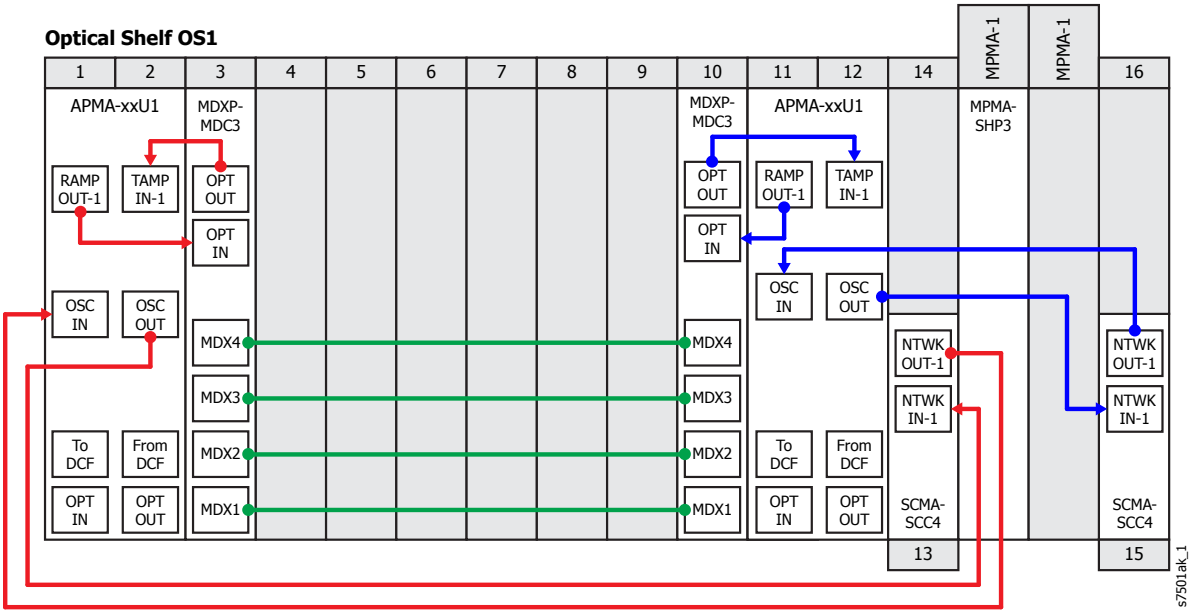


Figure 313: Cabling After Upgrade (Express node with M2U1 or ULU1)

Note: Figure 313 *is applicable to APMA-M2U1 Issue 3 and earlier or APMA-ULU1 Issue 5 and earlier.*

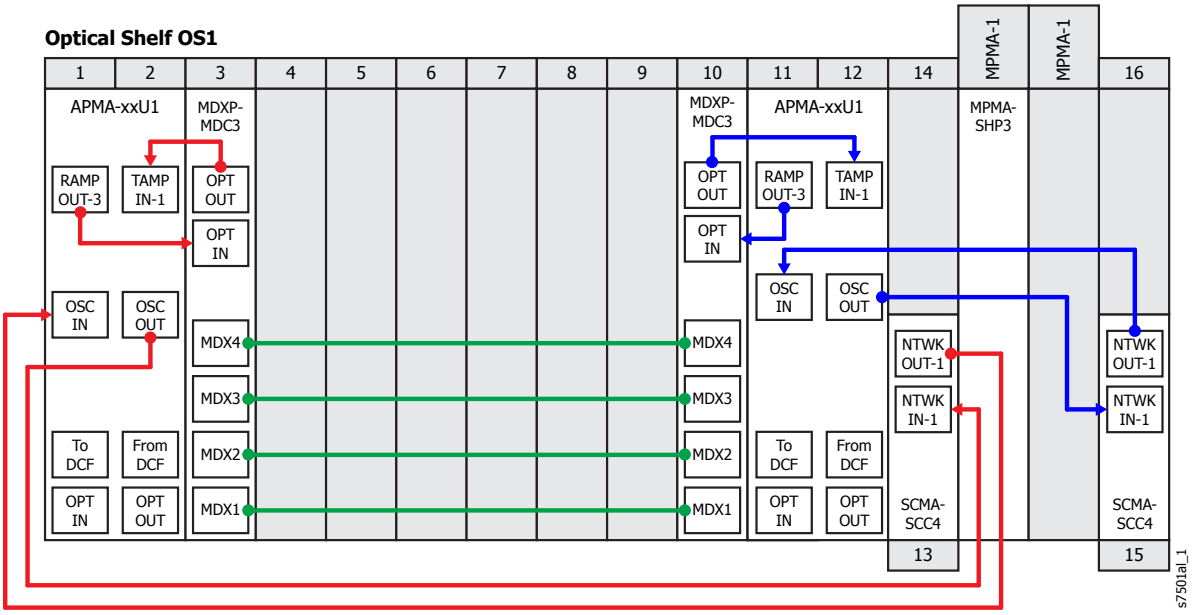


Figure 314: Cabling After Upgrade (Express node with M2U1 or ULU1)

Note: Figure 314 *is applicable to APMA-M2U1 Issue 4 and later or APMA-ULU1 Issue 6 and later.*

Change fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Remove Pass-Through Connections between Amplifiers

Step 1

Disconnect and remove the two pass-through cables connecting the amplifier plug-in units. These cables are shown in the following figure and listed in the following table.

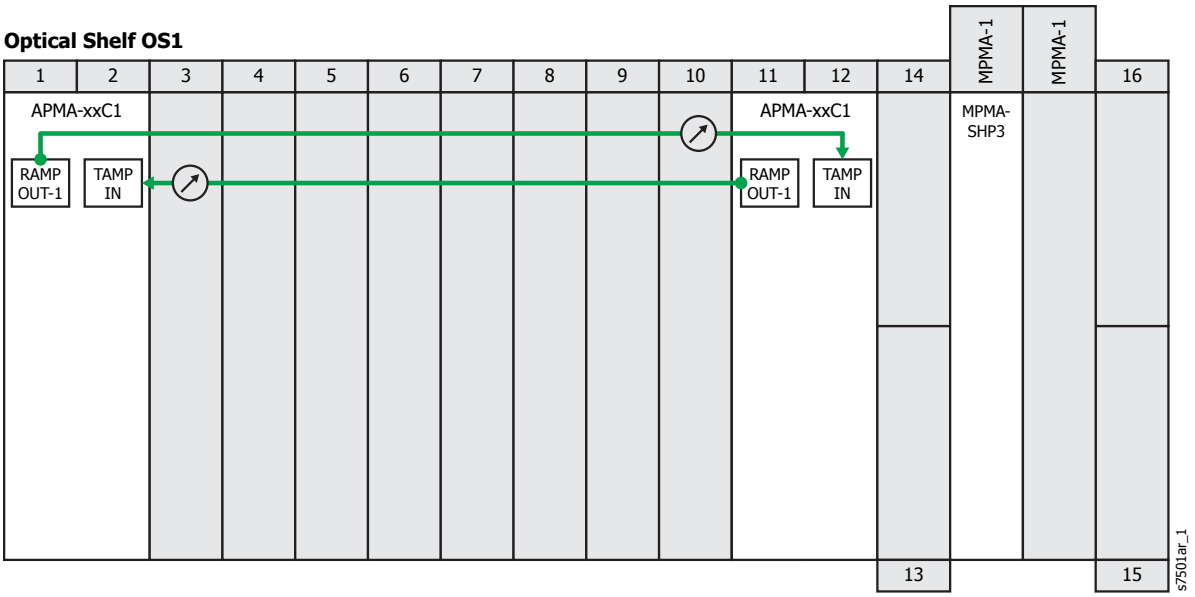


Figure 315: Pass-Through Connections between Amplifiers

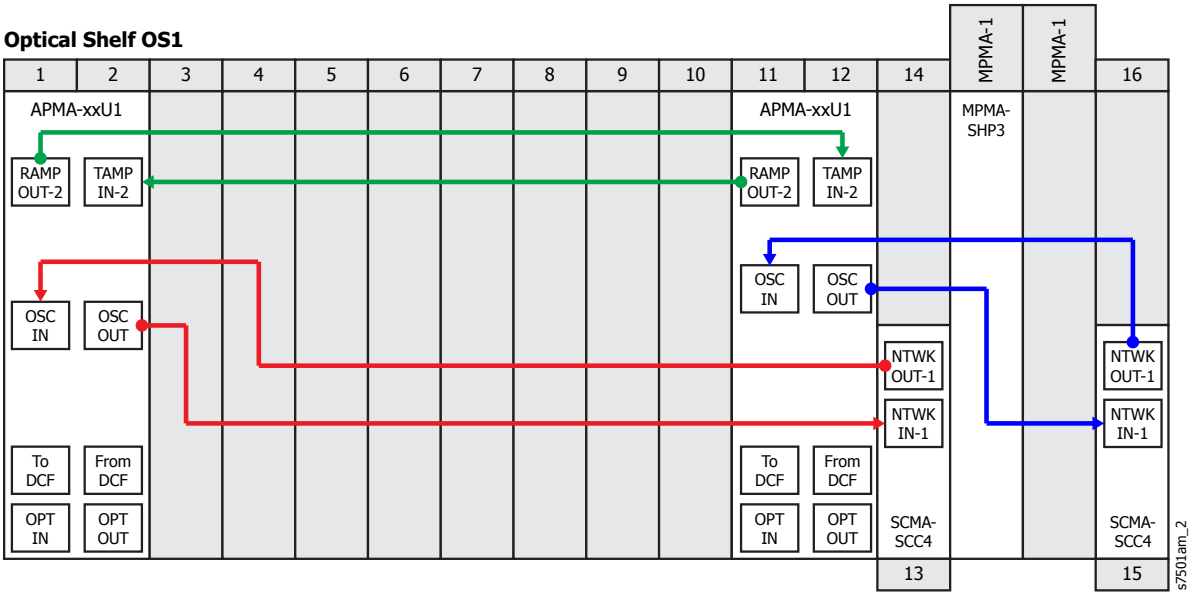


Figure 316: Pass-Through Connections between Amplifiers

Table 135: Pass-Through Connections between Amplifiers

From Amplifier (APMA-xxx1)		To Amplifiers (APMA-xxx1)	
Shelf Slot	**Connector**	**Shelf Slot**	**Connector**
1	RAMP OUT-1 (APMA-xxC1)	11	TAMP IN
	RAMP OUT-2 (APMA-xxU1)		TAMP IN-2
1	TAMP IN (APMA-xxC1)	11	RAMP OUT-1
	TAMP IN-2 (APMA-xxU1)		RAMP OUT-2

Step 2
Are the amplifier units APMA-xxC1 amplifiers?

If YES:
Remove the 14 dB optical attenuators from the TAMP IN connectors of the two amplifier plug-in units. These attenuators are shown in Figure 315.

If NO:
Go to Step 3.

Install Mux/Demux Connections to Amplifier in Slot 1

Step 3
Obtain and clean two LC-LC fiber-optic cables. Refer to Fiber Cable Handling.

Step 4
Connect the cable ends to the appropriate plug-in units and connectors as shown in the following figures and listed in the following table.

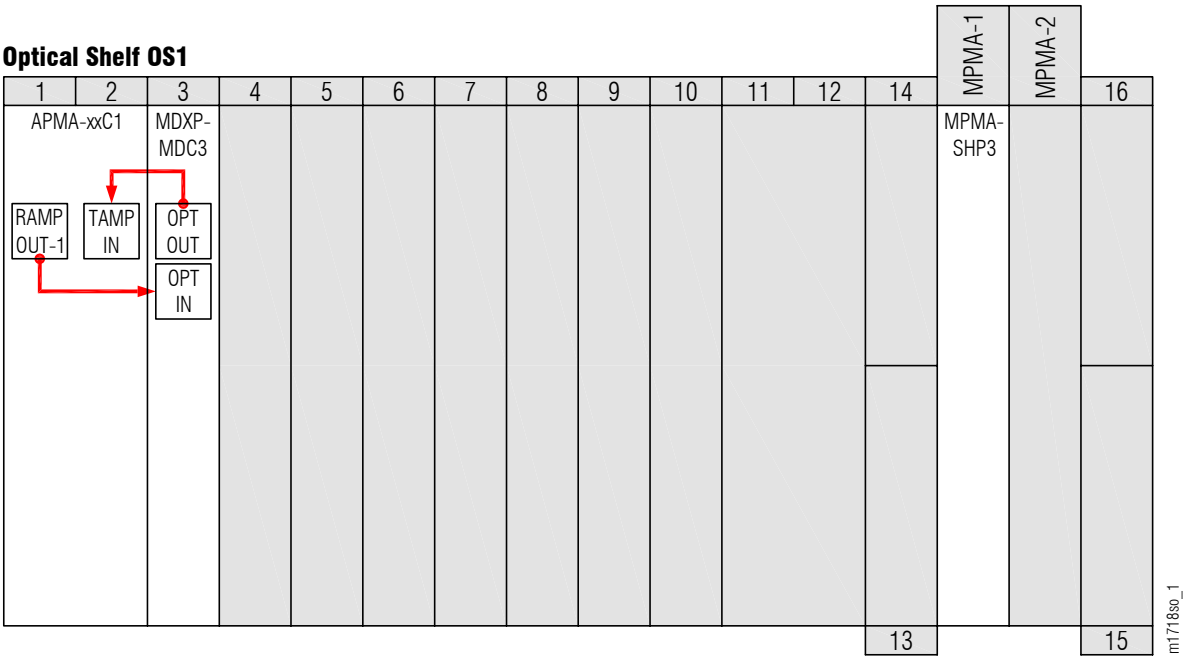


Figure 317: Mux/Demux Connections to Amplifier in Slot 1

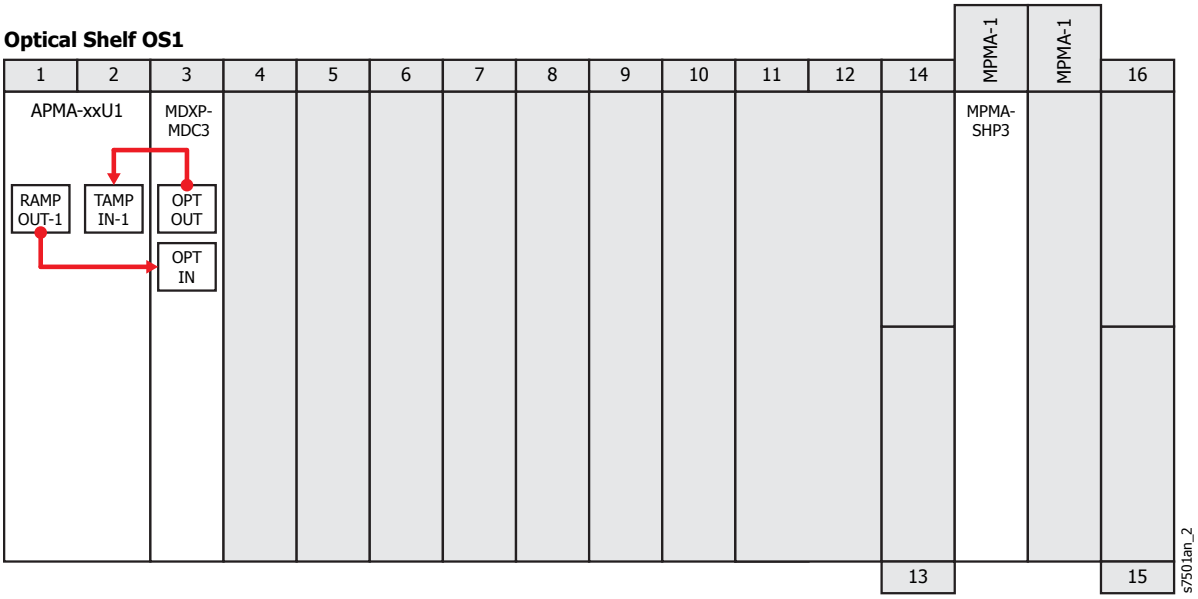


Figure 318: Mux/Demux Connections to Amplifier in Slot 1

Note: Figure 318 *is applicable to APMA-M2U1 Issue 3 and earlier or APMA-ULU1 Issue 5 and earlier.*

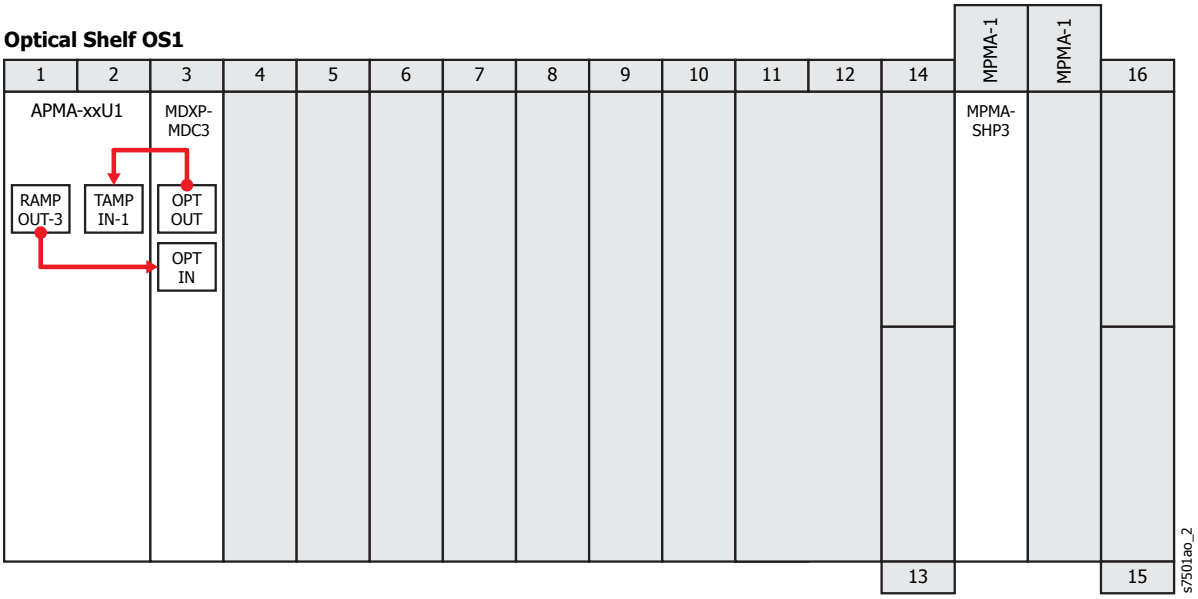


Figure 319: Mux/Demux Connections to Amplifier in Slot 1

Note: Figure 319 *is applicable to APMA-M2U1 Issure 4 and later or APMA-ULU1 Issue 6 and later.*

Table 136: Mux/Demux Connections to Amplifier in Slot 1

From Amplifier (APMA-xxx1)		To Mux/Demux (MDXP-MDC3)	
Shelf Slot	**Connector**	**Shelf Slot**	**Connector**
1	RAMP OUT-1	3	OPT IN
	RAMP OUT-3[95]		
1	TAMP IN (APMA-xxC1)	3	OPT OUT
	TAMP IN-1 (APMA-xxU1)		

Install Mux/Demux Connections to Amplifier in Slot 11

Step 5
Obtain and clean two LC-LC fiber-optic cables. Refer to Fiber Cable Handling.

Step 6
Connect the cable ends to the appropriate plug-in units and connectors as shown in the following figure and listed in the following table.

[95] If using Issue 4 and higher of the APMA-M2U1 or Issue 6 and higher of the APMA-ULU1 unit for the Small 32-channel FOADM configuration, use connector RAMP OUT-3 in place of connector RAMP OUT-1.

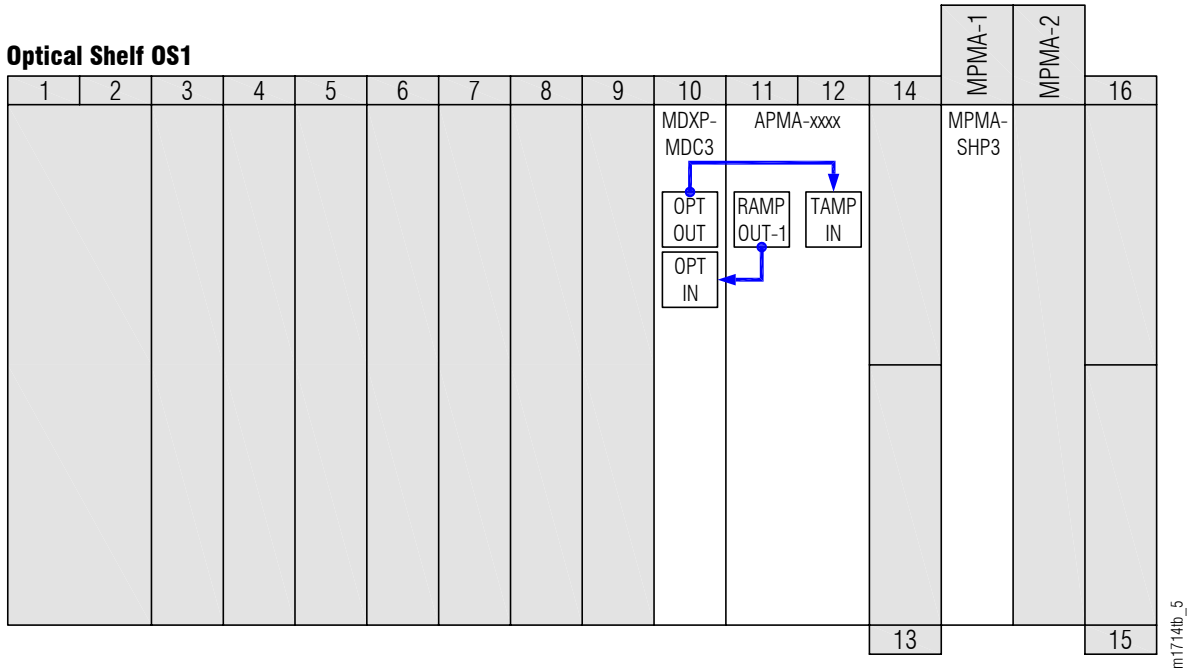


Figure 320: Mux/Demux Connections to Amplifier in Slot 11

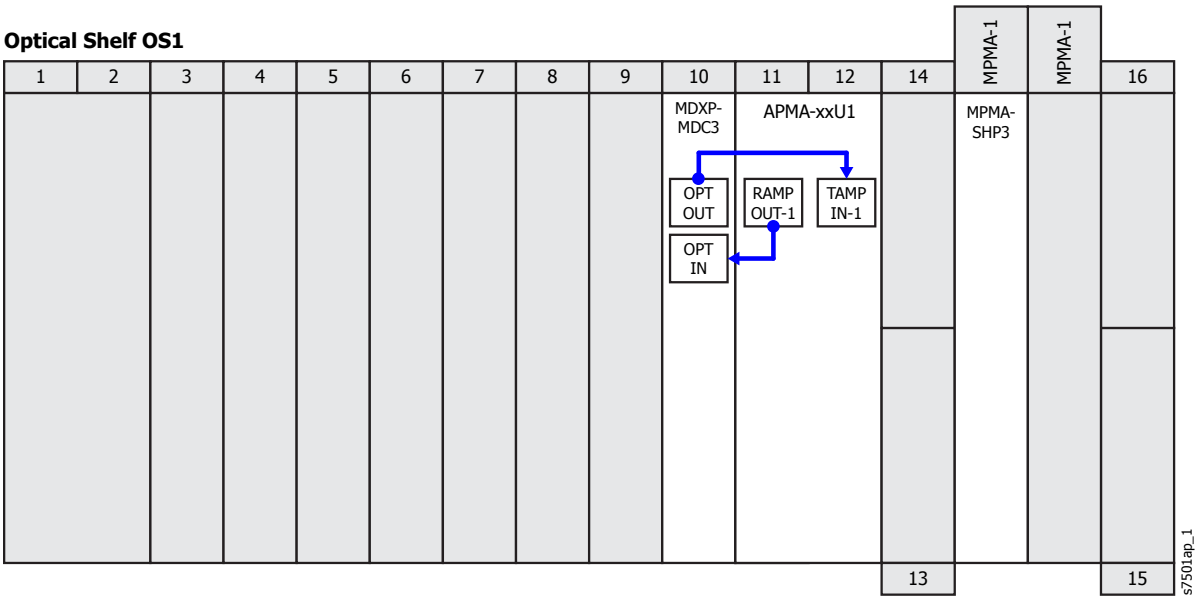


Figure 321: Mux/Demux Connections to Amplifier in Slot 11

Note: Figure 321 *is applicable to APMA-M2U1 Issue 3 and earlier or APMA-ULU1 Issue 5 and earlier.*

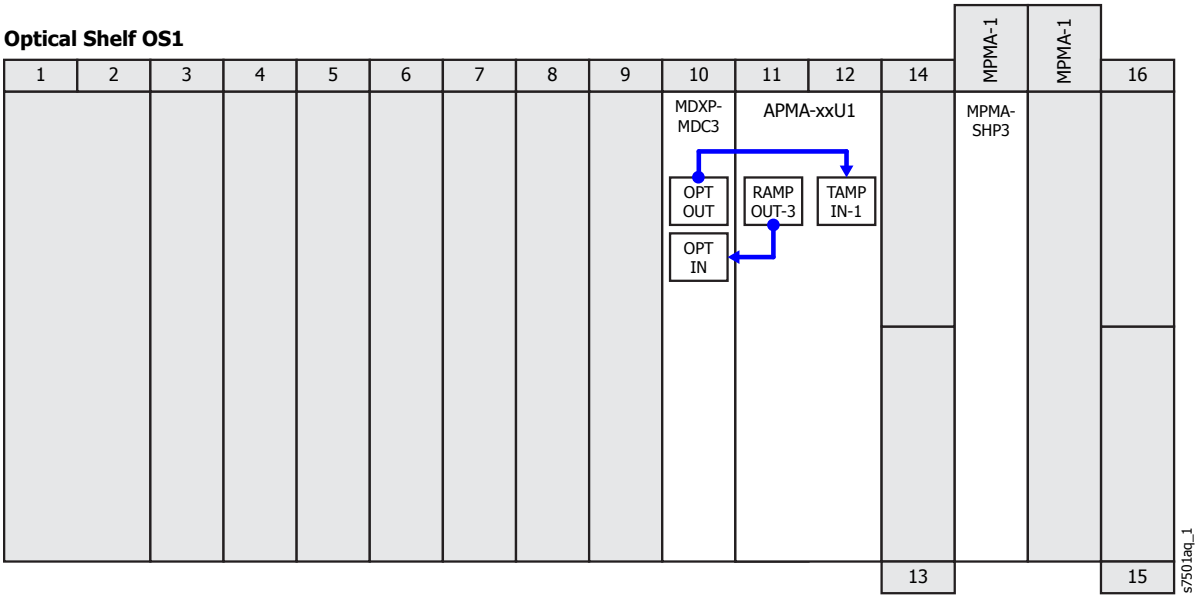


Figure 322: Mux/Demux Connections to Amplifier in Slot 11

Note: Figure 322 *is applicable to APMA-M2U1 Issue 4 and later or APMA-ULU1 Issue 6 and later.*

Table 137: Mux/Demux Connections to Amplifier in Slot 11

From Amplifier (APMA-xxx1)		To Mux/Demux (MDXP-MDC3)	
Shelf Slot	**Connector**	**Shelf Slot**	**Connector**
11	RAMP OUT-1	10	OPT IN
	RAMP OUT-3[96]		
11	TAMP IN (APMA-xxC1)	10	OPT OUT
	TAMP IN-1 (APMA-xxU1)		

Install Pass-Through Cables between Mux/Demux Units

Step 7
Obtain and clean the four MPO-MPO (16- or 24-fiber) fiber-optic cables. Refer to Fiber Cable Handling.

Step 8
Connect the cable ends to the appropriate plug-in units and connectors as shown in the following figure and listed in the following table.

[96] If using Issue 4 and higher of the APMA-M2U1 or Issue 6 and higher of the APMA-ULU1 unit for the Small 32-channel FOADM configuration, use connector RAMP OUT-3 in place of connector RAMP OUT-1.

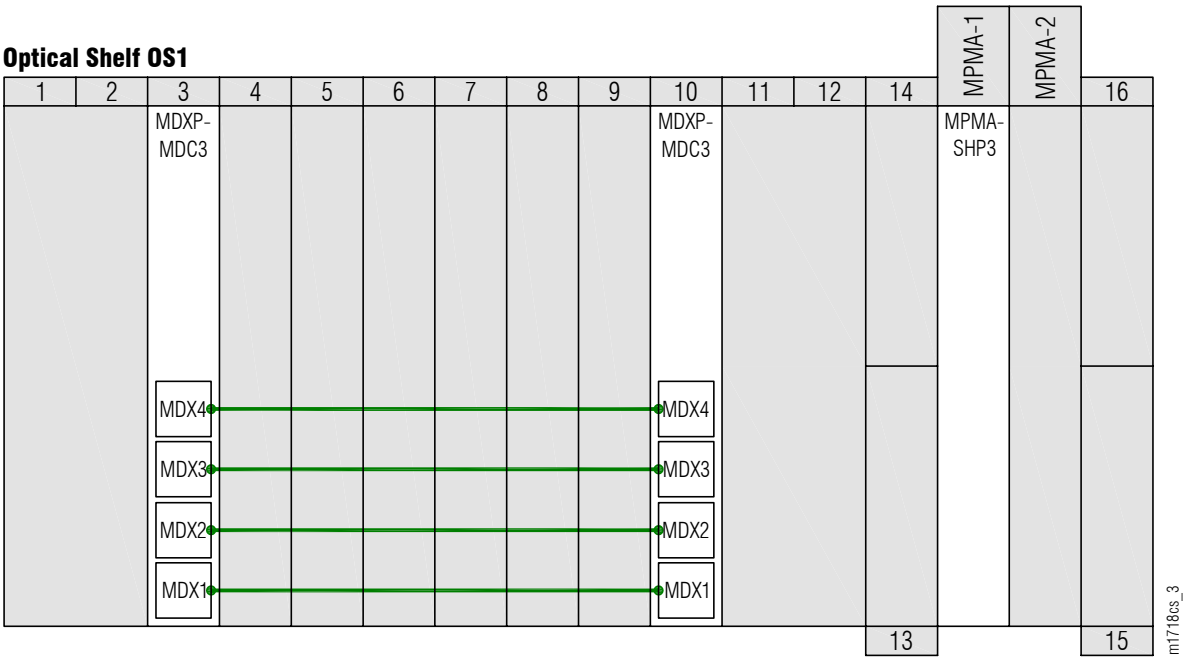


Figure 323: Pass-Through Cable Connections for Express Node

Table 138: Pass-Through Cable Connections–Express Node Application

Cable	From MDXP-MDC3		To MDXP-MDC3	
	Slot	Connector	Slot	Connector
1	3	MDX1	10	MDX1
2		MDX2		MDX2
3		MDX3		MDX3
4		MDX4		MDX4

Step 9
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode .

✔ This procedure is complete.

9.3.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the system from the ILA mode (amplifier to amplifier pass-through traffic flow) to the ROADM mode.

Note: *The mode conversion for APMA-xxC1 amplifiers is always forced (MODE=OVRD). Refer to* Converting Traffic Flow from ILA Mode to ROADM Mode *for more information.*

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=OVRD;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=OVRD;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select OVRD from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

The CONVIP condition clears when the conversion completes.

Step 3
Proceed to Unlocking Control Plane.

9.3.8 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Returning Network to Normal Operation.

9.3.9 Returning Network to Normal Operation

This procedure returns the ring network to normal operation.

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

To release protection switches and verify that the network is free of alarms and conditions, perform the following steps:

Note: *Perform Steps 11 through 20 for each node in the ring network.*

Step 1
If not already done, log on Nodes A, B, C, and D (refer to Step 1 in Preparing Network for Upgrade). If already logged on, proceed to the next step.

Provision Pass-Through Cross-Connects for Node B

Tables 139 through 140 list the equipment connection AIDs and the WCH cross-connect AIDs needed to pass through each WDM channel between WDM facilities in an Express application.

Table 139: Pass-Through Connections from WDM Facility OS1-1-PE1 to OS1-11-PE1 (Express Application)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
5	OS1-3-PC1	OS1-10-PC1	OS1-1-PE1-5	OS1-11-PE1-5
7	OS1-3-PC2	OS1-10-PC2	OS1-1-PE1-7	OS1-11-PE1-7
9	OS1-3-PC3	OS1-10-PC3	OS1-1-PE1-9	OS1-11-PE1-9
11	OS1-3-PC4	OS1-10-PC4	OS1-1-PE1-11	OS1-11-PE1-11
13	OS1-3-PC5	OS1-10-PC5	OS1-1-PE1-13	OS1-11-PE1-13
15	OS1-3-PC6	OS1-10-PC6	OS1-1-PE1-15	OS1-11-PE1-15
17	OS1-3-PC7	OS1-10-PC7	OS1-1-PE1-17	OS1-11-PE1-17
19	OS1-3-PC8	OS1-10-PC8	OS1-1-PE1-19	OS1-11-PE1-19
21	OS1-3-PC9	OS1-10-PC9	OS1-1-PE1-21	OS1-11-PE1-21
23	OS1-3-PC10	OS1-10-PC10	OS1-1-PE1-23	OS1-11-PE1-23
25	OS1-3-PC11	OS1-10-PC11	OS1-1-PE1-25	OS1-11-PE1-25
27	OS1-3-PC12	OS1-10-PC12	OS1-1-PE1-27	OS1-11-PE1-27
29	OS1-3-PC13	OS1-10-PC13	OS1-1-PE1-29	OS1-11-PE1-29
31	OS1-3-PC14	OS1-10-PC14	OS1-1-PE1-31	OS1-11-PE1-31
33	OS1-3-PC15	OS1-10-PC15	OS1-1-PE1-33	OS1-11-PE1-33

Table 139: Pass-Through Connections from WDM Facility OS1-1-PE1 to OS1-11-PE1 (Express Application) (Cont.)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
35	OS1-3-PC16	OS1-10-PC16	OS1-1-PE1-35	OS1-11-PE1-35
6	OS1-3-PC17	OS1-10-PC17	OS1-1-PE1-6	OS1-11-PE1-6
8	OS1-3-PC18	OS1-10-PC18	OS1-1-PE1-8	OS1-11-PE1-8
10	OS1-3-PC19	OS1-10-PC19	OS1-1-PE1-10	OS1-11-PE1-10
12	OS1-3-PC20	OS1-10-PC20	OS1-1-PE1-12	OS1-11-PE1-12
14	OS1-3-PC21	OS1-10-PC21	OS1-1-PE1-14	OS1-11-PE1-14
16	OS1-3-PC22	OS1-10-PC22	OS1-1-PE1-16	OS1-11-PE1-16
18	OS1-3-PC23	OS1-10-PC23	OS1-1-PE1-18	OS1-11-PE1-18
20	OS1-3-PC24	OS1-10-PC24	OS1-1-PE1-20	OS1-11-PE1-20
22	OS1-3-PC25	OS1-10-PC25	OS1-1-PE1-22	OS1-11-PE1-22
24	OS1-3-PC26	OS1-10-PC26	OS1-1-PE1-24	OS1-11-PE1-24
26	OS1-3-PC27	OS1-10-PC27	OS1-1-PE1-26	OS1-11-PE1-26
28	OS1-3-PC28	OS1-10-PC28	OS1-1-PE1-28	OS1-11-PE1-28
30	OS1-3-PC29	OS1-10-PC29	OS1-1-PE1-30	OS1-11-PE1-30
32	OS1-3-PC30	OS1-10-PC30	OS1-1-PE1-32	OS1-11-PE1-32
34	OS1-3-PC31	OS1-10-PC31	OS1-1-PE1-34	OS1-11-PE1-34
36	OS1-3-PC32	OS1-10-PC32	OS1-1-PE1-36	OS1-11-PE1-36

Table 140: Pass-Through Connections from WDM Facility OS1-11-PE1 to OS1-1-PE1 (Express Application)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
5	OS1-10-PC1	OS1-3-PC1	OS1-11-PE1-5	OS1-1-PE1-5
7	OS1-10-PC2	OS1-3-PC2	OS1-11-PE1-7	OS1-1-PE1-7

Table 140: Pass-Through Connections from WDM Facility OS1-11-PE1 to OS1-1-PE1 (Express Application) (Cont.)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
9	OS1-10-PC3	OS1-3-PC3	OS1-11-PE1-9	OS1-1-PE1-9
11	OS1-10-PC4	OS1-3-PC4	OS1-11-PE1-11	OS1-1-PE1-11
13	OS1-10-PC5	OS1-3-PC5	OS1-11-PE1-13	OS1-1-PE1-13
15	OS1-10-PC6	OS1-3-PC6	OS1-11-PE1-15	OS1-1-PE1-15
17	OS1-10-PC7	OS1-3-PC7	OS1-11-PE1-17	OS1-1-PE1-17
19	OS1-10-PC8	OS1-3-PC8	OS1-11-PE1-19	OS1-1-PE1-19
21	OS1-10-PC9	OS1-3-PC9	OS1-11-PE1-21	OS1-1-PE1-21
23	OS1-10-PC10	OS1-3-PC10	OS1-11-PE1-23	OS1-1-PE1-23
25	OS1-10-PC11	OS1-3-PC11	OS1-11-PE1-25	OS1-1-PE1-25
27	OS1-10-PC12	OS1-3-PC12	OS1-11-PE1-27	OS1-1-PE1-27
29	OS1-10-PC13	OS1-3-PC13	OS1-11-PE1-29	OS1-1-PE1-29
31	OS1-10-PC14	OS1-3-PC14	OS1-11-PE1-31	OS1-1-PE1-31
33	OS1-10-PC15	OS1-3-PC15	OS1-11-PE1-33	OS1-1-PE1-33
35	OS1-10-PC16	OS1-3-PC16	OS1-11-PE1-35	OS1-1-PE1-35
6	OS1-10-PC17	OS1-3-PC17	OS1-11-PE1-6	OS1-1-PE1-6
8	OS1-10-PC18	OS1-3-PC18	OS1-11-PE1-8	OS1-1-PE1-8
10	OS1-10-PC19	OS1-3-PC19	OS1-11-PE1-10	OS1-1-PE1-10
12	OS1-10-PC20	OS1-3-PC20	OS1-11-PE1-12	OS1-1-PE1-12
14	OS1-10-PC21	OS1-3-PC21	OS1-11-PE1-14	OS1-1-PE1-14
16	OS1-10-PC22	OS1-3-PC22	OS1-11-PE1-16	OS1-1-PE1-16
18	OS1-10-PC23	OS1-3-PC23	OS1-11-PE1-18	OS1-1-PE1-18
20	OS1-10-PC24	OS1-3-PC24	OS1-11-PE1-20	OS1-1-PE1-20
22	OS1-10-PC25	OS1-3-PC25	OS1-11-PE1-22	OS1-1-PE1-22
24	OS1-10-PC26	OS1-3-PC26	OS1-11-PE1-24	OS1-1-PE1-24

Table 140: Pass-Through Connections from WDM Facility OS1-11-PE1 to OS1-1-PE1 (Express Application) (Cont.)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
26	OS1-10-PC27	OS1-3-PC27	OS1-11-PE1-26	OS1-1-PE1-26
28	OS1-10-PC28	OS1-3-PC28	OS1-11-PE1-28	OS1-1-PE1-28
30	OS1-10-PC29	OS1-3-PC29	OS1-11-PE1-30	OS1-1-PE1-30
32	OS1-10-PC30	OS1-3-PC30	OS1-11-PE1-32	OS1-1-PE1-32
34	OS1-10-PC31	OS1-3-PC31	OS1-11-PE1-34	OS1-1-PE1-34
36	OS1-10-PC32	OS1-3-PC32	OS1-11-PE1-36	OS1-1-PE1-36

Step 2
Obtain the record of pass-through channels that was recorded when performing the steps in Record Pass-Through Channels for Node B.

Note: *You will perform Steps 3 through 9 for each pass-through channel.*

Step 3
In the preceding tables, identify the rows that correspond to the pass-through channel. Refer to these rows when performing Steps 4 through 9.

Step 4
From the rows identified in Step 3, identify the fromAID and toAID for the required equipment connections.

Step 5
At Node B, enter the equipment connections.

TL1	NETSMART 500

`ENT-CONN-EQPT:TID:fromAID,toAID:CTAG;`
fromAID, toAID:
• As identified in previous step
Example:
`ENT-CONN-EQPT:FUJITSU-NODEB:OS1-3-PC1,OS1-10-PC1:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	The Cross-Connects window opens.
	From the View Rate drop-down list, select XC_EQPT.
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment associated with the fromAID.
	From a different drop-down list, select the equipment associated with the toAID.
	Click on the fromAID to begin drawing a line that represents the connection.
	Click on the toAID to terminate the line.
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	Entity ▸ *Operations Dialog*
	Click Create.
	The dashed line becomes solid.
	Close the Operations dialog box.
	Close the Cross-Connects window.

Step 6
Verify that the equipment connections were entered.

TL1	NETSMART 500

`RTRV-CONN-EQPT:TID::CTAG;`
Example:
`RTRV-CONN-EQPT:FUJITSU-NODEB::CTAG;`
	In the tree view area, select the Connection Equip. tab.
	Verify that the equipment connection is present.

Step 7
From the row identified in Step 3, identify the fromAID and toAID for the required WCH cross-connects.

Step 8
At Node B, enter the WCH pass-through cross-connects.

Note: *The channel number (c) of the toAID and fromAID must match.*

TL1	NETSMART 500

`ENT-CRS-WCH:TID:fromAID,toAID:CTAG:::KEYWORD=DOMAIN;`
 	
fromAID, toAID (valid combinations):
• OS1-1-PE1-c, OS1-11-PE1-c
• OS1-11-PE1-c, OS1-1-PE1-c
  • c = 5…36
KEYWORD=DOMAIN:
• RDLNE = Y, **N**
 	
Example:
`ENT-CRS-WCH:FUJITSU-NODEB:OS1-1-PE1-1,OS1-11-PE1-1:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	
	The Cross-Connects window opens.
	
	From the View Rate drop-down list, select XC_WCH.
	
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment or facility associated with the fromAID.
	
	From a different drop-down list, select the equipment or facility associated with the toAID.
	
	Click on the fromAID to begin drawing a line that represents the connection.
	
	Click on the toAID to terminate the line.
	
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	
	Entity ▸ *Operations Dialog*
	
	Click Create.
	The dashed line becomes solid.
	
	Close the Operations dialog box.
	
	Do not close the Cross-Connects window.

Step 9
Verify that the WCH pass-through cross-connects were entered.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID::CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB::CTAG;`
	In the Cross-Connects window, verify that the cross-connect lines are solid.
	
	Close the Cross-Connects window.

Step 10
Is another pass-through required?

If YES:
Repeat Steps 3 through 9.

If NO:
Proceed to Step 11.

Release Protection Switches

Step 11
Retrieve conditions to identify the forced protection switches.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 12
Release each forced protection switch.

TL1	NETSMART 500

`RLS-PROTNSW-WCH:TID:AID:CTAG;`
AID:
• OS1-s-PE1-c
  • s = 1, 11 (slot number)
  • c = 5…36 (channel number)
 	
Example:
`RLS-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-1:CTAG;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Release tab.
	Click Release.

Step 13
Retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 14
Identify all OCh-DPRING–protected drop cross-connects that have parameter SST=SWITCH.

Note: *The value of SST (**DEF** or **SWITCH**) indicates whether the preferred path is currently used (**DEF**) or not (**SWITCH**).*

Step 15
Do local procedures require switch back to the preferred path?

If YES:
Proceed to Step 16.

If NO:
Proceed to Step 20.

Step 16
For each channel identified in Step 14, initiate a manual protection switch.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA: OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 17
At Node A, retrieve all cross-connects, and confirm that all OCh-DPRING–protected drop cross-connects are switched to the preferred path (SST=DEF).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 18
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 19
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 20.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 20.

Step 20
Repeat Steps 11 through 19 for each node in the ring network.

Verify Ring Network Is Free of Alarms and Conditions

Step 21
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 22
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 23.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 23.

Step 23
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

Provision Pass-Through Cross-Connects for Node B

Tables 141 through 142 list the equipment connection AIDs and the WCH cross-connect AIDs needed to pass through each WDM channel between WDM facilities in an Express application.

Table 141: Pass-Through Connections from WDM Facility OS1-1-PE1 to OS1-11-PE1 (Express Application)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
5	OS1-3-PC1	OS1-10-PC1	OS1-1-PE1-5	OS1-11-PE1-5
7	OS1-3-PC2	OS1-10-PC2	OS1-1-PE1-7	OS1-11-PE1-7
9	OS1-3-PC3	OS1-10-PC3	OS1-1-PE1-9	OS1-11-PE1-9
11	OS1-3-PC4	OS1-10-PC4	OS1-1-PE1-11	OS1-11-PE1-11
13	OS1-3-PC5	OS1-10-PC5	OS1-1-PE1-13	OS1-11-PE1-13
15	OS1-3-PC6	OS1-10-PC6	OS1-1-PE1-15	OS1-11-PE1-15
17	OS1-3-PC7	OS1-10-PC7	OS1-1-PE1-17	OS1-11-PE1-17
19	OS1-3-PC8	OS1-10-PC8	OS1-1-PE1-19	OS1-11-PE1-19
21	OS1-3-PC9	OS1-10-PC9	OS1-1-PE1-21	OS1-11-PE1-21
23	OS1-3-PC10	OS1-10-PC10	OS1-1-PE1-23	OS1-11-PE1-23
25	OS1-3-PC11	OS1-10-PC11	OS1-1-PE1-25	OS1-11-PE1-25
27	OS1-3-PC12	OS1-10-PC12	OS1-1-PE1-27	OS1-11-PE1-27
29	OS1-3-PC13	OS1-10-PC13	OS1-1-PE1-29	OS1-11-PE1-29
31	OS1-3-PC14	OS1-10-PC14	OS1-1-PE1-31	OS1-11-PE1-31
33	OS1-3-PC15	OS1-10-PC15	OS1-1-PE1-33	OS1-11-PE1-33
35	OS1-3-PC16	OS1-10-PC16	OS1-1-PE1-35	OS1-11-PE1-35
6	OS1-3-PC17	OS1-10-PC17	OS1-1-PE1-6	OS1-11-PE1-6
8	OS1-3-PC18	OS1-10-PC18	OS1-1-PE1-8	OS1-11-PE1-8
10	OS1-3-PC19	OS1-10-PC19	OS1-1-PE1-10	OS1-11-PE1-10
12	OS1-3-PC20	OS1-10-PC20	OS1-1-PE1-12	OS1-11-PE1-12
14	OS1-3-PC21	OS1-10-PC21	OS1-1-PE1-14	OS1-11-PE1-14

Table 141: Pass-Through Connections from WDM Facility OS1-1-PE1 to OS1-11-PE1 (Express Application) (Cont.)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
16	OS1-3-PC22	OS1-10-PC22	OS1-1-PE1-16	OS1-11-PE1-16
18	OS1-3-PC23	OS1-10-PC23	OS1-1-PE1-18	OS1-11-PE1-18
20	OS1-3-PC24	OS1-10-PC24	OS1-1-PE1-20	OS1-11-PE1-20
22	OS1-3-PC25	OS1-10-PC25	OS1-1-PE1-22	OS1-11-PE1-22
24	OS1-3-PC26	OS1-10-PC26	OS1-1-PE1-24	OS1-11-PE1-24
26	OS1-3-PC27	OS1-10-PC27	OS1-1-PE1-26	OS1-11-PE1-26
28	OS1-3-PC28	OS1-10-PC28	OS1-1-PE1-28	OS1-11-PE1-28
30	OS1-3-PC29	OS1-10-PC29	OS1-1-PE1-30	OS1-11-PE1-30
32	OS1-3-PC30	OS1-10-PC30	OS1-1-PE1-32	OS1-11-PE1-32
34	OS1-3-PC31	OS1-10-PC31	OS1-1-PE1-34	OS1-11-PE1-34
36	OS1-3-PC32	OS1-10-PC32	OS1-1-PE1-36	OS1-11-PE1-36

Table 142: Pass-Through Connections from WDM Facility OS1-11-PE1 to OS1-1-PE1 (Express Application)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
5	OS1-10-PC1	OS1-3-PC1	OS1-11-PE1-5	OS1-1-PE1-5
7	OS1-10-PC2	OS1-3-PC2	OS1-11-PE1-7	OS1-1-PE1-7
9	OS1-10-PC3	OS1-3-PC3	OS1-11-PE1-9	OS1-1-PE1-9
11	OS1-10-PC4	OS1-3-PC4	OS1-11-PE1-11	OS1-1-PE1-11
13	OS1-10-PC5	OS1-3-PC5	OS1-11-PE1-13	OS1-1-PE1-13
15	OS1-10-PC6	OS1-3-PC6	OS1-11-PE1-15	OS1-1-PE1-15
17	OS1-10-PC7	OS1-3-PC7	OS1-11-PE1-17	OS1-1-PE1-17
19	OS1-10-PC8	OS1-3-PC8	OS1-11-PE1-19	OS1-1-PE1-19

Table 142: Pass-Through Connections from WDM Facility OS1-11-PE1 to OS1-1-PE1 (Express Application) (Cont.)

Channel	Equipment Connection		WCH Cross-Connect	
	fromAID	toAID	fromAID	toAID
21	OS1-10-PC9	OS1-3-PC9	OS1-11-PE1-21	OS1-1-PE1-21
23	OS1-10-PC10	OS1-3-PC10	OS1-11-PE1-23	OS1-1-PE1-23
25	OS1-10-PC11	OS1-3-PC11	OS1-11-PE1-25	OS1-1-PE1-25
27	OS1-10-PC12	OS1-3-PC12	OS1-11-PE1-27	OS1-1-PE1-27
29	OS1-10-PC13	OS1-3-PC13	OS1-11-PE1-29	OS1-1-PE1-29
31	OS1-10-PC14	OS1-3-PC14	OS1-11-PE1-31	OS1-1-PE1-31
33	OS1-10-PC15	OS1-3-PC15	OS1-11-PE1-33	OS1-1-PE1-33
35	OS1-10-PC16	OS1-3-PC16	OS1-11-PE1-35	OS1-1-PE1-35
6	OS1-10-PC17	OS1-3-PC17	OS1-11-PE1-6	OS1-1-PE1-6
8	OS1-10-PC18	OS1-3-PC18	OS1-11-PE1-8	OS1-1-PE1-8
10	OS1-10-PC19	OS1-3-PC19	OS1-11-PE1-10	OS1-1-PE1-10
12	OS1-10-PC20	OS1-3-PC20	OS1-11-PE1-12	OS1-1-PE1-12
14	OS1-10-PC21	OS1-3-PC21	OS1-11-PE1-14	OS1-1-PE1-14
16	OS1-10-PC22	OS1-3-PC22	OS1-11-PE1-16	OS1-1-PE1-16
18	OS1-10-PC23	OS1-3-PC23	OS1-11-PE1-18	OS1-1-PE1-18
20	OS1-10-PC24	OS1-3-PC24	OS1-11-PE1-20	OS1-1-PE1-20
22	OS1-10-PC25	OS1-3-PC25	OS1-11-PE1-22	OS1-1-PE1-22
24	OS1-10-PC26	OS1-3-PC26	OS1-11-PE1-24	OS1-1-PE1-24
26	OS1-10-PC27	OS1-3-PC27	OS1-11-PE1-26	OS1-1-PE1-26
28	OS1-10-PC28	OS1-3-PC28	OS1-11-PE1-28	OS1-1-PE1-28
30	OS1-10-PC29	OS1-3-PC29	OS1-11-PE1-30	OS1-1-PE1-30
32	OS1-10-PC30	OS1-3-PC30	OS1-11-PE1-32	OS1-1-PE1-32
34	OS1-10-PC31	OS1-3-PC31	OS1-11-PE1-34	OS1-1-PE1-34
36	OS1-10-PC32	OS1-3-PC32	OS1-11-PE1-36	OS1-1-PE1-36

Step 24
Obtain the record of pass-through channels that was recorded when performing the steps in Record Pass-Through Channels for Node B.

Note: *You will perform Steps 25 through 31 for each pass-through channel.*

Step 25
In the preceding tables, identify the rows that correspond to the pass-through channel. Refer to these rows when performing Steps 26 through 31.

Step 26
From the rows identified in Step 25, identify the fromAID and toAID for the required equipment connections.

Step 27
At Node B, enter the equipment connections.

TL1	NETSMART 500

`ENT-CONN-EQPT:TID:fromAID,toAID:CTAG;`
fromAID, toAID:
• As identified in previous step
Example:
`ENT-CONN-EQPT:FUJITSU-NODEB:OS1-3-PC1,OS1-10-PC1:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	The Cross-Connects window opens.
	From the View Rate drop-down list, select XC_EQPT.
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment associated with the fromAID.
	From a different drop-down list, select the equipment associated with the toAID.
	Click on the fromAID to begin drawing a line that represents the connection.
	Click on the toAID to terminate the line.
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	Entity ▸ *Operations Dialog*
	Click Create.
	The dashed line becomes solid.
	Close the Operations dialog box.
	Close the Cross-Connects window.

Step 28
Verify that the equipment connections were entered.

TL1	NETSMART 500

`RTRV-CONN-EQPT:TID::CTAG;`
 	
Example:
`RTRV-CONN-EQPT:FUJITSU-NODEB::CTAG;`
	In the tree view area, select the Connection Equip. tab.
	
	Verify that the equipment connection is present.

Step 29
From the row identified in Step 25, identify the fromAID and toAID for the required WCH cross-connects.

Step 30
At Node B, enter the WCH pass-through cross-connects.

Note: *The channel number (c) of the toAID and fromAID must match.*

TL1	NETSMART 500

`ENT-CRS-WCH:TID:fromAID,toAID:`
`CTAG:::KEYWORD=DOMAIN;`
 	
fromAID, toAID (valid combinations):
• OS1-1-PE1-c, OS1-11-PE1-c
• OS1-11-PE1-c, OS1-1-PE1-c
  • c = 5...36
KEYWORD=DOMAIN:
• RDLNE = Y, **N**
 	
Example:
`ENT-CRS-WCH:FUJITSU-NODEB:`
`OS1-1-PE1-1,OS1-11-PE1-1:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	
	The Cross-Connects window opens.
	
	From the View Rate drop-down list, select XC_WCH.
	
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment or facility associated with the fromAID.
	
	From a different drop-down list, select the equipment or facility associated with the toAID.
	
	Click on the fromAID to begin drawing a line that represents the connection.
	
	Click on the toAID to terminate the line.
	
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	
	Entity ▸ *Operations Dialog*
	
	Click Create.
	The dashed line becomes solid.
	
	Close the Operations dialog box.
	
	Do not close the Cross-Connects window.

Step 31
Verify that the WCH pass-through cross-connects were entered.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID::CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB::CTAG;`
	In the Cross-Connects window, verify that the cross-connect lines are solid.
	Close the Cross-Connects window.

Step 32
Is another pass-through required?

If YES:
Repeat Steps 25 through 31.

If NO:
Proceed to Step 11.

Release Protection Switches

Step 33
Retrieve conditions to identify the forced protection switches.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 34
Release each forced protection switch.

TL1	NETSMART 500

`RLS-PROTNSW-WCH:TID:AID:CTAG;`
AID:
• OS1-s-PE1-c
  • s = 1, 11 (slot number)
  • c = 5…36 (channel number)
Example:
`RLS-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-1:CTAG;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Release tab.
	Click Release.

Step 35
Retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 36
Identify all OCh-DPRING–protected drop cross-connects that have parameter SST=SWITCH.

Note: *The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 37
Do local procedures require switch back to the preferred path?

If YES:
Proceed to Step 38.

If NO:
Proceed to Step 42.

Step 38
For each channel identified in Step 36, initiate a manual protection switch.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OS1-s-PE1-c
  • s = 1, 11
  • c = 5…36 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA: OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ ***Operations Dialog***
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 39
At Node A, retrieve all cross-connects, and confirm that all OCh-DPRING–protected drop cross-connects are switched to the preferred path (SST=DEF).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ ***Properties View***
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 40
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 41
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 42.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 42.

Step 42
Repeat Steps 33 through 41 for each node in the ring network.

Verify Ring Network Is Free of Alarms and Conditions

Step 43
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 44
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 45.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 45.

Step 45
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

✔ This procedure is complete.

9.4 Upgrade 32-Ch Express Node to 32-Ch FOADM Node Applicable to Small Configuration Systems

In this section:

The procedural flowchart is shown in the following figure.

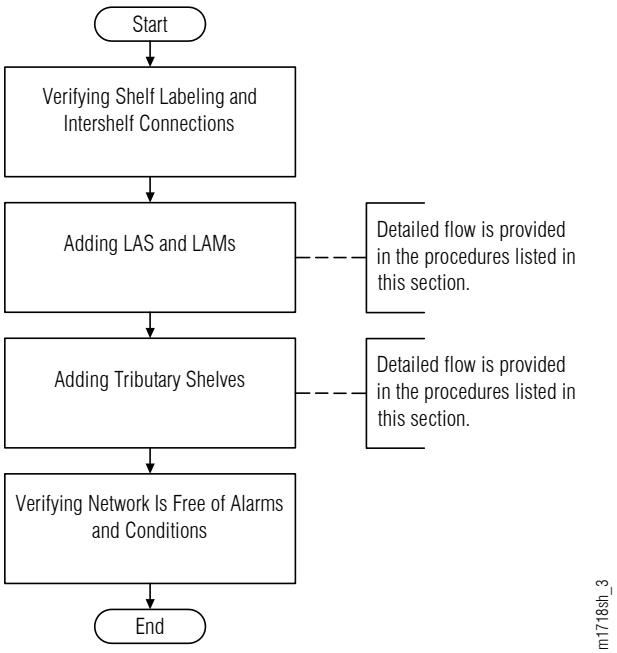


Figure 324: Upgrading Express Node to FOADM Node (Procedural Flowchart)

Attention: *Before adding shelves or services, ensure that all prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Caution: *Be sure to follow the procedures in the sequence listed.*

9.4.1 Verifying Shelf Labeling and Intershelf Connections

Use the following procedure to verify shelf labeling and intershelf connections:

Step 1
Verify the shelf labeling and intershelf connections using the procedure in Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units.

Step 2
Proceed to Adding LAS and LAMs.

9.4.2 Adding LAS and LAMs

Refer to the following table for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 143: Installing LAS and LAMs

Task	Document and Section
Install LAS shelf in rack.	Installing the LAS2 Shelf
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

9.4.3 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 144: Adding Tributary Shelves

Task	Document and Section
Install Tributary shelf in rack.	Installing the Optical/Tributary Shelf
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units
Create Tributary shelf entity and install shelf processors,	Create Subtending Shelves and Install Shelf Processors
Provision synchronization and/or Tributary shelf OSC units, if required.[97]	Provision Tributary Shelf Equipment Provision Synchronization

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

9.4.4 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify the network is free of alarms and conditions:

Step 1
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[97] Refer to procedure for applicability.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

9.5 Upgrade 32-Ch Express Node to 32-Ch ROADM Node Applicable to Small Configuration Systems

In this section:

The procedural flowchart is shown in the following figure.

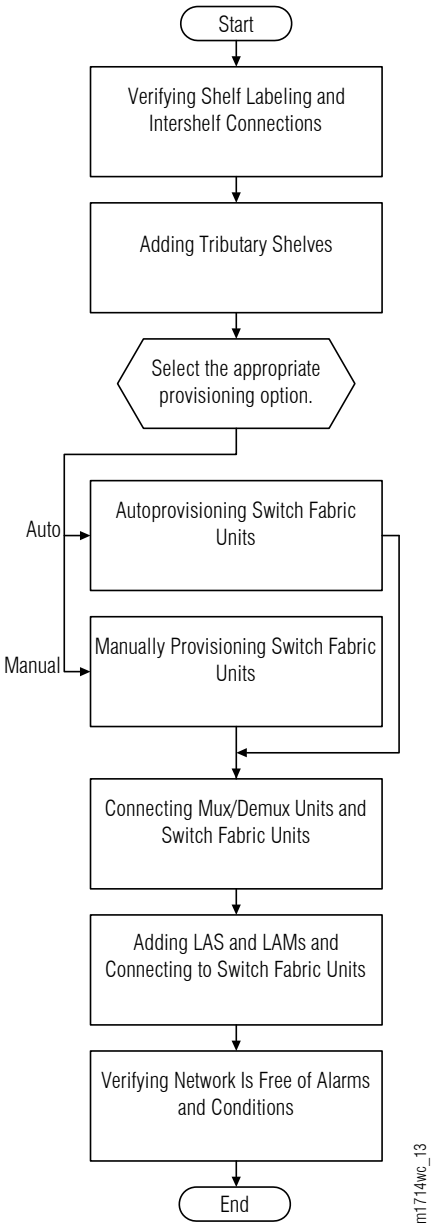


Figure 325: Upgrading Express Node to ROADM Node (Procedural Flowchart)

9.5.1 Verifying Shelf Labeling and Intershelf Connections

Use the following procedure to verify shelf labeling and intershelf connections:

Step 1
Verify shelf labeling and intershelf connections using the procedure in Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units.

Step 2
Proceed to Adding Tributary Shelves.

9.5.2 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 145: Adding Tributary Shelves

Task	Document and Section
Install Tributary shelf in rack.	Installing the Optical/Tributary Shelf
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision Synchronization and/or Tributary shelf OSC units, if required.[98]	Provision Tributary Shelf Equipment Provision Synchronization

Step 2
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning Switch Fabric Units.
- For manual provisioning, proceed to Manually Provisioning Switch Fabric Units.

[98] Refer to procedure for applicability.

9.5.3 Autoprovisioning Switch Fabric Units

The Switch Fabric (SWXP-SWC1 [Issue 2 and later]) plug-in units can be autoprovisioned using the procedure in Autoprovision Optical/ILA Shelf Equipment and Facilities.

Note: *For Mux/Demux unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical/ILA Shelf Equipment and Facilities, install and autoprovision the Switch Fabric units.

Step 2
Proceed to Connecting Mux/Demux Units and Switch Fabric Units.

9.5.4 Manually Provisioning Switch Fabric Units

The Switch Fabric units can be manually provisioned using the procedure in Manually Provision Optical/ILA Shelf Equipment.

Note: *For Mux/Demux unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to pre-provision the slot. In this case, the unit will assume the specific provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical/ILA Shelf Equipment, install and manually provision the Switch Fabric units.

Step 2
Proceed to Connecting Mux/Demux Units and Switch Fabric Units.

9.5.5 Connecting Mux/Demux Units and Switch Fabric Units

Danger: *Never handle exposed fiber with bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the cables installed.

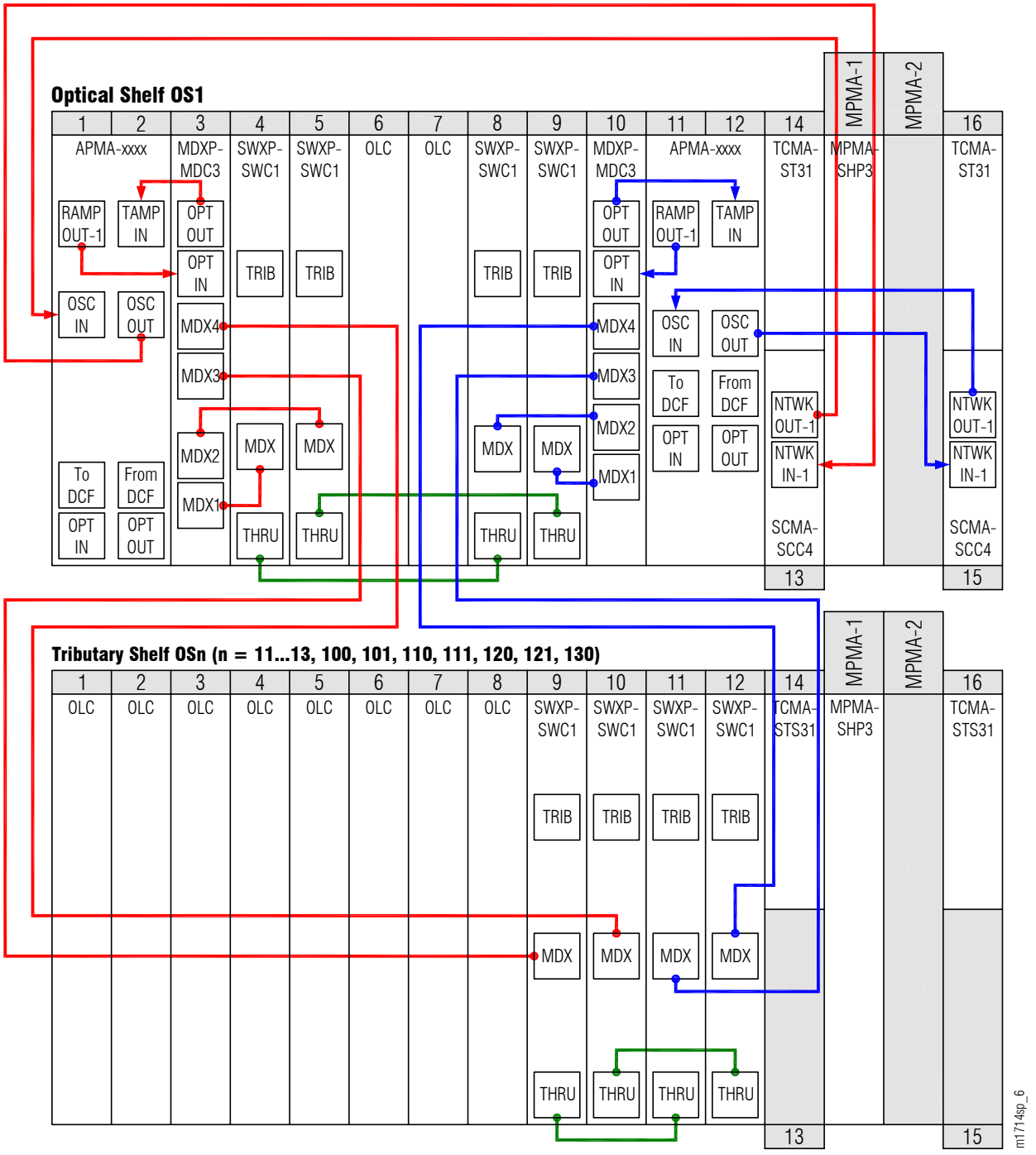


Figure 326: Fiber-Optic Cable Connections between Amplifier, Mux/Demux, and Switch Fabric Units (FLASHWAVE 7500 Small Configuration)

To install internal fiber-optic cables, perform the following steps:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain the required number of MPO-MPO fiber-optic cables and clean the connectors.

Step 2
Connect the cables to the connectors of the MUX/DMUX (MDXP-MDC3) plug-in units and Switch Fabric (SWXP-SWC1 [Issue 2 and later]) plug-in units as shown in the preceding figure and listed in the following table.

Table 146: Mux/Demux Unit to Switch Fabric Unit Fiber-Optic Cable Connections (FLASHWAVE 7500 Small Configuration)

From Mux/Demux Unit		To Switch Fabric Unit		
Optical Shelf Slot	Connector	Shelf	Slot	Connector
3	MDX1	Optical	4	MDX
3	MDX2	Optical	5	MDX
3	MDX3	Tributary	9	MDX
3	MDX4	Tributary	10	MDX
10	MDX1	Optical	8	MDX
10	MDX2	Optical	9	MDX
10	MDX3	Tributary	11	MDX
10	MDX4	Tributary	12	MDX

Step 3
Proceed to Adding LAS and LAMs and Connecting to Switch Fabric Units.

9.5.6 Adding LAS and LAMs and Connecting to Switch Fabric Units

After completing the procedures in Verifying Shelf Labeling and Intershelf Connections through Connecting Mux/Demux Units and Switch Fabric Units, refer to Table 147 for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 147: Installing LAS and LAMs

Task	Document and Section
Install LAS shelf in rack.	Installing the LAS2 Shelf
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

9.5.7 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify the network is free of alarms and conditions:

Step 1
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

9.6
Upgrade ILA Node to 40-Ch Express Node (In-Service)
Applicable to Small and ETSI Configuration Systems

In this section:

This procedure describes how to perform an in-service upgrade of an ILA node to an Express node. The ILA node must be operating on Release 5.1 or later software, and the amplifiers must be APMA-xxU1 Universal Amplifier units.

The procedural flowchart is shown in the following figure.

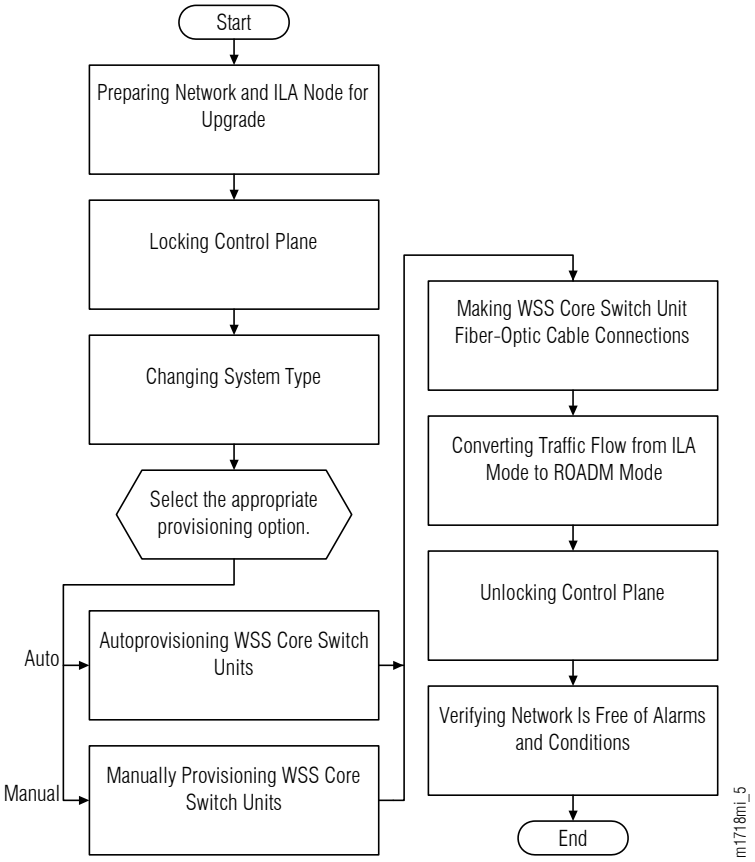


Figure 327: Upgrading ILA Node to Express Node–In Service (Procedural Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

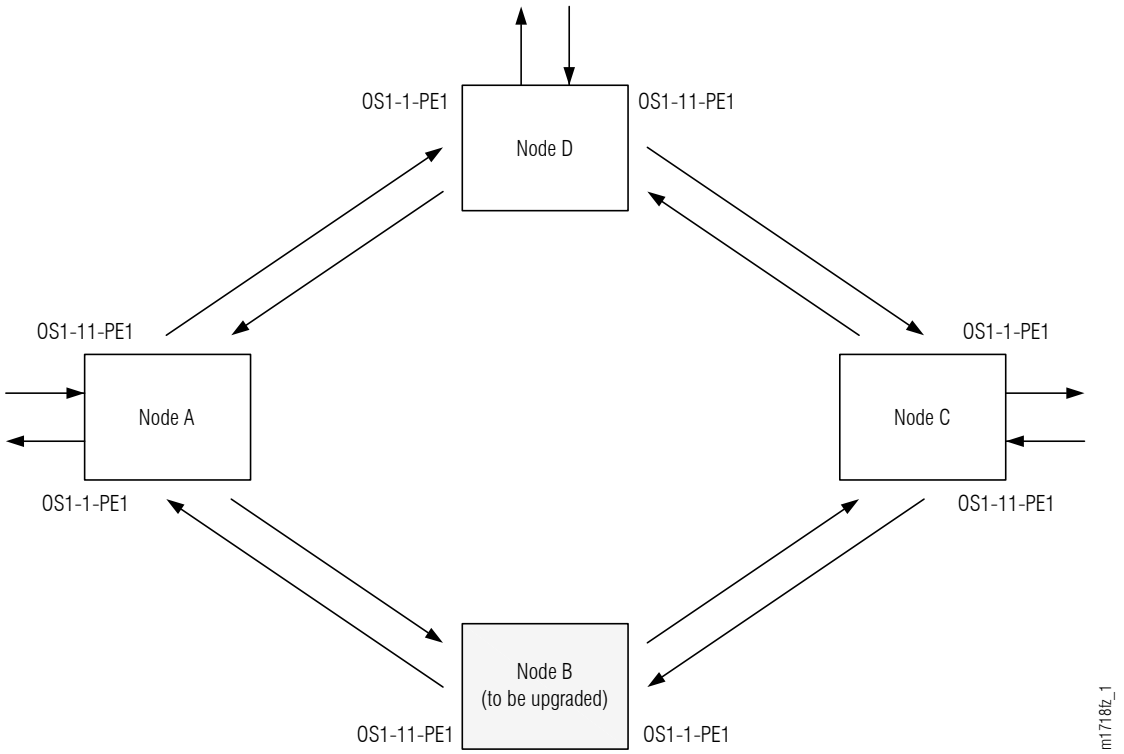


Figure 328: Ring Network Configuration

This procedure can also be used to upgrade linear networks as shown in the following figure.

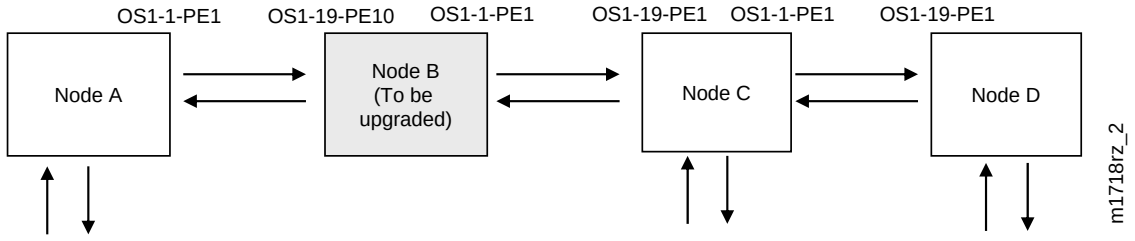


Figure 329: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

9.6.1 Preparing Network and ILA Node for Upgrade

Prepare the ILA node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500	

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[99]
		For **TERM2** (TCP/IP):
		TID: FUJITSU
		User ID: ROOT
		Password: ROOT/(Route66K)
		Conn. Mode: TCP/IP
		IP Address: 192.168.1.1
		Port: 2024

	Click Logon. The NETSMART 500 NE View opens. The Security Message dialog box opens. Click OK. ***Note:*** *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*	

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

[99] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node or for pass-though wavelengths (such as AIS-O, UNEQ-O)?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 2.

Verify Amplifier Type

Step 6
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-11 (slot 11)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-11:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slot 1 and 11.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE. Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 7
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to 32-Ch Express Node–Applicable to Small Configuration Systems, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

Clear Alarms and Conditions on Network

Step 8
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 9
Are any active alarms or conditions being reported on the node or for pass-though wavelengths (such as AIS-O, UNEQ-O)?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 10
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	Close the Properties dialog box.

Step 11
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 2.

Verify Amplifier Type

Step 12
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-11 (slot 11)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-11:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slot 1 and 11.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE. Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 13
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Upgrade ILA Node to 32-Ch Express Node–Applicable to Small Configuration Systems, for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

✔ This procedure is complete.

9.6.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the value for LOCK is Yes.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

9.6.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_S_ILA to FW7500U_S.

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_S_ILA to FW7500U_S.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_S;`
 	
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_S;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_S.
	• Click Modify.
	
	The Confirmation dialog box opens.
	Click Yes.
	The Warning dialog box opens.
	
	Wait approximately 5-20 minutes for the change to complete and the system to restart.
	Click Logon.

Note: *Any pass-through traffic is still being carried through the amplifier-to-amplifier connections. The traffic routing does not change until the OPR-MODE command is sent in* Converting Traffic Flow from ILA Mode to ROADM Mode.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	Click Yes in the pop-up window to continue.
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 8
Verify that the system type is FW7500U_S.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in unit should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the TYPE is FW7500U_S.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning WSS Core Switch Units.
- For manual provisioning, proceed to Manually Provisioning WSS Core Switch Units.

9.6.4 Autoprovisioning WSS Core Switch Units

The WSS Core Switch units (SFMA-CMC1) can be automatically provisioned as described in Autoprovision Optical/ILA Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical/ILA Shelf Equipment and Facilities, install and autoprovision the WSS Core Switch units in shelf OS1 in Node B.

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

9.6.5 Manually Provisioning WSS Core Switch Units

The WSS Core Switch unit (SFMA-CMC1) can be manually provisioned as described in Manually Provision Optical/ILA Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Manually Provision Optical/ILA Shelf Equipment, install and manually provision the WSS Core Switch units in shelf OS1 of Node B.

Note: *This procedure can be used to preprovision the slot. In this case, the unit will assume the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 2
Proceed to Making WSS Core Switch Unit Fiber-Optic Cable Connections.

9.6.6 Making WSS Core Switch Unit Fiber-Optic Cable Connections

Use this procedure to make fiber-optic cable connections between the amplifier units and the WSS Core Switch units.

Danger: *Never handle exposed fiber with bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections for the ILA node before the WSS Core Switch installation and cabling.

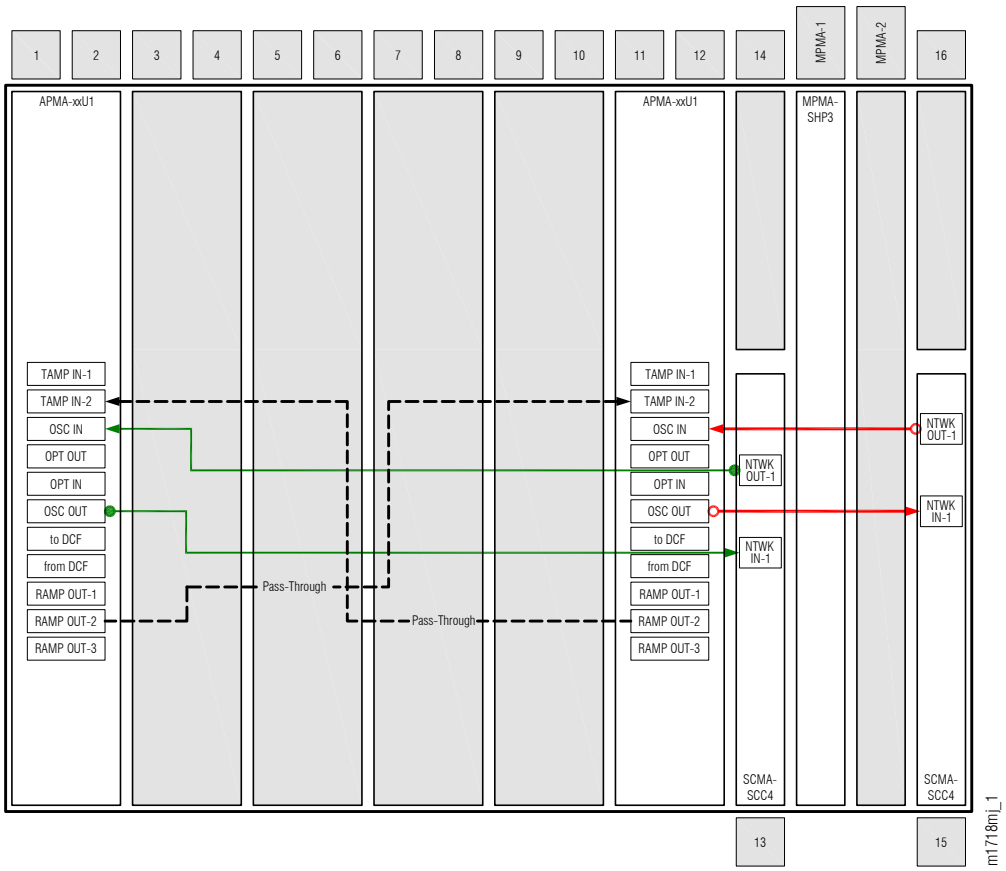


Figure 330: ILA Node Cabling Before WSS Core Switch Unit Installation and Cabling

The following figure shows the fiber-optic cable connections after the WSS Core Switch units are installed and cabled.

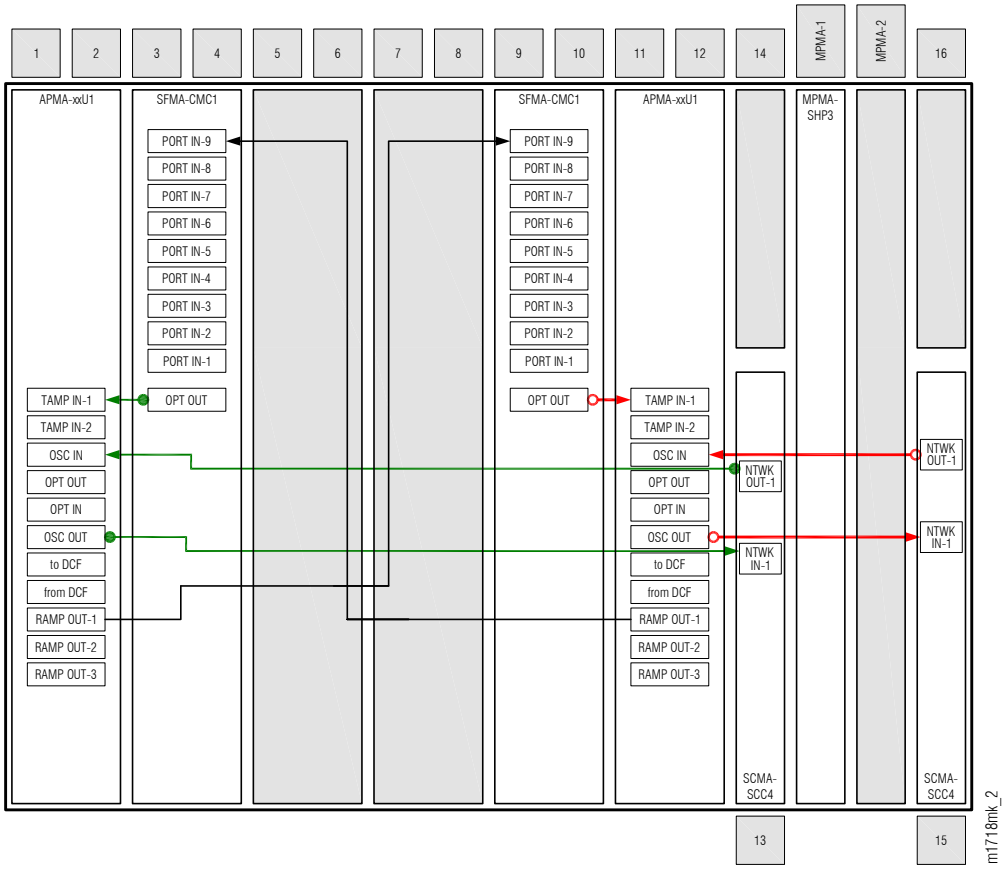


Figure 331: ILA Node Cabling After WSS Core Switch Unit Installation and Cabling

Note: *The ILA pass-through connections are removed in a later procedure.*

Make fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 2
Connect the cables to the connectors of the amplifier (APMA-xxU1) plug-in units and WSS Core Switch (SFMA-CMC1) plug-in units as shown in the preceding figure and listed in the following table.

Table 148: Amplifier Unit and WSS Core Switch Unit Fiber-Optic Cable Connections

Amplifier Unit		WSS Core Switch Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-1	3	OPT OUT
	RAMP OUT-1	9	PORT IN-9
11	TAMP IN-1	9	OPT OUT
	RAMP OUT-1	3	PORT IN-9

Step 3
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode.

9.6.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through WSS Core Switch units). This procedure affects the switch in traffic flow in less than 50 milliseconds. Additionally, this procedure allows you to perform required validations before completing the in-service traffic switch.

There are three modes of operation for this procedure:

- Test mode (MODE=TEST)–Performs the required tests and validations (refer to the following table). A transient condition is reported based on the test result:
  - OPR-MODECOMPLD–Successful test/validation
  - OPR-MODE-FAIL–Unsuccessful test/validation
- Automatic mode (MODE=AUTO)–Performs the required tests and validations (refer to the following table) and then switches the system mode to OADM if all of the tests and validations completed successfully. If any test or validation fails, the OPR-MODE-FAIL transient condition is reported with the cause of the failure.
- Override mode (MODE=OVRD)–Switches the system mode to OADM without performing any tests or validations. The override mode is ideal when the system does not have any traffic.

Caution: *Forced switching (MODE=OVRD) of the operation modes can result in traffic hits. If the node has pass-through traffic, Fujitsu recommends that the test mode or automatic mode of operation be used.*

Note: *The automatic mode of conversion is used in this procedure.*

The following table provides a detailed list of the tests and validations performed by the system when the test mode or automatic mode is used when converting operation modes. The tests and validations are listed in the order in which they are performed.

Table 149: Test Mode and Automatic mode System Tests and Validations

System Test/Validation	Description
System alarms	The system monitors the following conditions and alarms during the in-service conversion test mode: • Common unit failures–FLT, RMVD, MEA, WARMUP, FVM • Amplifier units–MLSPRE, MLSPOST, ALSPRE, ALSPOST, LDONPRE, LDONPOST, SAPPRE, SAPPOST • Amplifiers ports–INDWN on PC1and PC6, POS (high and low) on PC1, POS (high and low) on PC2 • WSS CORE Switch unit–INDWN on PC9 and LOL • WDM facility–LOS, PMI, BDIO • OSC facility–BERSF, BERSD, LOS, LOF, MISCON, CNTFAIL, DCCFAIL, TIM-S, INTROPF, LNR • WCH facility–UNEQ-O/AIS-O, NOLIGHT ***Note:*** *The system monitors the alarms throughout the test mode.*
PM validity check	The system performs the following PM validity checks during the in-service conversion test mode: • APMA-M2U1 unit–OPT on PC1 and PC2, OPR on PE2 • APMA-ULU1 unit–OPR on P1
Optical power level measurements	The system checks that the following optical power level measurements are within specified values: • Amplifier RAMP OUT-1 output port (PC1) and WSS Core Switch unit PORT IN-9 input port (PC9) • WSS Core Switch unit OPT OUT output port (PE1) and amplifier TAMP IN-1 input port (PC1)
Optical test pattern	The system performs optical test patterns to validate the signal flow of the active pass-through traffic between the amplifier (PC1) and the WSS Core Switch port (PE1). ***Note:*** *The testing is done by turning the WSS Core Switch unit VATT on and off for applicable channels.*

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=AUTO;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=AUTO;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select AUTO from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

The ILA-to-ROADM conversion process begins with the system automatically creating pass-through cross-connects for any existing ILA pass-through traffic. Equipment connections between the amplifier ports and WSS Core Switch unit ports are also automatically created. The system then goes into the test and validation mode and performs the actions listed in the preceding table. The CONVIP condition is generated during the conversion process and clears when the conversion completes or terminates.

Note: *If the operation terminates because of any failures or alarms, the OPR-MODE-FAIL standing condition, containing the cause of failure, is raised. The provisioned cross-connects and equipment connections remain on the node. These connections will not impact traffic and can be left in place while the conditions that caused the upgrade to fail are cleared. Refer to Responding to Alarms and Conditions for information on clearing alarms. If you want to perform the conversion regardless of alarms, use MODE=OVRD.*

When the conversion process successfully completes, the OPR MODE COMPLD transient condition is raised, and the direct connections between the amplifiers (PC2 and PC6 on both units) are automatically deleted.

Step 3
Remove the two ILA pass-through cables listed in the following table.

Table 150: Pass-Through Cable Connections between Amplifier Units

Amplifier Unit		Amplifier Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-2	11	RAMP OUT-2

Table 150: Pass-Through Cable Connections between Amplifier Units (Cont.)

Amplifier Unit		Amplifier Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-2	11	TAMP IN-2

Step 4
Continue to Unlocking Control Plane.

9.6.8
Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Verifying Network Is Free of Alarms and Conditions.

9.6.9 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify that the network is free of alarms and conditions:

Step 1
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

9.7
In-Service Upgrade ILA Node to 2D-ROADM Node

In this section:

This procedure describes how to perform an in-service upgrade of an ILA node to a 2D-ROADM node. The ILA node must be operating on Release 5.1 (or later) software, and the amplifiers must be APMA-xxU1 Universal Amplifier units.

Note: *If the ILA node is using a release earlier than Release 5.1 and/or amplifiers other than APMA-xxU1, follow the procedure in* Upgrade ILA Node to 2D-ROADM Node.

A flowchart of the overall process is shown in the following figure.

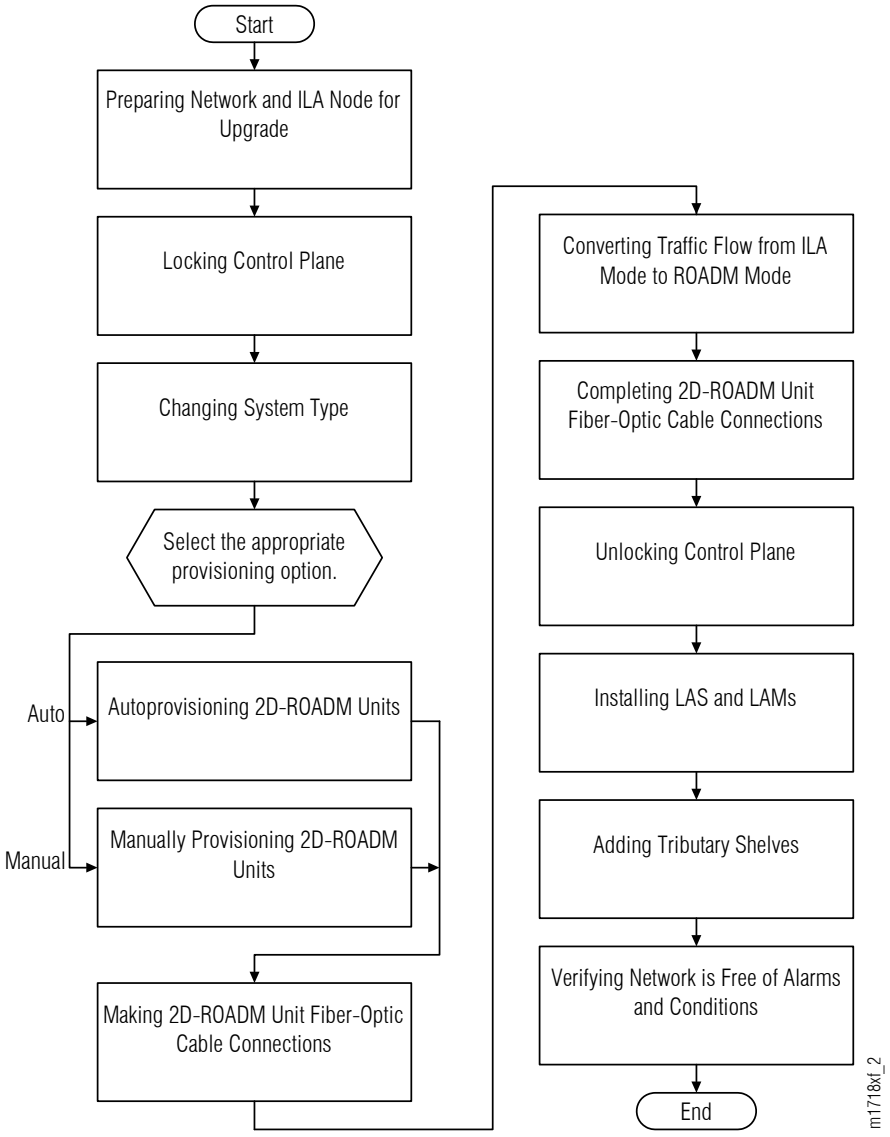


Figure 332: ILA Node to 2D-ROADM Node In-Service Upgrade (Procedure Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

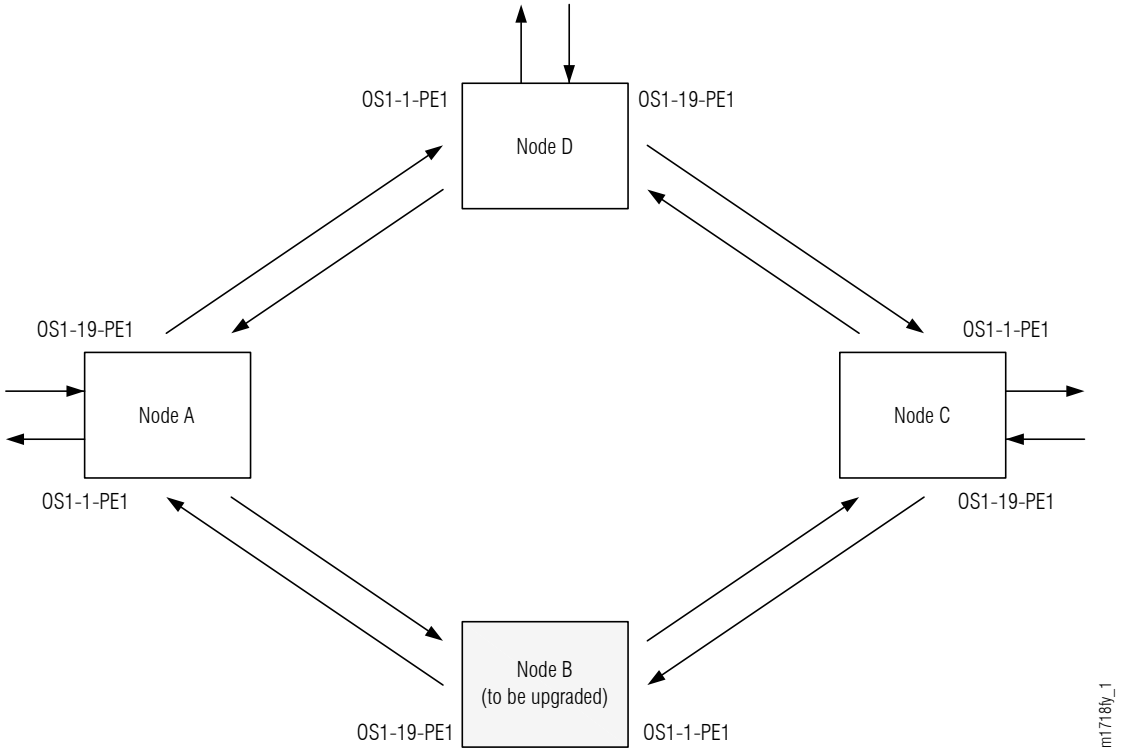


Figure 333: Ring Network Configuration

This procedure can also be used to upgrade linear networks as shown in the following figure.

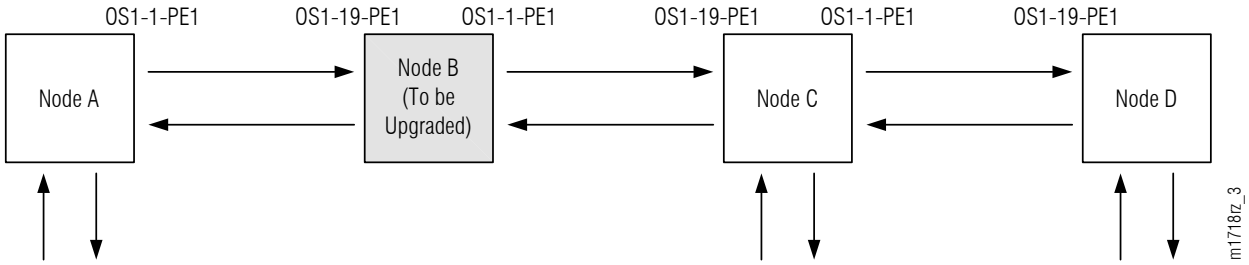


Figure 334: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to Provisioning Hierarchy for more information. Refer to Introduction to Maintenance and Trouble Clearing to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

9.7.1
Preparing Network and ILA Node for Upgrade

Prepare the ILA node for the upgrade as follows:

Step 1
If not already done, log on Nodes A, B, C, and D. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[100]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[100] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software:

- To upgrade from a release earlier than Release 5.1, follow the procedure in Upgrading System Software from Release 4.1, and then repeat this procedure.
- To upgrade from a release after 5.1, follow the procedure in Upgrading System Software from Release 4.2 or Later.

Verify Amplifier Type

Step 6
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 7
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Fiber Cable Handling for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

Clear Alarms and Conditions on Network

Step 8
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 9
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 10
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	Close the Properties dialog box.

Step 11
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software:

- To upgrade from a release earlier than Release 5.1, follow the procedure in Upgrading System Software from Release 4.1, and then repeat this procedure.
- To upgrade from a release after 5.1, follow the procedure in Upgrading System Software from Release 4.2 or Later.

Verify Amplifier Type

Step 12
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-19 (slot 19)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-19:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slots 1 and 19.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE.
	Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 13
Are the amplifiers of the correct type?

If YES:
Proceed to Locking Control Plane.

If NO:
You cannot perform an in-service upgrade on the ILA node. Refer to Fiber Cable Handling for upgrade procedures for ILA nodes with APMA-xxC1 amplifiers.

✔ This procedure is complete.

9.7.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the value for LOCK is Yes.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

9.7.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	The Confirmation dialog box opens.
	Click Yes.
	The Warning dialog box opens.
	Click Logon.

Note: *Any pass-through traffic is still being carried through the amplifier-to-amplifier connections. The traffic routing does not change until the OPR-MODE command is sent in* Converting Traffic Flow from ILA Mode to ROADM Mode.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	Click Yes in the pop-up window to continue.
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade).

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the TYPE is FW7500U_OADM.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning 2D-ROADM Units.
- For manual provisioning, proceed to Manually Provisioning 2D-ROADM Units.

9.7.4 Autoprovisioning 2D-ROADM Units

The 2D-ROADM units (SFMA-RDC1) can be autoprovisioned as described in Autoprovision Optical/ILA Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical/ILA Shelf Equipment and Facilities, install and autoprovision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

9.7.5 Manually Provisioning 2D-ROADM Units

The 2D-ROADM units (SFMA-RDC1) can be manually provisioned as described in Manually Provision Optical/ILA Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit assumes the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical/ILA Shelf Equipment, install and manually provision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

9.7.6 Making 2D-ROADM Unit Fiber-Optic Cable Connections

Use this procedure to make fiber-optic cable connections between the amplifier units and the 2D-ROADM units.

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections for the ILA node before the 2D-ROADM units are installed and cabled.

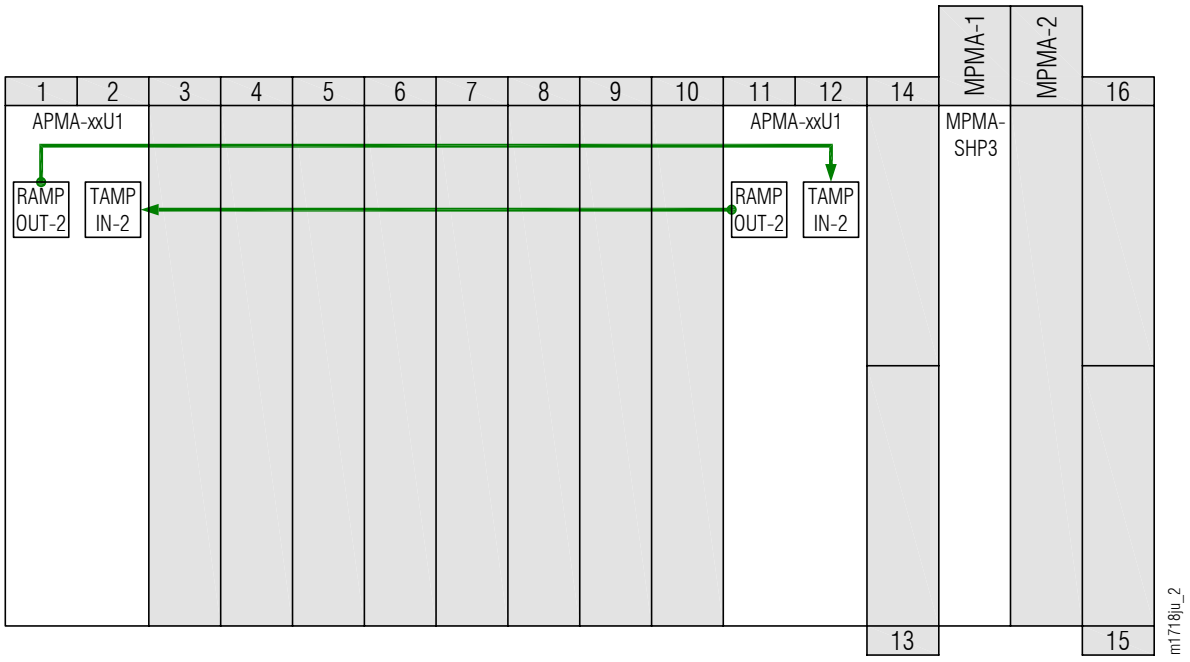


Figure 335: ILA Node Cabling Before 2D-ROADM Unit Installation and Cabling

The following figure shows the fiber-optic cable connections after the 2D-ROADM units are installed and cabled.

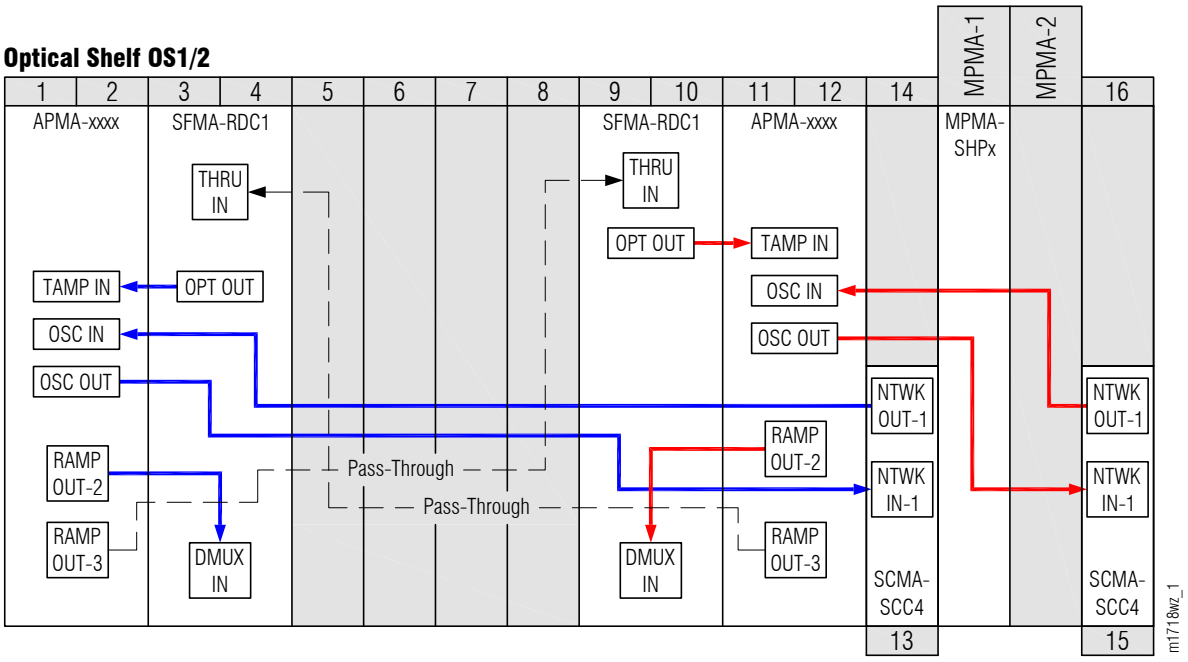


Figure 336: ILA Node Cabling After 2D-ROADM Unit Installation and Initial Cabling

Note: *Do not disconnect the ILA cables until the 2D-ROADM connections are made as described in* Completing 2D-ROADM Unit Fiber-Optic Cable Connections.

Make fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 2
Connect the cables to the connectors of the amplifier (APMA-xxU1) plug-in units and 2D-ROADM (SFMA-RDC1) plug-in units as shown in the preceding figure and listed in the following table.

Table 151: Amplifier Unit and 2D-ROADM Unit Fiber-Optic Cable Connections

Amplifier Unit		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN-1	3	OPT OUT

Table 151: Amplifier Unit and 2D-ROADM Unit Fiber-Optic Cable Connections (Cont.)

Amplifier Unit		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
	RAMP OUT-3	9	THRU IN
11	TAMP IN-1	9	OPT OUT
	RAMP OUT-3	3	THRU IN

Step 3
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode.

9.7.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through 2D-ROADM units). This procedure affects the switch in traffic flow in less than 50 milliseconds. Additionally, this procedure allows you to perform the required validations before completing the in-service traffic switch.

There are three modes of operation for this procedure:

- Test mode (MODE=TEST)—Performs the required tests/validations (refer to the following table). A transient condition is reported based on the test result:
  - OPR-MODE-COMPLD—Successful test/validation
  - OPR-MODE-FAIL—Unsuccessful test/validation
- Automatic mode (MODE=AUTO)—Performs the required tests/validations (refer to the following table) and then switches the system mode to OADM if all tests/validations are completed successfully. If any test/validation fails, the OPR-MODE-FAIL transient condition is reported with the cause of the failure.
- Override mode (MODE=OVRD)—Switches the system mode to OADM without performing any tests/validations. The override mode is ideal when the system does not have any traffic.

Caution: *Forced switching (MODE=OVRD) of the operation modes can result in traffic hits. If the node has pass-through traffic, Fujitsu recommends that the test mode or automatic mode of operation be used.*

Note: *The automatic mode of conversion is used in this procedure.*

The following table provides a detailed list of the tests and validations performed by the system when the test mode or automatic mode is used when converting operation modes. The tests and validations are listed in the order in which they are performed.

Table 152: Test Mode and Automatic mode System Tests and Validations

System Test/Validation	Description
System alarms	The system monitors the following alarms during the in-service conversion test mode: • Common unit failures–FLT, RMVD, MEA, WARMUP, FVM • Amplifier units–MLSPRE, MLSPOST, ALSPRE, ALSPOST, LDONPRE, LDONPOST, SAPPRE, and SAPPOST • Amplifiers ports–INDWN on PC1and PC6, POS (high and low) on PC1, POS (high and low) on PC2 • WSS CORE Switch unit–INDWN on PC9 and LOL • WDM facility–LOS, PMI, BDIO • OSC facility–BERSF, BERSD, LOS, LOF, MISCON, CNTFAIL, DCCFAIL, TIM-S, INTROPF, LNR • WCH facility–UNEQ-O /AIS-O, NOLIGHT ***Note:*** *The system monitors the alarms throughout the test mode.*
PM validity check	The system performs the following PM validity checks during the in-service conversion test mode: • APMA-M2U1 unit–OPT on PC2, OPR on PE2 • APMA-ULU1 unit–OPR on P1
Optical power level measurements	The system checks that the following optical power level measurements are within specified values: • Amplifier RAMP OUT-2 output port (PC1) and 2D-ROADM unit DMUX IN input port (PE1) • 2D-ROADM unit OPT OUT output port (PE1) and amplifier TAMP IN-1 input port (PC1)
Optical test pattern	The system performs optical test patterns to validate the signal flow of the active pass through traffic between the amplifier (PC1) and the 2D-ROADM port (PE1).

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=AUTO;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=AUTO;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select AUTO from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

The ILA–to–2D-ROADM conversion process begins with the system automatically creating pass-through cross-connects for any existing ILA pass-through traffic. The system then goes into the test and validation mode and performs the actions listed in Table 152. The conversion in process (CONVIP) condition is generated during the conversion process and clears when the conversion completes or terminates.

Note: *If the operation terminates due to the failure of any of the test or validation checks or alarms, the OPR-MODE-FAIL standing condition, containing the cause of the failure, is raised. Refer to Responding to Alarms and Conditions for information on clearing alarms. To perform the conversion regardless of alarms, use MODE=OVRD.*

When the conversion process successfully completes, the OPR-MODE-COMPLD transient condition is raised, and the direct connections between the amplifiers (PC2 and PC6 on both units) are automatically deleted.

Step 3
Proceed to Completing 2D-ROADM Unit Fiber-Optic Cable Connections.

9.7.8 Completing 2D-ROADM Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the connection after the ILA connection is removed and the interconnection between the amplifier and the 2D-ROADM unit is made.

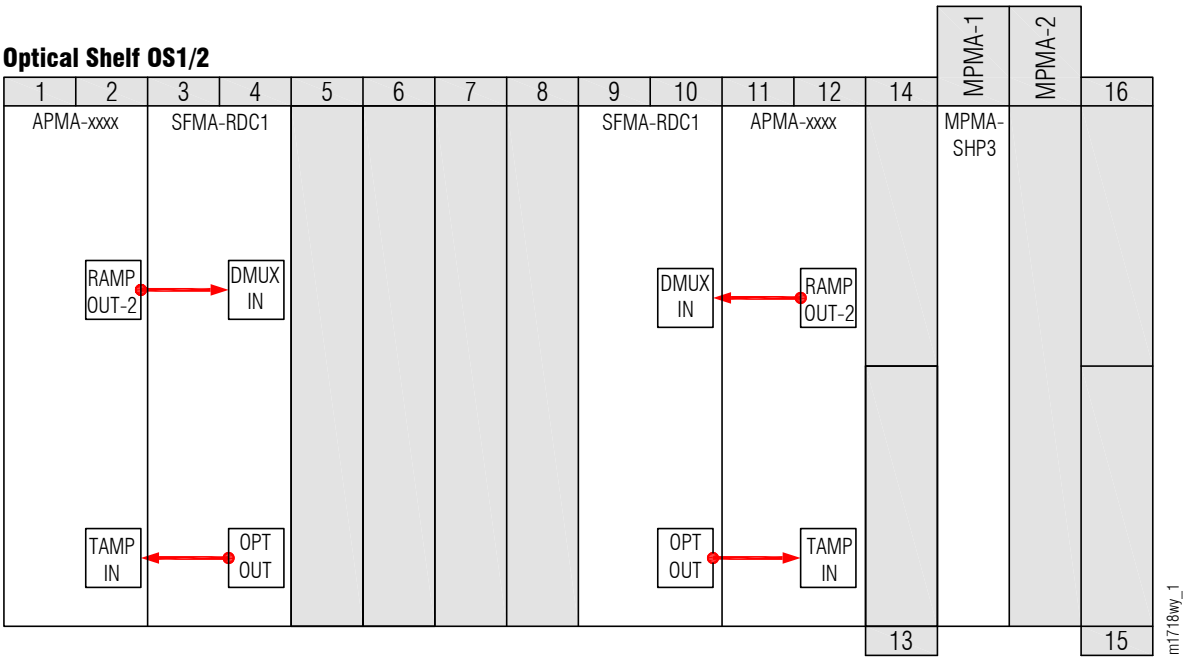


Figure 337: 2D-ROADM Unit Cabling with Drop

The ILA pass-through connections are no longer needed. The following steps guide you through disconnecting the TAMP IN-2 end of the pass-through connections on the amplifiers and making connections to the 2D-ROADM units.

To install internal fiber-optic cables, perform the following steps:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Step 1

Move the terminal connection of the ILA pass-through cables (see Figure 336) as follows:

a) Disconnect the fiber-optic cable from connector TAMP IN-2 of the Amplifier plug-in unit located in slot 19.

b) Reconnect this cable end to connector DMUX IN of the SFMA-RDC1 plug-in unit located in slot 3 as shown in the preceding figure and listed in the following table.

c) Disconnect the fiber-optic cable from connector TAMP IN-2 of the Amplifier plug-in unit located in slot 1.

d) Reconnect this cable end to connector DMUX IN of the SFMA-RDC1 plug-in unit located in slot 17 as shown in the preceding figure and listed in the following table.

Table 153: Amplifier and 2D-ROADM Unit Fiber-Optic Cable Connections

Amplifier		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-2	3	DMUX IN
11	RAMP OUT-2	9	DMUX IN

Step 2
Proceed to Unlocking Control Plane.

9.7.9 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and ILA Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
 	
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the Control Plane tab.
	
	For the LOCK command parameter, click No.
	Click Modify.
	
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
 	
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	
	Close the Operations dialog box.

Step 4
Proceed to Installing LAS and LAMs.

9.7.10 Installing LAS and LAMs

After completing the subprocedures in Preparing Network and ILA Node for Upgrade through Unlocking Control Plane, refer to Table 154, for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 154: Install LAS and LAMs

Task	Practice and Section
Install LAS shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

9.7.11 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 155: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision synchronization and/or Tributary shelf OSC units, if required[101].	Provision Synchronization

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

9.7.12
Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify the network is free of alarms and conditions.

Step 1
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[101] Refer to procedure for applicability.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

9.8 Upgrade ILA Node to 2D-ROADM Node

In this section:

Note: *This procedure applies to ILA nodes running a software release earlier than Release 5.1 and/or using an amplifier other than the AMPA-xxU1 Universal Amplifier unit. For systems running software later than Release 5.1 and using AMPA-xxU1 Universal Amplifier units, follow the procedure given in* In-Service Upgrade ILA Node to 2D-ROADM Node*, to upgrade an ILA node to a 2D-ROADM node.*

A flowchart of the overall process is shown in the following figure.

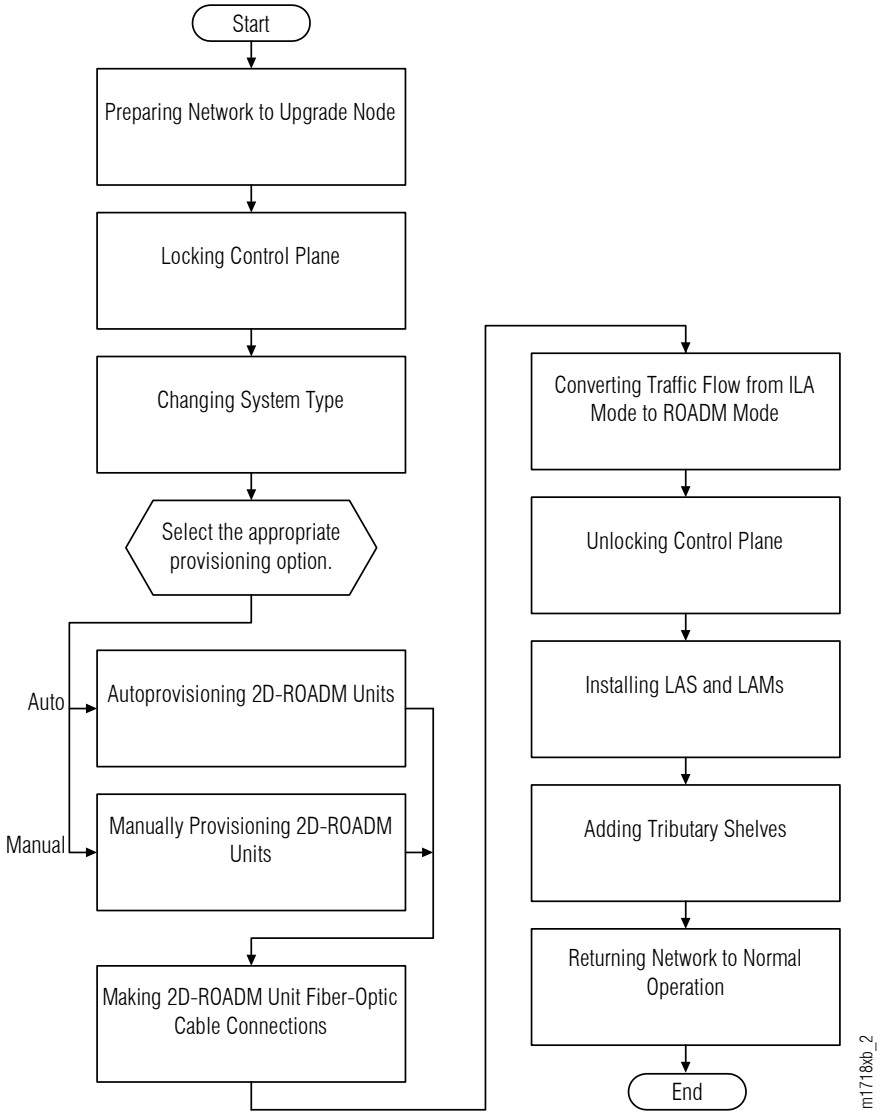


Figure 338: Upgrading ILA Node to 2D-ROADM Node (Procedure Flowchart)

This procedure describes how to prepare a ring network to upgrade one of the nodes in the ring from an ILA node to a 2D-ROADM node. This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

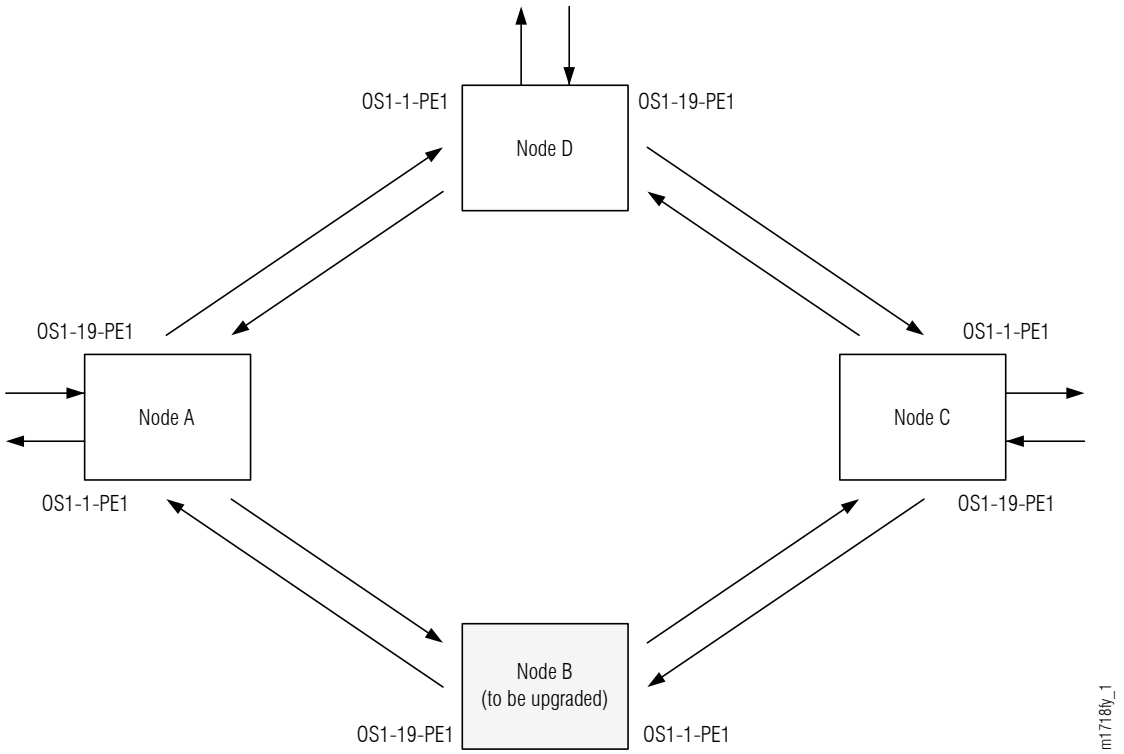


Figure 339: Ring Network Configuration

The procedure can also be used for linear networks; however, protection switching is not possible. See the following figure.

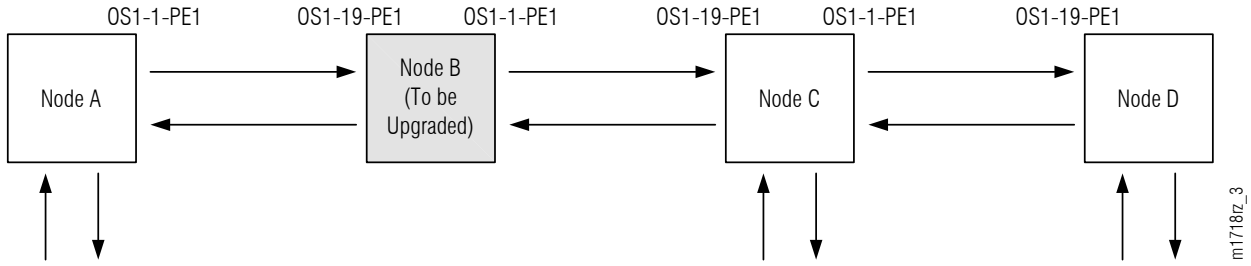


Figure 340: Linear Network Configuration

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to Introduction to TL1 Commands for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

9.8.1 Preparing Network to Upgrade Node

Prepare the network for the upgrade as follows:

Step 1

If not already done, log on Nodes A, B, C, and D. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values shown apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to Setting Up Craft Interface (TL1 Session through TERM1) through Setting Up Craft Interface (NETSMART 500 Session through TERM2).*

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[102]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	The NETSMART 500 NE View opens.
	The Security Message dialog box opens.
	Click OK.
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Clear Alarms and Conditions

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

[102] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 4
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 5
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct connect application (although it may still be protected).*

Step 6
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 7.

Step 7
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 8.

If NO:
Proceed to Step 9.

Step 8
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then go to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 9
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 10
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs), if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 11
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then go to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 12
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
 TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 13
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 14
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 156: Decision Table (Node A)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[103]	SST	
OS1-1-PE1-c	DEF	Yes
	SWITCH	No
OS1-19-PE1-c	DEF	No

[103] c = 1...40 (channel number)

Table 156: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[103]	SST	
	SWITCH	Yes

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 15.

If NO:
Proceed to Step 17.

Step 15
At Node A, for each channel identified in Step 14, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 16
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 156).

[103] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 17
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 18
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 19
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 20
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 21
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 22
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 23.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 23.

Step 23
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 12.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 24
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 25
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 26
Are any dropped channels currently taking traffic from OS1-19-PE1 (refer to the following table)?

Table 157: Decision Table (Node C)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[104]	SST	
OS1-1-PE1-c	DEF	No
	SWITCH	Yes
OS1-19-PE1-c	DEF	Yes

[104] c = 1...40 (channel number)

Table 157: Decision Table (Node C) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[104]	SST	
	SWITCH	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 27.

If NO:
Proceed to Step 29.

Step 27
At Node C, for each channel identified in Step 26, initiate a manual protection switch away from the OS1-19-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 28
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-19-PE1 (refer to Table 157).

[104] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 29
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 30
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 31
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-19-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-19-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 32
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 33
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 34
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 35.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 35.

Step 35
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-19-PE1.

Note: *Use the same criteria used in Step 24.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 36
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 37
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 38
For each drop cross-connect identified in Step 37, identify the ***break direction***, OS1-1-PE1 or OS1-19-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Traveling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 39
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 158: Decision Table (Node D)

Retrieved Cross-Connect Values		Break Direction[105]	Is Current Traffic Dropped from the Break Direction?
PSWDEF[106]	SST		
OS1-1-PE1-c	DEF	OS1-1-PE1	Yes
		OS1-19-PE1	No
	SWITCH	OS1-1-PE1	No
		OS1-19-PE1	Yes
OS1-19-PE1c	DEF	OS1-1-PE1	No
		OS1-19-PE1	Yes
	SWITCH	OS1-1-PE1	Yes
		OS1-19-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs), if applicable, and then go to Step 40.

If NO:
Proceed to Step 42.

Step 40
At Node D, for each channel identified in Step 39, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

105 Refer to Step 38.
106 c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 41
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 158).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 42
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 43
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 44
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 45
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 46
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 47
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 48.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 48.

Step 48
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-19-PE1).

Note: *Use the same criteria used in Step 36.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Verify that no dropped channels are currently taking traffic.
	Close the Properties dialog box.

Step 49
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 50
Proceed to Locking Control Plane.

Clear Alarms and Conditions

Step 51
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 52
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4.

Verify Traffic Protection

Step 53
Retrieve and record all cross-connects at Nodes A, C, and D, and confirm that they are correct (as expected).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that all cross-connects are correct.
	
	Close the Properties dialog box.

Note: *An audit of all the unprotected wavelengths and services passing through Node B should be done. If these services/connections are used by an external device providing protection, that device should be instructed to protection switch away from the path going through Node B. After the upgrade, the traffic can be switched back.*

Step 54
Determine whether the drop path cross-connects at Nodes A, C, and D are optical channel dedicated protection ring (OCh-DPRING)–protected.

Note: *The keyword PSWDEF indicates that a cross-connect is in a ring network and has path switch default. The absence of the keyword indicates that a cross-connect is in a direct connect application (although it may still be protected).*

Step 55
At Nodes A, C, and D, is each drop path cross-connect OCh-DPRING–protected?

If YES:
Proceed to Step 9.

If NO:
Some of the drop paths are unprotected. Proceed to Step 56.

Step 56
Do the unprotected drop paths go through Node B?

If YES:
Proceed to Step 57.

If NO:
Proceed to Step 9.

Step 57
Are you allowed to disturb the traffic on the unprotected drop paths?

If YES:
The traffic on the unprotected drop paths is lost until Node B upgrade completes. Proceed to Step 9.

If NO:
Reconfigure the unprotected drops for OCh-DPRING protection. Then go to Step 9.

Caution: *In a linear network, the upgrade process causes a service outage. Perform the migration procedure during a service window and/or when traffic is low.*

Note: *To configure OCh-DPRING protection, equipment connections and cross-connects must be added. Refer to* Equipment and Facility Provisioning.

Record Pass-Through Channels for Node B

Note: *These steps are used in combination with the steps in* Provision Pass-Through Cross-Connects for Node B, *to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

Step 58
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 59
From the retrieved cross-connects, identify and record the WCH channel numbers and the circuit identifiers (CKTIDs), if applicable, of all cross-connects to or from the OS1-1-PE1 facility.

Note: *Inspect the toAID and fromAID for each retrieved cross-connect. If the AIDs are in the form OS1-1-PE1-c (where c = 1...40), record the channel number c.*

Step 60
Save this record of pass-through channels. It will be used to perform the steps in Provision Pass-Through Cross-Connects for Node B. Then go to Step 12.

Perform Manual Protection Switches (Node A)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node A does not come through Node B.*

Step 61
At Node A, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
 TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 62
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 63
Are any dropped channels currently taking traffic from OS1-1-PE1 (refer to the following table)?

Table 159: Decision Table (Node A)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[107]	SST	
OS1-1-PE1-c	DEF	Yes
	SWITCH	No
OS1-19-PE1-c	DEF	No

[107] **c = 1...40 (channel number)**

Table 159: Decision Table (Node A) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-1-PE1?
PSWDEF[107]	SST	
	SWITCH	Yes

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 64.

If NO:
Proceed to Step 66.

Step 64
At Node A, for each channel identified in Step 63, initiate a manual protection switch away from the OS1-1-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 65
At Node A, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-1-PE1 (refer to Table 159).

[107] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 66
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 67
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 19.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 19.

Perform Forced Protection Switches (Node A)

Step 68
At Node A, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-1-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-1-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEA:`
`OS1-1-PE1-22:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 69
Retrieve conditions at Node A to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 70
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 71
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 72.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 72.

Step 72
At Node A, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-1-PE1.

Note: *Use the same criteria used in Step 12.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node C)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node C does not come through the span between Node A and Node C.*

Step 73
At Node C, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 74
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 75
Are any dropped channels currently taking traffic from OS1-19-PE1 (refer to the following table)?

Table 160: Decision Table (Node C)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[108]	SST	
OS1-1-PE1-c	DEF	No
	SWITCH	Yes
OS1-19-PE1-c	DEF	Yes

[108] **c = 1...40 (channel number)**

Table 160: Decision Table (Node C) (Cont.)

Retrieved Cross-Connect Values		Is Current Traffic Dropped from OS1-19-PE1?
PSWDEF[108]	SST	
	SWITCH	No

If YES:
Record the channel numbers and the circuit identifiers (CKTIDs) if applicable; then go to Step 76.

If NO:
Proceed to Step 78.

Step 76
At Node C, for each channel identified in Step 75, initiate a manual protection switch away from the OS1-19-PE1 side.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 77
At Node C, retrieve all cross-connects, and confirm that no channels are currently taking traffic from OS1-19-PE1 (refer to Table 160).

[108] **c = 1…40 (channel number)**

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 78
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 79
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 31.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 31.

Perform Forced Protection Switches (Node C)

Step 80
At Node C, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from OS1-19-PE1.

Note: *This step should not impact traffic because all traffic should already be directed away from OS1-19-PE1.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODEC:`
`OS1-1-PE1-14:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select FRCD.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 81
Retrieve conditions at Node C to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 82
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 83
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 84.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 84.

Step 84
At Node C, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from OS1-19-PE1.

Note: *Use the same criteria used in Step 24.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODEC:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Perform Manual Protection Switches (Node D)

Note: *These steps ensure that OCh-DPRING–protected traffic dropped at Node D does not come through the span between Node A and Node C.*

Step 85
At Node D, retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 86
Identify all OCh-DPRING–protected drop cross-connects, and record the values of keyword PSWDEF and parameter SST (`DEF` or `SWITCH`) for each.

Note: *Keyword PSWDEF is only set to a value if the cross-connect is an OCh-DPRING–protected drop. The value of PSWDEF is the WCH facility AID for the preferred path. The value of SST (`DEF` or `SWITCH`) indicates whether the preferred path is currently used (`DEF`) or not (`SWITCH`).*

Step 87
For each drop cross-connect identified in Step 86, identify the ***break direction***, OS1-1-PE1 or OS1-19-PE1, that will lose signal if the span between Node A and Node C is opened:

Note: *In general, the break direction is **not** the same for each drop.*

a) Identify (for example, from local records) the node in the ring network that is the source of the drop.

b) Traveling around the ring network from Node D in the OS1-1-PE1 direction, do you arrive at the break span between Node A and Node C before you arrive at the source node?

Step 88
Are any dropped channels currently taking traffic from the break direction (refer to the following table)?

Table 161: Decision Table (Node D)

Retrieved Cross-Connect Values		Break Direction[109]	Is Current Traffic Dropped from the Break Direction?
PSWDEF[110]	SST		
OS1-1-PE1-c	DEF	OS1-1-PE1	Yes
		OS1-19-PE1	No
	SWITCH	OS1-1-PE1	No
		OS1-19-PE1	Yes
OS1-19-PE1c	DEF	OS1-1-PE1	No
		OS1-19-PE1	Yes
	SWITCH	OS1-1-PE1	Yes
		OS1-19-PE1	No

If YES:
Record the channel number(s) and the circuit identifiers (CKTIDs), if applicable, and then go to Step 89.

If NO:
Proceed to Step 91.

Step 89
At Node D, for each channel identified in Step 88, initiate a manual protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1).

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear your system for a cabling or provisioning problem.*

109 Refer to Step 87.
110 c = 1...40 (channel number)

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 90
At Node D, retrieve all cross-connects, and confirm that no dropped channels are currently taking traffic from the break direction (refer to Table 161).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 91
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	View ▸ *Filter*
	
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 92
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 44.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 44.

Perform Forced Protection Switches (Node D)

Step 93
At Node D, for each OCh-DPRING–protected drop cross-connect, initiate a forced protection switch away from the break direction (OS1-1-PE1 or OS1-19-PE1) identified in Step 38.

Note: *This step should not impact traffic because all traffic should already be directed away from the break direction.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::FRCD;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
 	
Example:
`OPR-PROTNSW-WCH:FUJITSU-NODED:`
`OS1-1-PE1-19:CTAG::FRCD;`
	In the tree view, click the Facilities tab.
	
	Expand the appropriate shelf component, and select the WCH facility.
	
	Entity ▸ *Operations Dialog*
	
	Click the Protection tab.
	Click the Operate tab.
	
	From the SC drop-down list, select FRCD.
	Click Operate.
	
	A confirmation dialog box opens.
	Click Yes.
	
	Close the Operations dialog box.

Step 94
Retrieve conditions at Node D to verify that the forced protection switches occurred.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 95
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 96
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 97.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 97.

Step 97
At Node D, retrieve all cross-connects, and verify that no dropped channels are currently taking traffic from the break direction (OS1-1-PE1 or OS1-19-PE1).

Note: *Use the same criteria used in Step 36.*

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU-NODED:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	
	Verify that no dropped channels are currently taking traffic.
	
	Close the Properties dialog box.

Step 98
If more than one nonadjacent node exists, repeat Perform Manual Protection Switches (Node D), and Perform Forced Protection Switches (Node D), for each nonadjacent node.

Step 99
Proceed to Locking Control Plane.

✔ This procedure is complete.

9.8.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Changing System Type.

9.8.3 Changing System Type

Use these steps to change the system type for Node B from FW7500U_ILA to FW7500U_OADM.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Change system type from FW7500U_ILA to FW7500U_OADM.

Note: *This command terminates the communication session and restarts the NE.*

TL1	NETSMART 500

`ED-SYS:TID::CTAG:::TYPE=FW7500U_OADM;`
 	
Example:
`ED-SYS:FUJITSU::CTAG:::`
`TYPE=FW7500U_OADM;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the NE type tab.
	In the Operations dialog box:
	• From the Type drop-down list, select FW7500U_OADM.
	• Click Modify.
	
	The Confirmation dialog box opens.
	Click OK.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 3
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 4.

Step 4
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

Step 5
Reinitialize the system software.

Note: *This command automatically logs the user off the NE.*

TL1	NETSMART 500

`INIT-SYS:TID:AID:CTAG:::LEVEL=WARM;`
AID:
• ALL (null)
 	
Example:
`INIT-SYS:FUJITSU::CTAG:::LEVEL=WARM;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click Initialize tab.
	Click the NE tab.
	Select Level: WARM.
	Click Initialize.
	
	Click Yes in the pop-up window to continue.
	
	If a second pop-up window opens, the connection is lost, and you must log on the NETSMART 500 user interface again to continue by clicking Logon.

The NOT READY indicator on the NEM Shelf Processor plug-in unit lights amber and then goes out after 5 to 20 minutes. After the NOT READY indicator goes out, the FAIL/SVCE indicator lights green on the NEM Shelf Processor unit.

Step 6
After the NOT READY indicator goes out and the FAIL/SVCE indicator lights green, proceed to Step 7.

Step 7
Log on Node B (refer to Step 1 in Preparing Network to Upgrade Node).

The conversion in progress (CONVIP) condition is raised. The condition clears once the conversion process completes or terminates.

Step 8
Verify that the system type is FW7500U_OADM.

Note: *The FAIL/SVCE indicator on the NEM Shelf Processor plug-in units should be green.*

TL1	NETSMART 500

`RTRV-SYS:TID::CTAG;`
Example:
`RTRV-SYS:FUJITSU::CTAG;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 9
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning 2D-ROADM Units.
- For manual provisioning, proceed to Manually Provisioning 2D-ROADM Units.

9.8.4 Autoprovisioning 2D-ROADM Units

The 2D-ROADM units can be autoprovisioned as described in Autoprovision Optical Shelf Equipment and Facilities.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Autoprovision Optical Shelf Equipment and Facilities, install and autoprovision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

9.8.5 Manually Provisioning 2D-ROADM Units

The 2D-ROADM units can be manually provisioned as described in Manually Provision Optical Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Step 1
Using the procedure in Manually Provision Optical Shelf Equipment, install and manually provision the 2D-ROADM units in shelf OS1 of Node B.

Step 2
Proceed to Making 2D-ROADM Unit Fiber-Optic Cable Connections.

9.8.6 Making 2D-ROADM Unit Fiber-Optic Cable Connections

Danger: *Never handle exposed fiber with your bare hands or touch it to your body. A fiber fragment could enter the skin and be very difficult to detect and remove. Follow local safety precautions regarding fiber.*

Danger: *Never look into the end of a fiber-optic cable. Permanent eye damage or blindness can occur very quickly if the laser light is present. Follow local safety precautions regarding fiber.*

Warning: *To avoid damage to the equipment when connecting fibers, always verify the optical specifications. Verify that the optical signal into a receiver meets the appropriate optical specifications listed in* Optical Specifications.

The following figure shows the fiber-optic cable connections before the upgrade.

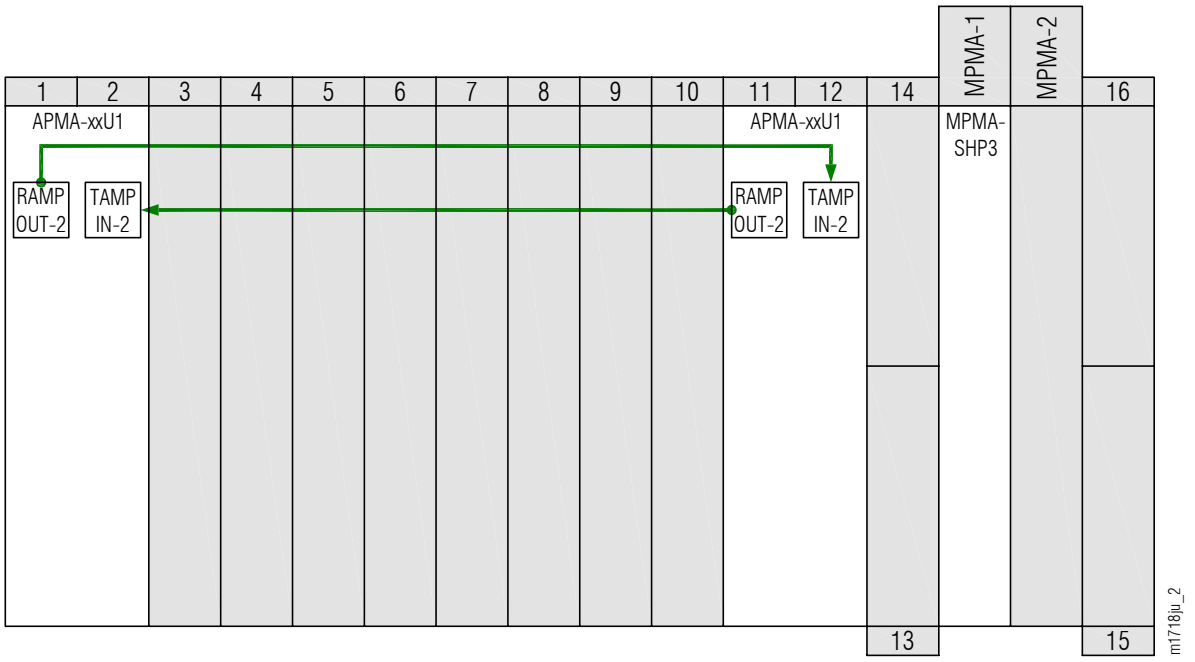


Figure 341: Cabling Before Upgrade (ILA Node)

The following figure shows the fiber-optic cable connections after the upgrade.

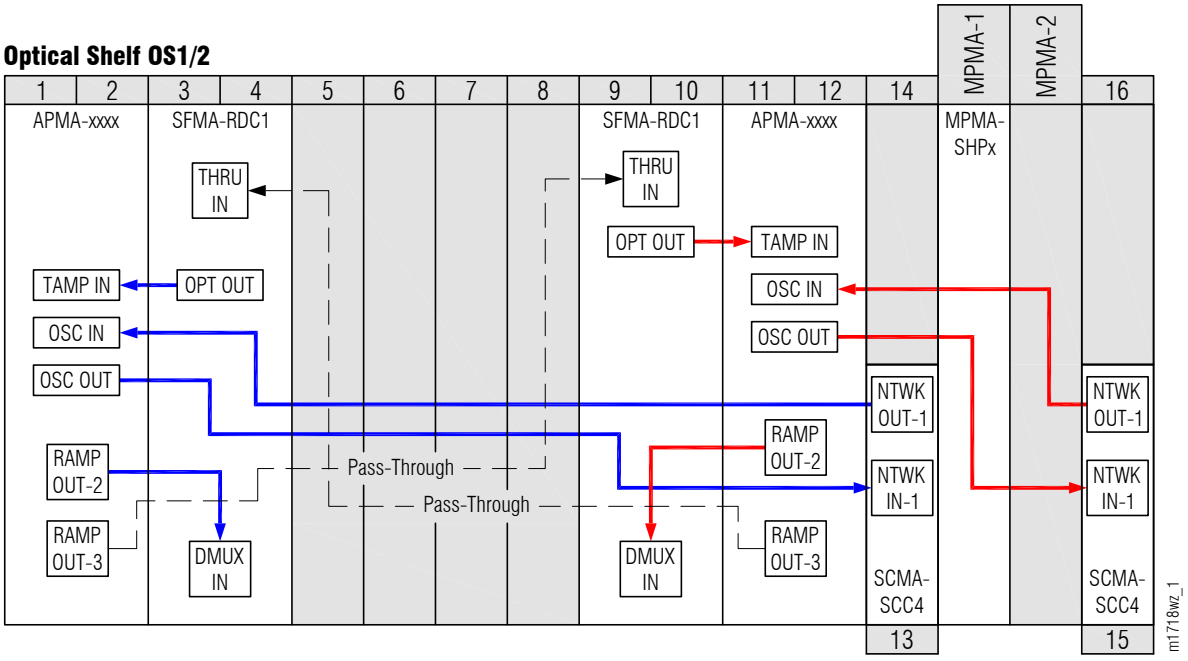


Figure 342: Cabling After Upgrade (2D-ROADM Node)

Change fiber-optic cable connections as follows:

Note: *For rules and precautions regarding handling, storing, cleaning, connecting, and disconnecting fiber-optic cables, refer to* Fiber Cable Handling.

Remove ILA Pass-Through Cables and Attenuators

Step 1
Disconnect and remove the ILA pass-through cables shown in Figure 341 and listed in the following table.

Note: *The optical attenuators located at the TAMP IN connectors are removed in the next step.*

Table 162: Pass-Through Connections between APMA-xxC1 Amplifier Units

From Amplifier Unit (APMA-xxC1)		To Amplifier Unit (APMA-xxC1)	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-1	11	TAMP IN
1	TAMP IN	11	RAMP OUT-1

Step 2
Disconnect and remove the two 14 dB optical attenuators from the TAMP IN connectors of the Amplifier plug-in units located in slots 1 and 11.

Install Pass-Through Cables

Step 3
Obtain and clean two LC-LC fiber-optic cables.

Step 4
Connect the cable ends to the appropriate plug-in units and connectors as shown in the following figure and listed in the following table.

Table 163: Pass-Through Cable Connections (2D-ROADM Configuration)

Amplifier (APMA-xxC1)		2D-ROADM Unit (SFMA-RDC1)	
Shelf Slot	Connector	Shelf Slot	Connector
1	RAMP OUT-3	9	THRU IN

Table 163: Pass-Through Cable Connections (2D-ROADM Configuration) (Cont.)

Amplifier (APMA-xxC1)		2D-ROADM Unit (SFMA-RDC1)	
Shelf Slot	Connector	Shelf Slot	Connector
11	RAMP OUT-3	3	THRU IN

Connect Amplifier and 2D-ROADM Units

Step 5
Obtain four LC-LC fiber-optic cables, and clean the connectors.

Step 6
Connect the cables to the connectors of the amplifier (APMA-xxC1) plug-in units and 2D-ROADM (SFMA-RDC1) plug-in units as shown in Figure 342 and listed in the following table.

Table 164: Amplifier Unit and 2D-ROADM Unit Fiber-Optic Cable Connections

Amplifier Unit		2D-ROADM Unit	
Shelf Slot	Connector	Shelf Slot	Connector
1	TAMP IN	3	OPT OUT
19	TAMP IN	17	OPT OUT
1	RAMP OUT-2	3	DMUX IN
19	RAMP OUT-2	17	DMUX IN

Step 7
Proceed to Converting Traffic Flow from ILA Mode to ROADM Mode.

✔ This procedure is complete.

9.8.7 Converting Traffic Flow from ILA Mode to ROADM Mode

Use this procedure to convert the traffic from the ILA mode (amplifier-to-amplifier pass-through traffic flow) to the ROADM mode (traffic flows through 2D-ROADM units).

Step 1
If not already done, log on Node B (refer to Step 1 of Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Convert the operation mode of Node B.

TL1	NETSMART 500
`OPR-MODE:TID::CTAG:::MODE=OVRD;` ***Example:*** `OPR-MODE:TID::CTAG:::MODE=OVRD;`	*NE* ▸ *System Operations* The Operations dialog box opens. Click the Operate Mode tab. Select OVRD from the MODE drop-down list. Click Modify. Do not close the Operations dialog box.

The conversion process takes approximately 5 minutes to complete.

Step 3
Proceed to Unlocking Control Plane.

9.8.8 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click No.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	Close the Operations dialog box.

Step 4
Proceed to Installing LAS and LAMs.

9.8.9 Installing LAS and LAMs

After completing the subprocedures in Preparing Network to Upgrade Node through Unlocking Control Plane, refer to the following table for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 165: Install LAS and LAMs

Task	Practice and Section
Install LAS shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

9.8.10 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 166: Adding Tributary Shelf

Task	Practice and Section
Install Tributary shelf in rack.	Installing Optical/Tributary Shelf, LAS, and Heat Baffle
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable
Create Tributary shelf entity and install shelf processors.	Create Subtending Shelves and Install Shelf Processors
Provision synchronization and/or Tributary shelf OSC units, if required[111].	Provision Synchronization and/or Tributary Shelf OSC Units

Step 2
Proceed to Returning Network to Normal Operation.

9.8.11 Returning Network to Normal Operation

To release protection switches and verify that the network is free of alarms and conditions, perform the following steps:

Note: *Perform Steps 5 through 13 for each node in the ring network.*

Provision Pass-Through Cross-Connects for Node B

Note: *These steps are used in combination with the steps in Record Pass-Through Channels for Node B, to ensure that Node B, after the upgrade, supports the same pass-through traffic that it supported before the upgrade.*

[111] Refer to procedure for applicability.

Step 1
If not already done, log on Nodes A, B, C, and D (refer to Step 1 in Preparing Network to Upgrade Node). If already logged on, proceed to the next step.

Step 2
Obtain the record of pass-through channels that was recorded when performing the steps in Record Pass-Through Channels for Node B.

Step 3
At Node B, for each WCH channel previously identified, provision pass-through cross-connects in both directions.

TL1	NETSMART 500

`ENT-CRS-WCH:TID:fromAID,toAID:CTAG :::KEYWORD=DOMAIN;`
fromAID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40
toAID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40
KEYWORD=DOMAIN:
• CKTID = Character string of up to 45 alphanumeric characters, including hyphens (-), delineated by escape quotes (\")
• **Null**
Example:
`(for channel 34) ENT-CRS-WCH:FUJITSU-NODEB: OS1-1-PE1-34,OS1-19-PE1-34:CTAG; ENT-CRS-WCH:FUJITSU-NODEB: OS1-19-PE1-34,OS1-1-PE1-34:CTAG;`
	NE ▸ *Graphical Cross-Connects*
	The Cross-Connects window opens.
	From the View Rate drop-down list, select XC_WCH.
	From any one of three drop-down lists (top-left, top-right, or bottom), select the equipment or facility associated with the fromAID.
	From a different drop-down list, select the equipment or facility associated with the toAID.
	Click on the fromAID to begin drawing a line that represents the connection.
	Click on the toAID to terminate the line.
	The pending connection is now represented by a dashed line with an arrow pointing to the toAID.
	Entity ▸ *Operations Dialog*
	Click Create.
	The dashed line becomes solid.
	Close the Operations dialog box.
	Do not close the Cross-Connects window.

Step 4
At Node B, verify that pass-through cross-connects have been provisioned in both directions for each WCH channel previously identified in Record Pass-Through Channels for Node B.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEB:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	The Properties dialog box opens.
	Verify that the provisioning parameters are correct.
	Close the Properties dialog box.

Release Protection Switches

Step 5
Retrieve conditions to identify the forced protection switches.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 6
Release each forced protection switch.

TL1	NETSMART 500

`RLS-PROTNSW-WCH:TID:AID:CTAG;`
AID:
• OS1-s-PE1-c
  • s = 1, 19 (slot number)
  • c = 1…40 (channel number)
Example:
`RLS-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-1:CTAG;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ *Operations Dialog*
	Click the Protection tab.
	Click the Release tab.
	Click Release.

Step 7
Retrieve all cross-connects.

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
 	
Example:
`RTRV-CRS-WCH:FUJITSU:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	
	Select one or more cross-connect components.
	
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	
	Entity ▸ *Properties View*
	
	The Properties dialog box opens.
	Record the cross-connects.
	
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 8
Identify all OCh-DPRING–protected drop cross-connects that have parameter SST=SWITCH.

Note: *The value of SST (**`DEF`** or **`SWITCH`**) indicates whether the preferred path is currently used (**`DEF`**) or not (**`SWITCH`**).*

Step 9
Do local procedures require switch back to the preferred path?

If YES:
Proceed to Step 10.

If NO:
Proceed to Step 14.

Step 10
For each channel identified in Step 8, initiate a manual protection switch.

Caution: *A momentary hit of traffic occurs each time traffic is switched.*

Note: *Observe the TL1 response messages, and verify that the traffic has switched. Denial of a manual switch indicates that the switch could not be performed without dropping traffic. If this situation occurs, trouble clear the system for a cabling or provisioning problem.*

TL1	NETSMART 500

`OPR-PROTNSW-WCH:TID:AID:CTAG::MAN;`
AID:
• OSn-s-PE1-c
  • n = 1…4
  • s = 1, 19
  • c = 1…40 (channel number)
Example:
`OPR-PROTNSW-WCH:FUJITSU:`
`OS1-1-PE1-22:CTAG::MAN;`
	In the tree view, click the Facilities tab.
	Expand the appropriate shelf component, and select the WCH facility.
	Entity ▸ ***Operations Dialog***
	Click the Protection tab.
	Click the Operate tab.
	From the SC drop-down list, select MAN.
	Click Operate.
	A confirmation dialog box opens.
	Click Yes.
	Close the Operations dialog box.

Step 11
At Node A, retrieve all cross-connects, and confirm that all OCh-DPRING–protected drop cross-connects are switched to the preferred path (SST=DEF).

TL1	NETSMART 500

`RTRV-CRS-WCH:TID:ALL:CTAG;`
Example:
`RTRV-CRS-WCH:FUJITSU-NODEA:ALL:CTAG;`
	In the tree view, click the Cross Connect tab.
	Select one or more cross-connect components.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ ***Properties View***
	The Properties dialog box opens.
	Record the cross-connects.
	Close the Properties dialog box.

The normal response format for each retrieved cross-connect is:

```
  TID DATE TIME
M CTAG COMPLD
  "fromAID,toAID:CCT:KEYWORD=DOMAIN:SST"
```

Step 12
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 13
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 14.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 14.

Step 14
Repeat Steps 5 through 13 for each node in the network, and then go to Step 15.

Verify Network Is Free of Alarms and Conditions

Step 15
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	The Active Alarms window opens.
	View ▸ *Filter*
	The Alarm Filter dialog box opens.
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	Verify the condition in the Active Alarms window.
	Close the Active Alarms window.

Step 16
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 17.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 17.

Step 17
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

✔ This procedure is complete.

9.9
Upgrade 40-Ch Express Node to 40-Ch WSS Node
Applicable to Small and ETSI Configuration Systems

In this section:

The procedural flowchart is shown in the following figure.

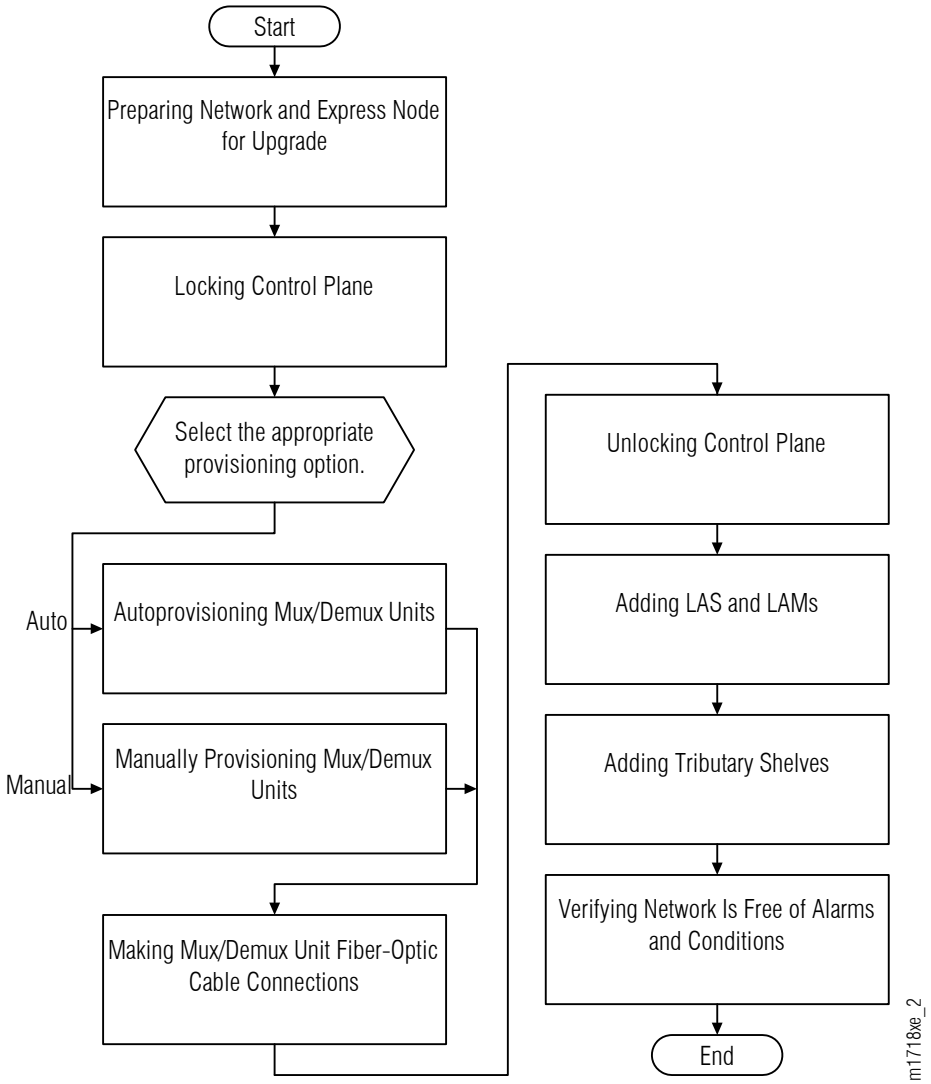


Figure 343: Upgrading Express Node to 40-Ch WSS Node–In Service (Procedural Flowchart)

This procedure is written for the example 4-node ring shown in the following figure. In this example, Node B is the node that is to be upgraded, Node A and Node C are its neighbors, and Node D is the other node, which is not adjacent to Node B. The procedure can also be used for ring networks with more than four nodes. In multiple-node ring networks, all nodes that are not adjacent to Node B are treated as Node D is treated.

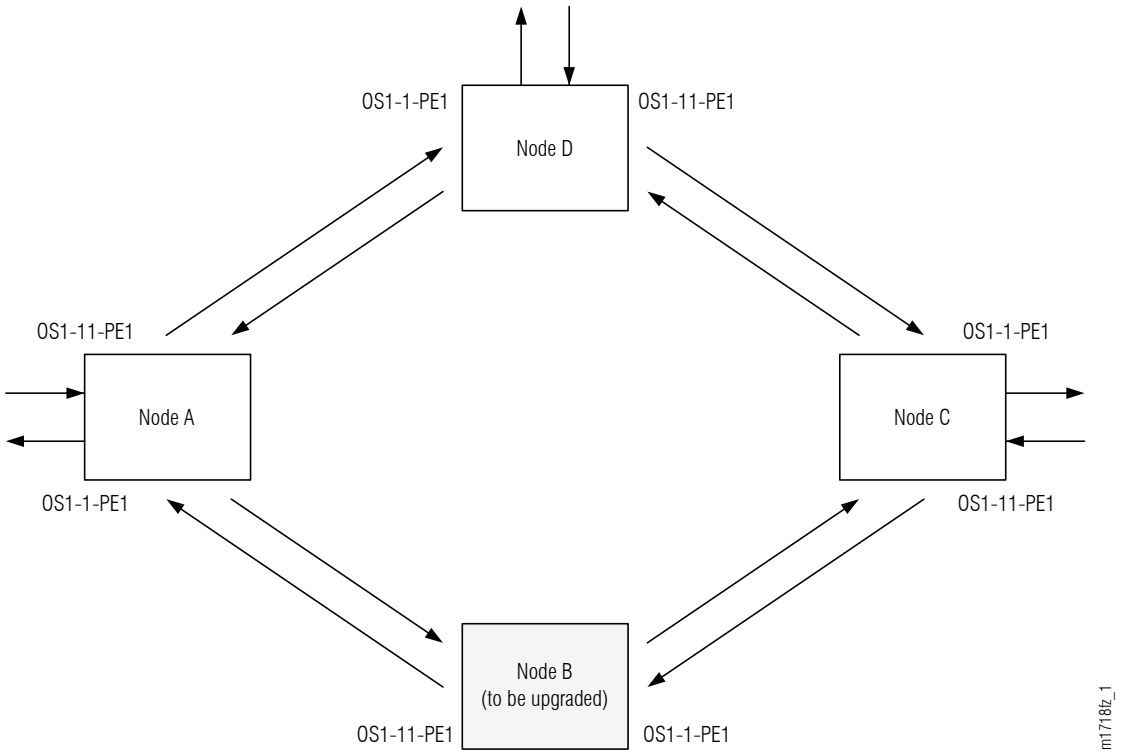


Figure 344: Ring Network Configuration

This procedure can also be used to upgrade linear networks as shown in the following figure.

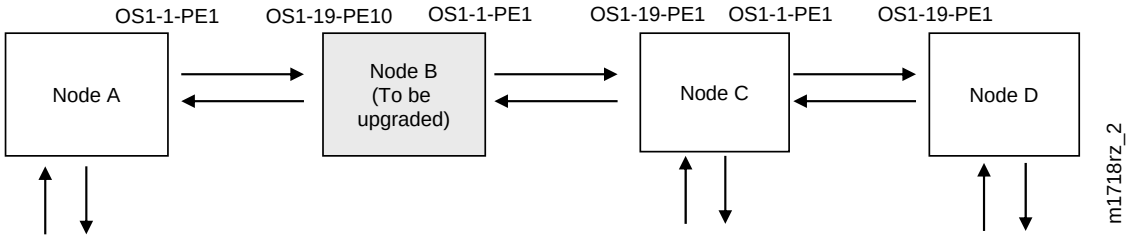


Figure 345: Linear Network Configuration

Attention: *Before performing this procedure, ensure that prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

9.9.1 Preparing Network and Express Node for Upgrade

Prepare the Express node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

TL1	NETSMART 500	

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	Comm. Port: COMx (for example, COM2)
	Configure: use default[112]
		For **TERM2** (TCP/IP):
		TID: FUJITSU
		User ID: ROOT
		Password: ROOT/(Route66K)
		Conn. Mode: TCP/IP
		IP Address: 192.168.1.1
		Port: 2024

	Click Logon. The NETSMART 500 NE View opens. The Security Message dialog box opens. Click OK. ***Note:*** *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*	

Clear Alarms and Conditions on Network

Step 2
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

[112] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 4
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 5
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 4.

Verify Amplifier Type

Step 6
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-11 (slot 11)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-11:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slot 1 and 11.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE. Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 7
Proceed to Locking Control Plane.

Clear Alarms and Conditions on Network

Step 8
At each node, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

Step 9
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 4.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 4 to verify the software version of Node B.

Verify Software Version

Step 10
At Node B, retrieve the software version information.

TL1	NETSMART 500

`RTRV-VERSION:TID::CTAG;`
 	
Example:
`RTRV-VERSION:FUJITSU::CTAG;`
	In the tree view, select the NE (the top-level system entity).
	
	Entity ▸ *Properties View*
	
	In the Current Values area of the Properties dialog box, determine the value of Active GISSUE.
	
	Close the Properties dialog box.

Step 11
Is the active GISSUE correct?

Note: *The GISSUE value for FLASHWAVE 7500 Release 6.1 software is 06-01-1.*

If YES:
Proceed to Step 6.

If NO:
Upgrade the system software as described in Upgrading System Software from Release 4.1, and then repeat Step 10.

Verify Amplifier Type

Step 12
Retrieve the amplifier types installed on Node B.

TL1	NETSMART 500

`RTRV-EQPT:TID:AID:CTAG;`
AID:
• OS1-1 (slot 1)
• OS1-11 (slot 11)
Example:
`RTRV-EQPT:FUJITSU:OS1-1&OS1-11:CTAG;`
	In the tree view, select the Equipment tab.
	Expand the Main Optical shelf.
	Select slot 1 and 11.
	Note: *Select more than one component using CTRL+click (multiple) or SHIFT+click (range).*
	Entity ▸ *Properties View*
	In the Current Values area of the Properties dialog box, determine the value of TYPE. Use the Selected Entities drop-down list to select between selected amplifiers.
	Close the Properties dialog box.

The amplifier types must be APMA-M2U1 or APMA-ULU1.

Step 13
Proceed to Locking Control Plane.

✔ This procedure is complete.

9.9.2 Locking Control Plane

These steps are used to lock the control plane feature for Node B. The control plane must be locked before the system type can be changed.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and Express Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Lock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=Y;`
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=Y;`
	NE ▸ *System Operations*
	The Operations dialog box opens.
	Click the Control Plane tab.
	For the LOCK command parameter, click Yes.
	Click Modify.
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is locked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
 	
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the value for LOCK is Yes.
	
	Close the Operations dialog box.

Step 4
Select the applicable procedure:

- For autoprovisioning, proceed to Autoprovisioning Mux/Demux Units.
- For manual provisioning, proceed to Manually Provisioning Mux/Demux Units.

9.9.3 Autoprovisioning Mux/Demux Units

The Mux/Demux unit (MDMA-RMC1) can be autoprovisioned as described in Autoprovision Optical/ILA Shelf Equipment and Facilities.

Note: *For Mux/Demux unit slot locations, refer to* Slot Labels and AIDs.

Note: *All equipment except shelves can be autoprovisioned. Shelves require manual provisioning to be placed in service.*

Step 1
Using the procedure in Autoprovision Optical/ILA Shelf Equipment and Facilities, install and autoprovision the Mux/Demux unit.

Step 2
Proceed to Making Mux/Demux Unit Fiber-Optic Cable Connections.

9.9.4 Manually Provisioning Mux/Demux Units

The Mux/Demux unit (MDMA-RMC1) can be manually provisioned as described in Manually Provision Optical/ILA Shelf Equipment.

Note: *For plug-in unit slot locations, refer to* Slot Labels and AIDs.

Note: *This procedure can be used to preprovision the slot. In this case, the unit will assume the specified provisioning when the unit is eventually installed in the slot. Note that an unequipped alarm will be raised until the unit is installed.*

Step 1
Using the procedure in Manually Provision Optical/ILA Shelf Equipment, install and manually provision the Mux/Demux unit.

Step 2
Proceed to Making Mux/Demux Unit Fiber-Optic Cable Connections.

9.9.5 Making Mux/Demux Unit Fiber-Optic Cable Connections

Step 1
Using the procedure in Connect MDMA-RMC1 Unit to Amplifier and SFMA-CMC1 Units, install fiber-optic cables to connect the Mux/Demux units.

Step 2
Proceed to Unlocking Control Plane.

9.9.6 Unlocking Control Plane

These steps are used to unlock the control plane feature for Node B. The control plane feature was locked in Locking Control Plane, to change the system type. These steps restore the control plane to the unlocked state.

Step 1
If not already done, log on Node B (refer to Step 1 in Preparing Network and Express Node for Upgrade). If already logged on, proceed to the next step.

Step 2
Unlock the control plane.

TL1	NETSMART 500

`ED-CPLANE:TID::CTAG:::LOCK=N;`
 	
Example:
`ED-CPLANE:FUJITSU::CTAG:::LOCK=N;`
	NE ▸ *System Operations*
	
	The Operations dialog box opens.
	Click the Control Plane tab.
	
	For the LOCK command parameter, click No.
	Click Modify.
	
	Do not close the Operations dialog box.

Step 3
Verify that the control plane is unlocked.

TL1	NETSMART 500

`RTRV-CPLANE:TID::CTAG;`
 	
Example:
`RTRV-CPLANE:FUJITSU::CTAG;`
	In the Current Values area of the Operations dialog box, verify that the updated information is correct.
	
	Close the Operations dialog box.

Step 4
Proceed to Adding LAS and LAMs.

9.9.7 Adding LAS and LAMs

After completing the procedures in Preparing Network and Express Node for Upgrade through Unlocking Control Plane, refer to the following table for detailed procedures for installing the LAS and LAMs to support add/drop services at Node B.

Step 1
Install LAS and LAMs using the procedures referenced in the following table.

Table 167: Installing LAS and LAMs

Task	Document and Section
Install LAS shelf in rack.	Installing the ETSI LAM/DCM Shelf (SDL1)
Install LAMs and MPO connections.	Install LAMs and MPO Connections

Step 2
Proceed to Adding Tributary Shelves.

9.9.8 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 168: Adding Tributary Shelves

Task	Document and Section	
	Small Configuration	ETSI Configuration
Install Tributary shelf in rack.	Installing the Optical/Tributary Shelf	Installing the Optical/Tributary Shelf
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables	Installing Power and Ground Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units	
Create Tributary shelf entity, and install shelf processors,	Create Subtending Shelves and Install Shelf Processors	
Provision synchronization and/or Tributary shelf OSC units, if required.[113]	Provision Tributary Shelf Equipment Provision Synchronization	

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

9.9.9 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify that the network is free of alarms and conditions:

Step 1
At each node, retrieve alarms and conditions.

[113] Refer to procedure for applicability.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to Responding to Alarms and Conditions for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
 	
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	
	Click Yes to continue.

This procedure is complete.

9.10
Upgrade 40-Ch WSS Node to HUB Node
Applicable to Small and ETSI Configuration Systems

In this section:

The procedural flowchart is shown in the following figure.

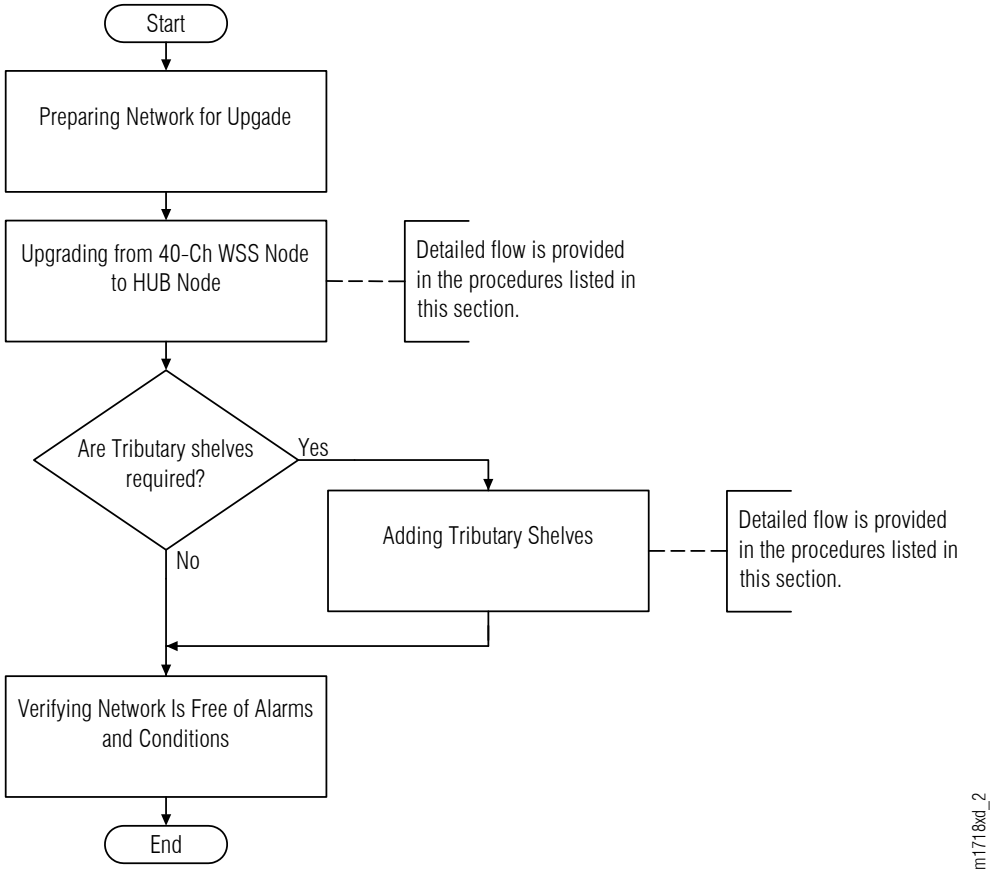


Figure 346: Upgrading 40-Ch WSS Node to HUB Node (Procedural Flowchart)

The FLASHWAVE 7500 Small/ETSI Configuration system supports HUB nodes that include more than one Optical shelf. HUB nodes are typically used to interconnect rings and to route traffic from one ring to another within the optical domain.

The degree of connectivity of a HUB node is defined as the number of network connections to the node. The following figure illustrates the concept of degrees of connectivity. For example, a ROADM node is a 2-degree node, and a HUB node that is part of two interconnected rings is a 4-degree node. The Small/ETSI Configuration system supports HUB nodes up to eight degrees, as illustrated in the following figure.

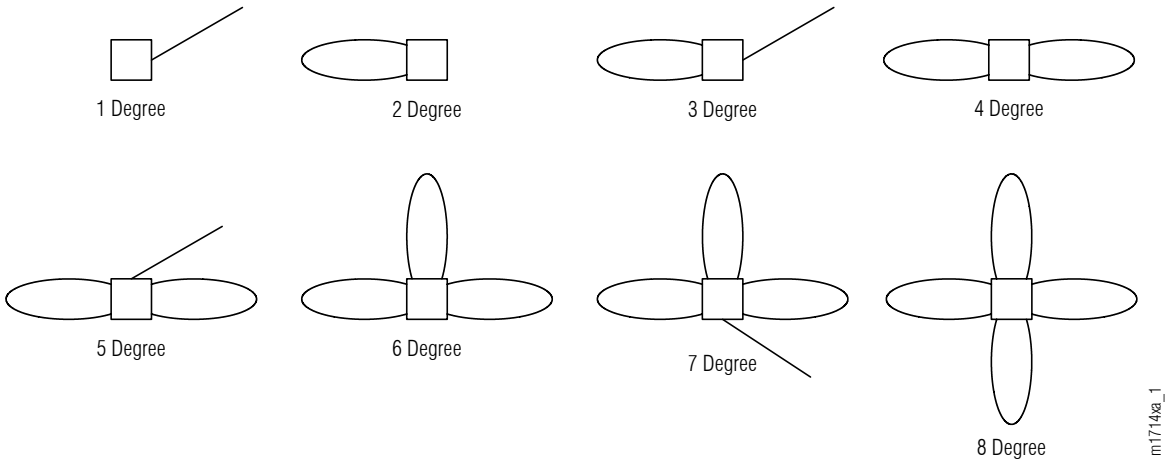


Figure 347: Degrees of Connectivity (Small Configuration, HUB Node)

For more information on HUB applications, refer to Core, Small, and ETSI Configuration Applications.

Attention: *Before adding shelves or services, ensure that all prerequisite procedures have been performed in the proper sequence. Failure to do so may result in an error. Refer to* Provisioning Hierarchy *for more information. Refer to* Introduction to Maintenance and Trouble Clearing *to clear error messages.*

Attention: *When entering TL1 commands or NETSMART 500 steps, refer to* Introduction to TL1 Commands *for information about preconditions, postconditions, AIDs, and parameters. Specific information is available by clicking the hyperlinked TL1 command name (for example, ACT-USER) in the TL1 column.*

9.10.1 Preparing Network for Upgrade

Prepare the node for the upgrade as follows:

Step 1
Log on Node B. If already logged on, proceed to the next step.

Note: *Up to 11 users (including operations support system [OSS]) can log on a single node for monitoring or provisioning purposes.*

Note: *The target identifier (TID), user identifier (UID), and private identifier (PID) values apply to initialized (factory default) systems. Consult your Network System Administrator for specific TID, UID, and PID values.*

Note: *The following table includes brief instructions for setting up the craft interface. For detailed information, refer to* Setting Up Craft Interface (TL1 Session through TERM1) *through* Setting Up Craft Interface (NETSMART 500 Session through TERM2).

TL1	NETSMART 500
Start a terminal or terminal emulator program (for example, HyperTerminal). For **TERM1** (Serial): Press CTRL+X. For **TERM2** (TCP/IP): Establish a Telnet session using IP address 192.168.1.1 and default port 23. The Welcome screen opens. Press 3 for TL1.	To launch the NETSMART 500 user interface from a Microsoft® Windows® platform, select the following from the Windows taskbar: *Start* ▸ *All Programs* ▸ *Fujitsu* ▸ *NETSMART 500* The NETSMART 500 Dashboard opens. Click the Logon icon, or select : *NE* ▸ *Logon* ***Note:*** *If this is an Enhanced Security System, a warning message appears. You must read and agree to the conditions to access the system. Click I Agree to continue.* The NE Logon dialog box opens. Make the following selections:

`ACT-USER:TID:UID:CTAG::PID;`
TID:
• FUJITSU (Target identifier of the node; 7 to 20 non–case-sensitive, alphanumeric characters)
UID:
• ROOT (User identifier; 4 to 10non–case-sensitive, alphanumeric characters)
PID:
• ROOT/(Route66K) (Private identifier associated with the UID. For the basic mode, the PID must have 6 to 10 characters with at least one non–case-sensitive, alphabetic character and one nonalphabetic character such as a number or ! @ # $ % ^ ( ) _ + | ~ { } [ ] ? or -. For the enhanced security mode, the PID must have 10 to 20 characters with at least two characters from each of four groups: lowercase letters, uppercase letters, numbers, and special characters ! @ # $ % ^ & ( ) or *. The enhanced security PID can also include special characters _ + | { } [ ] or ~. The PID must not contain the associated UID.)
 	
Example:
`ACT-USER:FUJITSU:ROOT:CTAG::ROOT;`
	For **TERM1** (Serial):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: Serial
	
	Comm. Port: COMx (for example, COM2)
	
	Configure: use default[114]
	
	For **TERM2** (TCP/IP):
	TID: FUJITSU
	User ID: ROOT
	Password: ROOT/(Route66K)
	Conn. Mode: TCP/IP
	IP Address: 192.168.1.1
	Port: 2024
	
	Click Logon.
	
	The NETSMART 500 NE View opens.
	
	The Security Message dialog box opens.
	Click OK.
	
	Note: *Refer to NETSMART 500 User Guide, for complete instructions on starting the NETSMART 500 user interface.*

Step 2

At each node, retrieve alarms and conditions.

[114] The default serial port settings are recommended: baud rate– 9600, parity– none, data bits– 8, stop bits– 1.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
 	
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	
	The Active Alarms window opens.
	
	View ▸ *Filter*
	
	The Alarm Filter dialog box opens.
	
	Ensure that all Fault Types and Severity Levels are selected in the Alarm Filter dialog box.
	Click Close.
	
	Verify the condition in the Active Alarms window.
	
	Close the Active Alarms window.

Step 3
Are any active alarms or conditions being reported on the node?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Upgrading from 40-Ch WSS Node to HUB Node.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Upgrading from 40-Ch WSS Node to HUB Node.

9.10.2 Upgrading from 40-Ch WSS Node to HUB Node

The procedures related to the upgrade from 40-Ch WSS node to HUB node are given in Introduction to Equipment Installation, and Introduction to System Turn-Up Small and ETSI Configuration. The following table lists the procedures in the order in which they are completed.

Step 1
Follow the procedures listed in the following table to upgrade from a 40-Ch WSS node to a HUB node.

Table 169: Upgrading from 40-Ch WSS Node to HUB Node

Task	Document and Section	
	Small Configuration	ETSI Configuration
Install Auxiliary shelf in rack.	Installing the Optical/Tributary Shelf	Installing the Optical/Tributary Shelf

Table 169: Upgrading from 40-Ch WSS Node to HUB Node (Cont.)

Task	Document and Section	
	Small Configuration	ETSI Configuration
Install LAS and DCM shelf.	Installing the ETSI LAM/DCM Shelf (SDL1)	
Install power, ground, and alarm cables to Auxiliary shelf.	Installing Power, Ground, and Alarm Cables	Installing Power and Ground Cables
Install LAN cable to Auxiliary shelf.	Installing LAN Cable (Optical/Tributary Shelf)	Installing LAN Cable (Optical/Tributary Shelf)
Install RICC cable to Auxiliary shelf.	Installing RICC Cable (Optical Shelf)	Installing RICC Cable (Optical Shelf)
Verify shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units	
Create Auxiliary shelf, and install shelf processors.	Create Subtending Shelves and Install Shelf Processors	
Provision Auxiliary shelf equipment and facilities.	Provision Optical/ILA Shelf Equipment and Facilities	
Provision Tributary shelf equipment.	Provision Tributary Shelf Equipment	
Interconnect amplifier and OSC units.	Interconnect Amplifier and OSC Units	
Install 40-Ch WSS system cables.	Install WSS System Cables	
Install LAMs and MPO connections.	Install LAMs and MPO Connections	
Connect DCMs.	Connect DCMs or Loopback Cables	
Connect network fiber-optic cables.	Connect Network Fiber-Optic Cables	

Step 2
Proceed to Adding Tributary Shelves.

9.10.3 Adding Tributary Shelves

Use the following procedure to add Tributary shelves:

Step 1
Install Tributary shelves (if required) using the procedures referenced in the following table.

Table 170: Adding Tributary Shelves

Task	Document and Section	
	Small Configuration	ETSI Configuration
Install Tributary shelf in rack.	Installing the Optical/Tributary Shelf	Installing the Optical/Tributary Shelf
Install power, ground, and alarm cables to Tributary shelf.	Installing Power, Ground, and Alarm Cables	Installing Power and Ground Cables
Install LAN cable to Tributary shelf.	Installing LAN Cable (Optical/Tributary Shelf)	Installing LAN Cable (Optical/Tributary Shelf)
Verify Tributary shelf labeling and intershelf connections.	Verify Shelf Labeling, Verify LAN and RICC Cable Connections, and Install Fan Units	
Create Tributary shelf entity, and install shelf processors,	Create Subtending Shelves and Install Shelf Processors	
Provision synchronization and/or Tributary shelf OSC units, if required.[115]	Provision Tributary Shelf Equipment Provision Synchronization	

Step 2
Proceed to Verifying Network Is Free of Alarms and Conditions.

9.10.4 Verifying Network Is Free of Alarms and Conditions

Use the following procedure to verify the network is free of alarms and conditions:

Step 1
At each node in the system, retrieve alarms and conditions.

TL1	NETSMART 500

`RTRV-COND-ALL:TID::CTAG;`
Example:
`RTRV-COND-ALL:FUJITSU::CTAG;`
	NE ▸ *Alarms*
	View ▸ *Filter*
	Verify that all Fault Types and Severity Levels are selected as reporting.
	Click Close.
	Close Active Alarms window.

[115] Refer to procedure for applicability.

Step 2
Are any active alarms or conditions being reported on the nodes?

If YES:
Clear all active alarms and conditions. After all alarms and conditions are cleared (or accounted for), proceed to Step 3.

Note: *Refer to* Responding to Alarms and Conditions *for information on clearing alarms.*

If NO:
Proceed to Step 3.

Step 3
Log off the nodes.

TL1	NETSMART 500

`CANC-USER:TID:UID:CTAG;`
Example:
`CANC-USER:FUJITSU:ROOT:CTAG;`
	File ▸ *Exit*
	Click Yes to continue.

This procedure is complete.

Index

F

H

I

L

M

N

O

P

R

S

T

U

V

W